GDPR: A Practical Guide for Schools

Document date	8 May 2018
Version	14

Contents

Title	Page Number
Why we have developed 'GDPR: A Practical Guide for Schools'	2
What is GDPR? And why do schools need to prepare for GDPR?	3
Key definitions	7
Where to start? – Overall organisation	10
The Information Governance and Management Organisation (IGMO)	12
Data streams and data handling	13
Training and education of data handlers	15
Data streams and pupils and parents	16
Data streams and employees	24
Data streams and governors	27
Data streams and alumni / past parents	30
Development and alumni relations	32
Data breaches	50
Privacy impact assessment	55
Draft privacy notices and appendices	61
Draft letter to suppliers and draft data processing agreements	72
Draft trip letters to parents and travel agent	74
Data retention and data retention policy	75
Subject Access Requests	88
Cyber Security	92
Our GDPR checklist for schools	93

Why have we developed a GDPR guide for schools?

Every school is different. What personal data a school gathers and stores, and why and how a school processes personal data will differ, therefore there cannot be a 'one size fits all' approach to complying with GDPR. The GDPR is principle-based legislation and compliance means respecting these principles. This means that there is often no definitive 'right' or 'wrong', and it will depend on the context. For example, what one individual considers to be fair processing of their personal data may be different to another.

Therefore, this guide does not try to give you definitive answers on how to comply with GDPR but aims to help schools understand the changes to data protection legislation, and to outline the process each school needs to go through to achieve GDPR compliance. It is about giving schools the confidence to apply the principles of GDPR to the circumstances of your own school. This guide contains detailed information on the different aspects of GDPR in relation to the specific needs of schools and refers to further information and resources that are available on the ICO website or from other specialist organisations where appropriate.

What does this guide include?

We know that schools want to do the right thing and to comply with data protection legislation.

This guide includes information and guidance on all aspects of data compliance tailored to the independent schools' sector, including audit questions designed to expose any areas within a school that may not be GDPR compliant, templates tailored to schools, and responses to FAQs from ISBA and IDPE members.

It contains sections dealing with each of the five main data streams schools govern and manage, and the different areas of compliance that schools need to consider from cyber security and data breaches to updating privacy policies and data retention. At the end of the document there is a checklist designed to act as a quality check on the work done by the school as its moves towards GDPR compliance.

Who is it for?

This guide is intended for any individual within a school who is involved in any aspect of data control. It will be particularly relevant to bursars, governors, senior leaders and development/alumni relations professionals, who are all likely to have some responsibility for data control.

Caution

GDPR is an update of existing data protection legislation and whilst the law comes into force on 25 May 2018, the ICO has emphasised that GDPR compliance should be seen as a journey which requires an ongoing commitment. This document has been produced by ISBA and IDPE, in association with legal partners, Farrer & Co, based on advice and guidance that is currently available, and it will be regularly updated as further guidance is released.

In using the guide, schools acknowledge that this is not definitive GDPR guidance This guide has been compiled using information from multiple sources to provide a clear starting point for schools as they evolve their data compliance policies and procedures. It provides tailored guidance, and where appropriate refers to other guidance that is available either from the ICO itself or from other specialist organisations.

Please note that the information in this Guide is intended to provide only a general overview of the law in this area.

It is not intended to be a substitute for legal advice tailored to the circumstances of your school.

What is GDPR?

The General Data Protection Regulation (GDPR) is a new law which will replace the current Data Protection Act (DPA) 1998. The GDPR is the biggest overhaul of data protection legislation for over 25 years and every organisation that processes personal data will have to comply with the GDPR – it is not optional. Many of the requirements under GDPR already apply under the DPA, the GDPR however seeks to strengthen individual rights and introduce new ones where necessary.

What is the new Data Protection Bill and how does this differ

The GDPR affects all member states of the EU and has already been passed – we are currently in a grace period given to allow the UK to develop its new data protection framework. Despite Brexit, all organisations processing personal data will still have to comply with the GDPR. However, the GDPR gives members states limited opportunities to make provisions for how GDPR applies in their country – one element of this is the Data Protection Bill.

The Data Protection Bill is currently making its way through Parliament: in its current form it is going to have certain narrow, but potentially significant, impacts on independent school in areas such as safeguarding and subject access requests. For further information visit https://ico.org.uk/for-organisations/data-protection-bill/ but amendments are still being made and schools should be alert for updates as it reaches the final form that will become the Data Protection Act 2018.

Why do schools need to prepare for GDPR?

Schools process personal data and therefore it is their legal responsibility to comply with the new data protection legislation. Schools act as data controllers in a number of ways, including:

- As an employer processing the personal data of staff, volunteers and governors
- As an educational provider processing the personal data of pupils and their parents/guardians, and marketing its services
- As a 'membership' organisation processing the personal data of alumni and past parents, and raising awareness of appeals

Likewise, other organisations related to the school may also be data controllers such as alumni societies, PTAs or school clubs, and will also need to consider compliance under GDPR.

When do schools need to be compliant with GDPR?

GDPR becomes effective on 25 May 2018. Schools need to be thinking now about how they become compliant and make any necessary changes to ensure this.

The Information Commissioner's Officer (ICO) will be regulating on GDPR from 25 May 2018, but don't panic. GDPR is an update of existing requirements under the current data protection legislation and the Information Commissioner has emphasised that *'those who self-report, who engage with the ICO to resolve issues and who can demonstrate effective accountability arrangements can expect this to be taken into account when we consider regulatory action.'*

Who does GDPR apply to?

The GDPR applies to data controllers, i.e. the school and to data processors. A controller determines the purposes and means of processing personal data; the processor is responsible for processing personal data on behalf of a controller.

The GDPR applies to the processing of personal data carried out by organisations operating within the EEA (meaning the EU plus Iceland, Norway and Liechtenstein – whether this will in time also include the UK is still to be determined, but the Regulation itself will be made law in the UK before it leaves the EU and will remain UK law unless specifically repealed).

It also applies to organisations outside the EEA that offer goods or services to individuals in the EU. Therefore, while a UK school with international students must comply (as an organisation within the EEA), equally a school setting up an international school outside of the EEA will still need to comply if marketing to and accepting students from within the EEA. Although this raises an "international transfer of personal data", it should be permissible as part of a contract with the data subject: but that is far from the only way in which regulated schools at home or abroad will need to apply.

The GDPR applies to the processing of 'personal data', meaning the processing of any personal information relating to an individual, who can be directly or indirectly identified as a result.

GDPR, like the existing data protection legislation and UK privacy law, only applies to living individuals. There is, however, a duty of care in respect to the personal data of the deceased in some cases and if retaining "personal" data on an individual who is deceased, it is still important to consider what you are retaining and the purpose for doing so.

What is different under GDPR to the current data protection legislation (Data Protection Act 1998)?

As before, the principles of the new GDPR focus on the purpose for processing personal data; organisations must process personal data in a lawful, fair and transparent way, and for specified explicit and legitimate purposes. **GDPR however expects a higher standard of transparency (in Privacy Notices) and accountability (in demonstrating internal decision-making) about these purposes.**

Legal basis for processing personal data

The requirement to have a lawful basis in order to process personal data is not new, however the GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing. The six lawful bases for processing any personal data are broadly similar to the old conditions for processing, however there are some changes (for example to the definition of 'consent') and for public authorities, including for these purposes Free Schools and Academies, who now need to consider the new 'public task' basis first for most of their processing.

(a) Consent: the individual has freely given clear, informed consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life (the ICO takes a stricter view on this than certain government guidance).

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

There is no one way to process personal data; and no single basis is 'better' than the others. Each school will need to review their existing lawful bases for processing personal data, and check that these remain the most appropriate. In many cases these are likely to be the same as the existing condition(s) for processing. For further information, visit https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Special category data

If processing special category data, the school will need to identify both a lawful basis for general processing and an additional condition for processing this type of data. For further information, visit https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Accountability and transparency

The GDPR brings in new accountability and transparency requirements. The school must clearly demonstrate compliance through documenting their purpose(s) for processing personal data and the appropriate lawful basis (or bases) in their privacy notice(s) and inform individuals about how and why they are processing their personal data, through regularly sharing their privacy notice.

Schools must also consider when and if the purpose for processing personal data changes, for example when a pupil leaves school and the school continue to communicate with them as an alum, has the purpose for processing personal data changed? and if so, is this detailed within the school's privacy policy and has this information been shared with the individuals in question?

Individual rights

As well as setting out the different bases for processing personal data, the GDPR also includes a number of rights for individuals which schools will need to consider:

- The right to be informed – the GDPR is more specific about the information you need to provide to individuals about what you do with their personal data, and – whether or not you collect the information from them directly – you must provide this in a way that is easy to access, read and understand. This is where Privacy Notices come in.

- The right of access – under the GDPR, individuals will have the right to obtain: confirmation that their data is being processed and access to their personal data. You must provide a copy of the information free of charge (unless a request is clearly excessive or unfounded), within one month of the request.

- The right to rectification – the GDPR includes a right for individuals to have inaccurate data rectified, and if a request is made you have one calendar month to respond.

- The right to erasure – the GDPR introduces a new right, the right to erasure (sometimes called the right to be forgotten). Such a request can be made in writing or verbally and should be responded to within a month. There are however, certain circumstances when the right to erasure does not apply.

- The right to restrict processing – this is an alternative to the right to erasure and offers individuals the opportunity to restrict how their personal data is processed, for example where personal data is inaccurate or an individual wants to limit how an organisation uses their data. Again, a request can be made in writing or verbally and should be responded to within a month.

- The right to data portability – this allows an individual to obtain and reuse their personal data for their own purposes across different services.

- The right to object (including objecting to direct marketing) – individuals have the right to object to processing of their personal data based on legitimate interests (to 'opt out') or the performance of a task in the public interest/exercise of official authority. This includes processing of personal data for the purpose of direct marketing, profiling and scientific/historic research and statistics. The right to object must be included in your school's privacy notice and at the first point of communication.

- The right to withdraw consent – where consent is relied on. This does not mean that any processing previously carried out in reliance on that consent becomes unlawful, or must necessarily always be rectified, but the withdrawal must be respected.

- Rights in relation to automated decision making and profiling – under GDPR, you can only carry out automated decision making or automated processing of personal data (without any human involvement), including profiling them, where this type of decision-making is necessary for a contract, authorised by Union or Member state law or based on the individual's consent.

For further information, visit https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Other key changes under GDPR

- Contracts – whenever a data controller uses a data processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place. This was always the case, but the requirements have become more prescriptive. For further information, visit https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

- Documentation – the documentation of processing activities, covering areas such as the purpose for processing personal data, data sharing and retention, is a new requirement under the GDPR. There is a limited exemption for small and medium-sized organisations. If you have less than 250 employees, for further information, visit https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

- DPIAs – Data Privacy Impact Assessments or DPIAs are the GDPR version of a Privacy Impact Assessment. The GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in high risk to individuals' interests. If your DPIA identifies a high risk which you cannot mitigate, you must consult with the ICO. You will need to review your existing processing operations and decide whether you need to carry out a DPIA, and a DPIA is likely to be necessary if an area of work is new or potentially high risk. However, a DPIA need not be especially long or complicated and can be adapted to the processing need and likely impact.

- DPOs – the GDPR introduces a duty for certain organisations to appoint a DPO or Data Protection Officer to monitor internal compliance, and to inform and advise your data protection obligations. Maintained schools, Free Schools and Academies / Multi-Academy Trusts (MATs) will need to do so. Current indications are that most

independent schools will not need to appoint a DPO: however if they do, or use that title, they will need to comply with the DPO requirements (which are quite burdensome). All schools should however appoint a data lead to demonstrate your school's compliance with GDPR. If the ICO decides at a later date that it is best practice for independent schools to appoint a DPO, this person may be well-positioned to step into those shoes – subject to any potential conflict with their other role at the school.

- Security of personal data – the GDPR requires personal data to be processed in a manner that ensures a level of security appropriate to its nature. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires appropriate technical and organisational measures (including policy and staffing). For further information, visit https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

- International transfer of personal data – the GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. There are various technical work-arounds to this.

- Data breaches – the GDPR introduces a duty to inform the ICO within 72 hours (including weekends or out of working hours) if a school has a data breach that is likely to cause any risk to individuals, and your school should must have a data breach policy in place outlining this process.

Key definitions

Information Commissioner's Office (ICO): is the UK's independent body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. For more information, visit: https://ico.org.uk/about-the-ico/

Article 29 Working Party: is the short name for the Data Protection Working Party established by the European Commission to provide independent advice on data protection matters and help in the development of harmonised policies for data protection in the EU member states.

General Data Protection Regulations (GDPR): is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU).

Data Protection Bill: updates data protection laws in the UK, supplementing the GDPR, as well as extending data protection laws to areas which are not covered by the GDPR. It is likely to come into force later this year, although it was meant to take effect alongside GDPR.

Privacy and Electronic Communications Regulations (PECR): sits alongside the current Data Protection Act (and in the future the Data Protection Bill/GDPR) to give individuals specific privacy rights in relation to electronic communications, including marketing calls, e-mails, texts and faxes.

ePrivacy regulation: is the new EU regulation which aims to update the EU's existing e-Privacy framework in light of GDPR and is likely to come into force later this year.

Personal data: any information relating to a living individual who can be directly or indirectly identified from it. This include name, address, contact details but could also include two or more non-specific pieces of information that when combined could identify specific individuals, including for example, a combination of gender, birth rate, geographic indicator and descriptors. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

Processing personal data: means doing something with personal data – this includes personal data acquisition, processing, storage and disposal.

Special categories of personal data: data relating to highly sensitive pieces of information about an individual, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric information, health and a natural person's sex life or sexual orientation. It no longer includes criminal records or allegations, but these are similarly regulated under the Data Protection Bill.

Data controller: a controller determines the purposes and means of processing personal data. It is possible to have more than one data controller responsible for the same set of data, i.e. a school and alumni association. This may be as independent or joint data controllers: the latter requires more paperwork and regulatory compliance, but the data sharing between the two should be regulated by contract in either case.

Data processor: is responsible for processing personal data on behalf of a controller. An example may be an IT provider or payroll processor.

Data audit/data asset register: is the assessment of data held by an organisation, in relation to its purpose.

Data Protection Impact Assessment (DPIA): is a process which aims to identify and minimise the risks to an individual's privacy. You must do a DPIA for certain types of processing, but also if your processing is likely to result in a high risk to individuals' privacy rights.

Information Governance Management Organisation (IGMO): the overarching data governance and management organisation in a school.

Data Protection Officer (DPO): is an individual responsible for monitoring internal compliance. Whilst independent schools may not need to appoint a DPO, all schools should have a data lead, responsible for informing and advising on data protection obligations.

Data handler: is a member of staff (or volunteer) within an organisation who is responsible for processing personal data; this could be obtaining, recording or holding the data or carrying out any operation or set of operations on the data.

Data subject: is the person that the data relates to.

Data stream: is data relating to a group of individuals within a school community, for example pupils, alumni or staff.

Data set: is a specific segment or collection of data within a data stream, for example year 7 pupils, alumni from years 2000-2010 or teaching staff.

Lawful basis for processing: are the specific reasons, set out in law, for which you can process personal data (see section 'What is GDPR?' For further information).

Consent: is one of the six lawful bases for processing. Consent is when an individual has freely given clear, informed consent for you to process their personal data for a specific purpose. Under GDPR, consent must be a freely given, specific, informed and unambiguous indication of the individual's wishes.

Legitimate interests: is one of the six lawful bases for processing. An organisation can rely on legitimate interests when the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Legitimate interest is the most flexible lawful basis for processing personal data and is likely to be most appropriate where you are using personal data in ways that individuals would reasonably expect and where it has a minimal impact on their privacy.

However, to be lawful it does require a prior data risk assessment and specific inclusion within the Privacy Notice.

Legitimate Interests Assessment (LIA): is a test carried out by a data controller to decide if they can rely on legitimate interests as the lawful basis for processing personal data.

Privacy notice: is a document that explains how you will process an individual's personal data and should include, why you hold data, what data you hold, how you process this, if this data is shared with any other organisations and what rights the individual has.

Direct marketing: is the promotion of an organisation's aims and ideals, as well as the sale of products and services.

Prospect research: is used to learn more about existing or potential donors' backgrounds and their propensity and capacity to give.

Wealth screening: is a specific form of prospect research which looks at indicators of wealth to understand existing or potential donors' capacity to give.

Telephone Preference Service (TPS): is a central opt out register whereby individuals can register their wish not to receive unsolicited sales and marketing telephone calls. It is relevant under PECR as consent is needed to make contact with individuals via telephone numbers registered with the TPS.

Subject Access Request (SAR): is where an individual requests access to the information you hold about them.

Data Breach: is when there is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Where they reach a certain threshold of likely harm, these will have to reported to the ICO and in some cases those individuals affected. For more information please see page 53.

Data sharing: is the disclosure of data from one or more organisations to a third-party organisation or organisations, so within the context of a school this could be sharing data an ongoing basis with an alumni organisation or could be sharing personal data to a mail-house on a one-off occasion. The data sharing may happen between one or more data controllers, and routine or regular data sharing ought to be captured in a data sharing agreement. Please note that providing data to a data processor to carry out services on the school's behalf is not considered "sharing" in this sense, but must be regulated by a special type of binding contract.

Where to start? - Overall organisation

The changes to the data protection legislation under GDPR can seem somewhat daunting, particularly if you are responsible for data compliance throughout the school. The questions below act as a good starting point for schools to consider the different areas of compliance which need to be addressed when preparing for GDPR and links to further information and/or resources.

Date	
Type of school? Pupil age range, Boarding or not?	
Is the school registered with the ICO? If so, for which forms of data? Are there any other forms of data that need to be considered?	
Are there any other organisations related to the school that are data controllers and need to register with the ICO, i.e. alumni society?	
Have you carried out a data audit to identify what personal data you process and why?	
Is there an existing privacy notice? (It was known as the data protection policy) If so, when was it last updated?	
Is the privacy notice being updated and shared with your school community in light of GDPR?	
If so, is the update in age appropriate language? There may be a need for a privacy notice that is understandable by pupils of a particular age group, such as preparatory or secondary.	
Does the privacy notice notify individuals of their new data subject rights? Can it demonstrate how these rights will be observed by the school?	
Are further 'specialist' privacy notices needed for specific data streams within the school, such as staff or working with alumni/development?	
Are the legal bases for processing personal data under GDPR listed in the privacy notice? If the school is relying on legitimate interests as a basis for processing data are these all listed in the privacy notice?	
Has the school got consent to process "special category" personal data where necessary? (This cannot be covered by "legitimate interests", nor the parent contract: it might be lawful if the school is acting under a statutory right or obligation, including in connection with employment or some	

other duty of care; or if urgent e.g. medical grounds exist; or if it is covered under one of the special conditions of the Data Protection Bill concerning safeguarding or social care)	
Is this consent being updated in light of changes under GDPR?	
Has a DPO been appointed? If not, is the decision not to do so well-documented, and who is the compliance lead within the school?	
Are governors fully aware of their responsibilities around compliance under GDPR?	
Have all staff/volunteers who process personal data received relevant training in data protection?	
Is there a “data protection” policy which covers processing personal data of staff and volunteers?	
Is there a “storing and retention of records” policy?	
Is there an “acceptable use” policy for electronic devices within the school?	
Do you have contracts and data processing agreements in place for all suppliers who process personal data on behalf of the school?	

The Information Governance and Management Organisation (IGMO)

The handling of data in any organisation needs to be approached methodically, thoroughly and with due regard to the laws that govern its gathering, generation, storage, processing and disposal.

The GDPR alters the responsibilities for schools very sharply and the onus is now on schools to both identify and evidence their legal bases for processing personal data.

The data held by schools should be sufficient to allow routine contact with parents and to ensure the education, safety and welfare of the child within the school, whilst respecting and communicating their privacy rights

This guide, in each of the sections, aims to demonstrate a school's commitment to the key principles of GDPR: transparency, accountability and fair processing. The data processes that are recommended are designed to build an auditable process which demonstrates the integrity of a school and ensures transparency across the school community.

The key to successful adoption of the GDPR is a change in mindset of all individuals involved in data handling, management and governance in a school. There will need to be a culture change in how personal data is processed throughout the school, and certain activities that have to date been acceptable for example working from home will need to be more tightly regulated, secured and organised.

Handling the data in a school has a number of practical complications that make the need for a well-designed and administered **Information Governance and Management Organisation (IGMO)** a necessity to preserve confidentiality and maintain the school's reputation as an establishment worthy of the trust of pupils, parents, alumni and staff.

What should the IGMO be responsible for?

The following policies are considered to be part of the IGMO, and must be carefully revised to ensure they reflect the new responsibilities the school faces under GDPR:

- Privacy notice
- Data retention policy
- Data disposal policy
- Data sharing policy / agreements
- CCTV policy
- Taking, storing and using images of children policy
- Policy and procedures for Data Processors including contracts with suppliers
- Policy and procedures for Data Controllers
- Policy and procedures for training those involved in the IGMO
- Action in the event of an internal or external data breach
- Subject access requests

Data streams and data handling

A school deals with five main data streams, which are:

- Pupils
- Parents
- Governors
- Employees / volunteers
- Alumni / past parents

Each stream will have its own sensitivities, lawful bases for processing, and methods of processing, including for example the retention period or how data is disposed.

Mapping the data flow of each data set onto a timeline assists in identifying the points at which there should be contact between the school and the data subject, and the points at which policies dictate a potential change in the lawful basis for processing, the way personal data is processed, or in the rights of the individual.

Working through the data sets in each of the data streams will identify a number of contact points. Each contact point provides an opportunity to reinforce the messages of transparency and privacy that the new legislation requires.

Data Protection Officer (DPO), Chief Privacy Officer or data compliance lead

The GDPR introduces a duty for organisations to appoint a Data Protection Officer (DOP) if they are a public authority or carry out certain types of processing activities such as large-scale processing of special category data. Whilst schools may not be required to appoint a DPO, the school will require a Chief Privacy Officer or data compliance lead to oversee data protection compliance and help improve accountability.

For more information on the role of the DPO, visit https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/ and see ISBA's own guidance here: https://members.theisba.org.uk/53359

Data handlers (DHs)

Data handlers are staff (or volunteers) within the school who are responsible for processing personal data; this could be obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including:

- organisation, adaptation or alteration of the information or data
- retrieval, consultation or use of the data
- disclosure of the information or data by transmission, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction of the information or data

DHs are responsible for specific data sets within the above data streams. Within a school, the data sets and responsible DHs could be as follows:

- Joining, Progress and Departure data – DH should be the Registrar/School Secretary.
- Marketing and Communications – The DH should be the Marketing Assistant or in a small school the Marketing Officer.
- Medical data – DH should be the Registrar/School Secretary or, if the school is large enough the Matron.
- Development office or alumni information – DH should be the Development Officer.

- Education DHs should be each class, form and specialist teacher.
- Pastoral Information DHs should be form teachers, Heads of House and Deputy Head (Pastoral).
- Disciplinary Information DHs should be form teachers, Heads of House and Deputy Head.
- Incidents and Accidents DHs should be medical staff, form teachers, sports staff and Bursar.
- Safeguarding DH should be the DSL or as dictated by the circumstances.

Access to different data sets: Different data sets will be accessible to different members of school staff. There should be a discipline between DHs which ensures the sharing of personal data relating to a pupil or any other individual within a data set is done only on a need to know basis. Who should have access to specific data sets should be clearly identified in xxx policy and this will assist in preventing, or certainly reducing internal data breaches where information is shared inadvertently.

Staff training

Whilst all staff (and volunteers) will require a certain level of understanding of data protection principles and school policies and procedures around data protection, the distinct roles outlined above, the data compliance lead, be that the Data Protection Officer or the Chief Privacy Officer and Data Handlers (DHs) will require more specific training around their roles and responsibilities.

Staff regulation

A system of monitoring staff who have received data protection training similar to the annual child protection Staff Suitability Form would enable schools to review on an annual basis familiarity of all staff with data handling, processing and security.

Training and education of data handlers

Is the data compliance lead aware of their responsibilities?	
Has the data compliance lead received the necessary training before taking up their data compliance responsibilities?	
Have data handlers been identified for each of the data sets?	
Are each of the data handlers aware of their responsibilities?	
Are each of the data handlers trained before they take up their data handling responsibilities?	
Is data protection training for all staff refreshed at regular intervals?	
Are records of this training kept to demonstrate the school's commitment to data protection?	
Is "data processing" a topic in the induction training for all new members of staff at the school?	

Data streams: pupils and parents – an outline

When dealing with pupils, schools have to deal with two broad data sets. The first is generated by the child joining, progressing through, and departing from, the school. The second set is generated by the interaction between the child and the school, this will cover education, pastoral information, disciplinary information and any incidents or accidents the child is involved in.

Most, but not all of this information will be straightforward to deal with as category two data, however, there will be instances where category three data (sensitive data concerning health, medical conditions, family circumstances or some other factor) has to be processed. Both categories can be processed by the school using the lawful basis of the parent contract, as there is a contract/legal obligation in place between the parents and the school to process the personal data of the pupil.

As an overall data flow, the data relationship between the parents (and pupil) and the school could be as detailed below, the green shaded area denotes the parents and pupil as "prospective" and the gold shaded area where the pupil will have responsibility for his or her own data. The details of this change are unclear currently except that the age of roughly 13 is the point at which the relationship between school and parents alters.

DATA CONTROL - A TEMPLATE FOR SCHOOLS - EDUCATION BASIC DATA																				
	Pupil Status or progress	**Prospective**	**Prospective**	**Offered place**	**Accepted Place**	**Started in Nursery**	**Reception**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**	**Year 11**	**Year 12**	**Former Pupils**
	Originator of contact	Parents	School	School	Parents	School	School	School	School	School	School	School	School	School	School	School	School	School	School	Development Office
	Type of communication	Phone call or email from parents					Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Half yearly and annual reports, exam results	Email/Letter from Development Office
Data Held	**Basic contact details Child's DOB, name, sex and year group**	Requesting education reports medical conditions or SE Needs					Update / confirm information held is correct.	Update / confirm information held is correct.	Update / confirm information held is correct.	Update / confirm information held is correct.	Update / confirm information held is correct.	Update / confirm information held is correct.	Update / confirm information held is correct.	Update / confirm information held is correct.	Update / confirm information held is correct.	Update / confirm information held is correct.	Update / confirm information held is correct.	Update / confirm information held is correct.	Update / confirm information held is correct.	
	Seen by	Registrar/school sec, Head	Registrar/school sec, Head, class teacher, SEN teacher																	
Data Held	**Medical condition(s) SE Needs**				Data as above plus any medical conditions, Doctor's contact details and SE Needs			As above	As above	As above	As above	As above	As above	As above	As above	As above	As above	As above	As above	
	Seen by				Registrar/school sec, Head, Matron															
Data Held	**Emergency contact numbers, family members details**					Emergency contact numbers, names, email addresses and relationship to the pupil.		As above	As above	As above	As above	As above	As above	As above	As above	As above	As above	As above	As above	
	Seen by					Registrar/school sec, Head, class teacher, SEN teacher														
	Permissions from parent for the school to hold data	From parents to contact previous school			Medical details passed to catering company. Basic contact details included in Parent/teacher Association (if agreed with parents) which would be administered by the school.	Taking, storing and processing images of children; Privacy policy, data sharing agreement	Keep permissions up to date annually	Keep permissions up to date annually	Keep permissions up to date annually	Keep permissions up to date annually	Keep permissions up to date annually	Keep permissions up to date annually	Keep permissions up to date annually	Keep permissions up to date annually	Keep permissions up to date annually	Keep permissions up to date annually	Keep permissions up to date annually	Keep permissions up to date annually	Keep permissions up to date annually	Request permission to hold name address, phone number and email address on alumni data base.

It will sometimes be necessary to get separate consents for particular activities that the pupil and school undertakes. These will not simply be data protection consents, but may be parental consents to certain activities or treatments, or uses of the pupil's intellectual property (e.g. artworks). However, there may be a personal data element that needs to be captured.

These will include, but will not be limited to:

- Taking, using, storage and disposal of images;

  (this may be covered by legitimate interests, and for ordinary and less intrusive uses of images this may be a more pragmatic approach; but for other specific uses of images of an individual, for example in external marketing, it will be advisable – and indeed common sense – to seek consent for the parent or pupil, if not both)

- School trips and events; and

- Minibus use.

An additional complication is that school data will need to be transported from the school site with the pupils and staff who are participating in an event or outing. This may include special category data, such as dietary requirements, allergies or a medical condition. A policy will be need to regulate this, and it is suggested that the data is compiled to comply with the schools "Trips and Events" policy and returned to the school on completion of the activity.

As an audit, the following questions act as a check on compliance bearing in mind that the child's career through the school will generate data in four distinct but inter-related areas so the question should be answered with those headings in mind:

- Education Termly and annual reports will be generated as will data on test and exam results.
  Distribution of this data will change with the age of child within the school.
- Pastoral information Reports and contact with the pupils, parents or guardians will be raised from time to time.
- Disciplinary information Reports will be raised as required, contact with the parents or guardians may be required. Within the school, the senior management and house staff may need to be involved at different times during a child's career.
- Incidents and Accidents This is data that would be generated by an entry in the accident book, or for something more serious a Health and Safety RIDDOR report.

How is initial contact made with the school by prospective parents?	Website response, email, call or letter?
What is contained in the school's response concerning data protection and what form does the communication take? *Data protection information can be an explanatory "pop up" on the school website in response to a request for a prospectus, or a paragraph in an email or letter to the enquiring parent; but a link should be provided to the full Privacy Notice where possible.*	

Does the response contain an explanation of the data processes and privacy rules the school exercises? *Necessary to ensure transparency.*	
Has a pupil file been started? If so, have the parents been informed about the school's data storage, retention and disposal policy?	
With which other employees in the school is the data shared? *Who needs to know?*	
Is any of the pupil data classed as "special category"? *Medical or health issues, or family background?*	
If so, does the school's privacy notice detail how this is to be handled? And, have the parents been informed as to how the data will be handled?	
If the prospective parents do NOT enrol their child(ren) how is their data then handled? *The "legitimate interest" the school had while the parents were prospective has now altered. It may be there is a legitimate purpose to retain this information for longer – for example, if there are two ages at which pupils can enter the school or a space comes up – but there must be a documented rationale for why the "unrecruited" parent or pupil data is kept, and this should be transparent upon collection.*	
If the prospective parents do enrol their child(ren) how are they made aware of the school's policies relating to data protection and which consents (permissions) are they asked to give the school?	May include: • Taking and storing images of children • Biometrics • Trips and events out of school • Minibus travel
How often are these permissions refreshed with parents? *This can be annually. Or, once in a pupil's career. Whichever is the case the periodicity needs to be reflected in school policies.*	
How is the parental and pupil data stored? *Who has access, is it the minimum required, is it regularly reviewed as dictated by the retention policy?*	
Are pupils/parents made aware of which school publications or website areas may include their personal data? "*Taking, storing and using images of children" policy is relevant as is the consents the school*	

has for the use of images after a child has left the school.	
Are parents and pupils aware of how and where the school publishes exam results? *Firstly, to the pupils / parents; but also results are published as marketing material. Often anonymised BUT be clear with parents and older pupils if/how/when information will be used. Consent is recommended if published results are not anonymised.*	
Are the pupils and parents made aware of the archiving and disposal policies? *This needs to be in the parent contract and in the letter that accepts their son or daughter into the school.*	
Are parents made aware of the data handling within the school and (if applicable) the data processing conducted by contractors? *This needs to be in the parent contract and in the letter that accepts their son or daughter into the school.*	
Is the data shared with any other person or organisation, if so with who and why?	
Is data ever transferred outside the UK, by the school or its contractors? *Be aware of overseas school trips, and of parents hosting children in countries other than UK. This may be lawfully managed but requires care.*	
If providing data to a contractor working for the school (e.g. catering), has the school checked the contractor's privacy and processing policies? *This is necessary as the contractor needs to have a data regime that mirrors that of the school.*	
Have parents/pupils been informed that their data will be processed by these kinds of organisations? How? *This can be included in your school's privacy policy: you do not need to list exhaustively but an idea should be conveyed.*	
Has a privacy impact assessment been carried out for this data flow and its data acquisition, processing, storage and disposal?	

Statements for data collection forms (admissions)

Below are suggested statements to add to the different data collection forms that are used in admissions.

Enquiry form (e.g. prospectus enquiry form on the website and printed enquiry form to take out to feeder school events)

Option A:

I / We consent to XXXX School collecting, storing and processing the data provided on this form □

[THE CONSENT APPROACH IS NOT RECOMMENDED UNLESS LEGALLY REQUIRED, FOR EXAMPLE BECAUSE MEDICAL DATA IS INVOLVED]

I / We would like to receive emails and news bulletins from XXXX School □

Option B:

[PREFERRED IF POSSIBLE]

I / We understand that the personal data provided above will be processed for the legitimate business of XXXX School managing the admissions process. I / We understand that this information will be held until such time as the above-named child is no longer of an age to apply for a place at the School, or until I / we request that our personal data no longer be retained. □

I / We agree to you keeping in touch about admissions-related information (future deadlines and admissions events) and news about, and activities on offer from XXXX School. □

We will never sell your data and we promise to keep your details safe and secure.

You can change your mind at any time by emailing admissions@XXXXschool...

For further details on how your data is used and stored please visit: XXXX school website

Data Collection forms for new joiners and current pupils (e.g. general data collection form and health form)

Option A:

I / We consent to XXXX School collecting, storing and processing the data provided on this form for the time periods stipulated in the School's Privacy Policy. □

[THE CONSENT APPROACH IS NOT RECOMMENDED UNLESS LEGALLY REQUIRED, FOR EXAMPLE BECAUSE MEDICAL DATA IS INVOLVED]

For further details on how your data is used and stored please read XXXX School's Privacy Notice *[link if digital form or otherwise provide]*

Option B:

[PREFERRED IF POSSIBLE]

I / We understand that the personal data provided above will be processed for the purposes set out in XXXX School's Privacy Notice [*link if digital form or otherwise provide*]

For the purposes of data protection law, XXXX School is the data controller for any personal data you supply to us. This personal data will be processed in accordance with data protection law, only used for the purpose(s) for which you have supplied it to us and our Privacy Notice, and (except where you have consented) only shared with third parties where it is necessary for us to do so and the law allows it. If we share your personal information with another organisation (e.g. another school, ISI, DfE or another government department etc.) this will be to help us act upon what you have told us or because these organisations need to be made aware of what you are telling us (in order for them to act upon it).

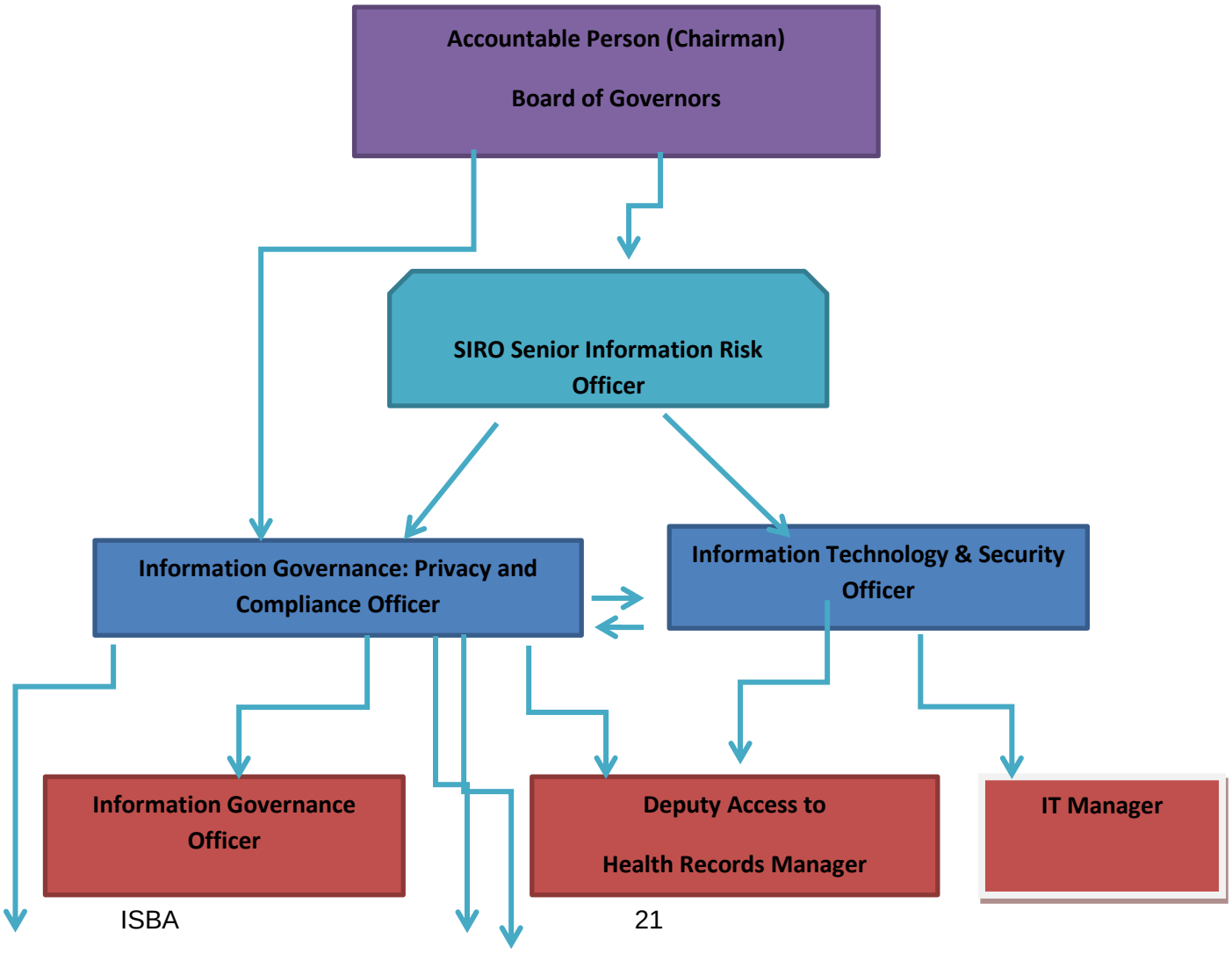
Please let us know if you do not wish us to share your information with relevant organisations but also be aware that we might not be able to act upon your correspondence if we do not share it. It is also important to note that, in certain circumstances, we might have a legal obligation to share the information that you have supplied to us with other organisations.

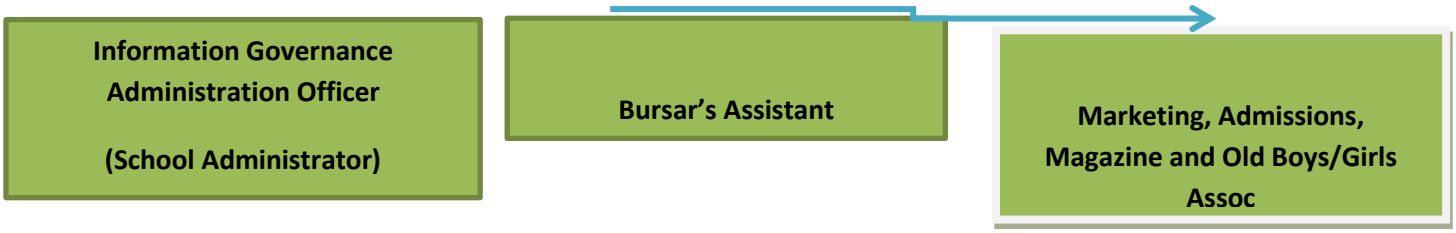
Information Governance Management Organisation Framework

xxxxxx School

Responsibility for Information Governance rests with the most senior level of accountability, specifically the Board, however, support is provided through a robust framework for managing Information Governance that extends throughout the Informatics Department and reflects the various responsibilities of Information Governance.

The attached document reflects the current IGMO structure.





Robust Information Governance requires clear and effective management accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

Roles		
Role	Filled By	Details
Accountable Officer	Chairman	Overall responsibility for all aspects of Information Governance
Information Governance Lead	Information Governance Privacy and Compliance Officer	Responsibility for assessing, monitoring and reporting compliance with, and emerging issues in, Information Governance
Senior Information Risk Owner (SIRO)	Chief Information Officer	Implement and lead the Information Governance risk assessment and management process
Information Security	Information Governance Privacy and Compliance Officer IT Information Security Officer	Responsibility for ensuring compliance with Information Security Standards
Information Governance Incident Management	Senior Information Risk Owner (SIRO) Information Governance Privacy	Responsibility for the incident management process/chairing incident panels/ investigations and investigation subject matter expertise

	and Compliance Officer IT Information Security Officer Information Governance	
Data Protection and Freedom of Information Lead	Information Governance Privacy and Compliance Officer	Responsibility to assessing and monitoring compliance with Data Protection and Freedom of Information legislative requirements
Subject Access Request Management	Information Governance Privacy and Compliance Officer	Advise and manage the provision of the Trust Subject Access Request function and demonstrate compliance with IGT v15 factor 205

Information Governance Meeting Structure

The Information Governance committee will be made up of the following members

Headmaster
Senior Information Risk Officer
Bursar
Responsible Governor

The committee will meet once per term and the minutes will be circulated to all governors prior to the termly governors' meeting for further consideration.

A GDPR Risk Register will be maintained keeping a record of any Data Protection breaches that come to light and how they have been resolved. The Risk Register will be inspected by the chairman and the responsible governor annually.

Data streams: employees – an outline

With employees, records are required to be kept of applications, the interview, reference and clearance process before an employee starts with the school. It should be noted that volunteers should also be included in this process as far as school policies dictate. Once employed, an employee's career path into, through and on departure from the school needs to be recorded, including annual appraisals, changes in terms and, if applicable, disciplinary procedures.

- Recruitment Full records are required of the advertising, selection and clearance processes.
- Contract / Terms & Conditions This will include bank and payment details.
- Medical Info Records are required including emergency contact details, as well as any reasonable adjustments made to accommodate the employee.
- Training Termly and annual reports will be required.
- Pastoral information Reports will be raised from time to time such as annual appraisals or supervisions
- Disciplinary information Reports will be raised as required.
- Incidents and Accidents This is data that would be generated by an entry in the accident book, or for something more serious a Health and Safety RIDDOR report.

Overleaf is a reminder of a typical data flow for employee information will be handled by the school.

DATA CONTROL - A TEMPLATE FOR SCHOOLS - EMPLOYEE DATA								
	Status or progress	**Prospective Employee**	**Interviewee**	**Offered post**	**Accepted post**	**Started employment**	**Annual Appraisal**	**Former employee**
	Originator of contact	Prospective Employee	School	School	Employee	School	School	School
	Type of communication	Application form and CV		Offer letter	Employment contract		Annual Appraisal	
Data Held	**Basic contact details, name, sex and post applied for.**						Update / confirm information held is correct.	
	Seen by	Head, Bursar, HR Head and HR Admin	Head, Bursar, HR Head and HR Admin and interview panel		Head, Bursar, HR Head and HR Admin		Head, Bursar, Line Manager	
Data Held	**Medical condition(s) any pastoral needs**				Data as above plus any medical conditions, Doctor's contact details and SE Needs			
	Seen by	Head, Bursar, HR Head and HR Admin			Registrar/school sec, Head, Matron			
Data Held	**Emergency contact numbers, family members details**					Emergency contact numbers, names, email addresses and relationship to the rmployee		
	Seen by			Head, Bursar, HR Head and HR Admin		Head, Bursar, HR Head and HR Admin		
Data Held	**Detail of incidents and accidents**				Accident book entries or RIDDOR events throughout employment			
	Seen by				Head, Bursar, HR Head, Line manager as appropriate.			
Data Held	**Detail of training**				Record what and when and to what level in employee file		Record what and when and to what level in employee file	
	Seen by				Line Manager, HR manager		Line Manager, HR manager	
	Permissions from employee for the school to hold data	Gain permission		Update permission	Keep permissions up to date annually		Keep permissions up to date annually	Retain records, inform employee that this is the case IICSA is the overriding reason.

How is initial contact made with the school by prospective employees? Does the advert give any data handling information?	
What is contained in the response concerning data and what form does the communication take?	
Does the response contain an explanation of the data processes and privacy rules the school exercises?	
Has an employee file been started?	
With which other existing employees in the school is the prospective employee's data shared?	
Is any of the prospective employee data classed as "special category"?	
If so, does the school's privacy notice detail how this is to be handled?	
If the candidate is NOT employed how is their data handled? *Consent will be required to retain the data from the "unrecruited" candidate.*	
If the candidate is employed, how are they made aware of the school's data protection policies and which permissions are they asked to give the school concerning the processing, storage, archiving and disposal of their data?	
How often are these permissions refreshed with employees?	
How is the employee data stored?	
Are employees made aware of where their data is held within the school?	
Is employee data shared with anyone outside of the HR function, if so with who and why?	
Is data ever transferred outside the UK, by the school or its contractors? *Be aware of staff accompanying overseas school trips*	
If sharing is with a contractor working for the school, has the school checked the contractor's privacy and processing policies?	
Have employees been informed that their data will be shared with these other organisations? How?	
Has a privacy impact assessment been carried out for this area of data acquisition, processing, storage and disposal?	

Data streams: Governors – an outline

Governance The processes of governance require records: these are straight-forward and the storage, retention and accessibility regulations have not changed. However, best practice is likely to emerge under GDPR whereby governors will be expected to carry out official school business on secure school systems, including school email accounts. If this is not yet practicable, governors should be aware of applicable policies around confidentiality and security of data handling, including the security of personal devices.

Should there be the need to make an enforced change to the composition of the governing body, the records surrounding that (a governor becoming unfit to hold office as an example) then this data will need to be treated in the same way as the most sensitive HR records.

Every piece of information requested, generated, stored, transmitted and disposed of has to be done under the firm direction of a data policy for the particular activity.

Governance records This area is included for completeness. The record will include but not be limited to:

- The Memorandum and Articles and changes to them.
- The Scheme of Governance plus any changes.
- The annual accounts.
- The confirmation reports to Companies House.
- The annual reports to the Charities Commission.
- The report accompanying the annual accounts.
- The annual public benefit statement.

DATA CONTROL - A TEMPLATE FOR SCHOOLS - GOVERNANCE DATA BOARD MEMBERS						
	Governance	Prospective Governor	Offered place	Accepted Place	Appointed	Former Governors
	Originator of contact	Prospective Governor	School	Parents	School	Development Office
	Type of communication	Phone call or email from Chairman				Email/Letter from Development Office
Data Held	Basic contact details for each member of the Board, name, contact details, DOB.					
	Seen by	Clerk and Chairman				
Data Held	Medical condition(s)			Only if relevant		
	Seen by			Clerk, Chairman and Head		
Data Held	Emergency contact numbers, family members details			Emergency contact numbers, names, email addresses and relationship to Governor.		
	Seen by			Clerk, Chairman and Head		
	Permissions from Board Member for the school to hold data					Request permission to hold name address, phone number and email address on alumni data base.

DATA CONTROL - A TEMPLATE FOR SCHOOLS - GOVERNANCE DATA			
Data Held	Board Papers	Termly	Retained until?
	Seen By	Board members, Clerk and Head	Ad infinitum
Data Held	Annual report and Accounts	Annually	Retained until?
	Seen by	Board members, Clerk and Head	Seven years, in reality longer.

Data shared with, and held by, Governors

How is initial contact made by the school with prospective governors?	
Are governors required to use secure school systems for school business?	
If not, what policies are they subject to in order to maintain security and confidentiality?	
Are they aware that, if used for official school business and likely to contain relevant personal data, their personal accounts or devices may be searchable under a SAR since they are in effect in control of the school?	
What is contained in the communication concerning data and what form does the communication take? Does each Governor have his/her own school email address?	
Does the communication contain an explanation of the data processes and privacy rules the school exercises?	
Is a file started in which the governor's data is stored?	
With which other existing employees in the school is the data belonging to the governor shared?	
Is any of the governor's data classed as "special category"?	
If so, does the school's privacy notice detail how this is to be handled?	
If the governor is not recruited and does not wish to be contacted further how is their data handled?	
If the governor is recruited how are they made aware of the school's policies and which permissions are they asked to give the school concerning the processing, storage, archiving and disposal of their data?	
How often are these permissions refreshed with the Governors?	
How is the governor's data stored?	
Are governors made aware of where their data is held within the school?	
Is the data shared, if so with whom?	
Is data ever transferred outside the UK, by the school or its contractors?	

If sharing is with a contractor working for the school, has the school checked the contractor's privacy and processing policies?	
Are the governors made aware of the other organisations with whom data is shared?	
Has a privacy impact assessment been carried out for this area of data acquisition, processing, storage and disposal?	In particular, how is information sent to governors? Is the school sending data to governors' private e mail addresses?

Data streams: alumni and past parents – an outline

How is initial contact made by the school with alumni?	
What is contained in the communication concerning data and what form does the communication take?	
Does the communication contain an explanation of the data processes and privacy rules the school exercises?	
Is a file started in which the alum's data is stored?	
With which other existing employees in the school is the data belonging to the alumni shared?	
Is any of the alumni data classed as "special category"?	
If so, does the school's privacy notice detail how this is to be handled?	
If the alum does not wish to be contacted further how is their data handled?	
If the alum is willing to be contacted regularly how are they made aware of the school's policies and which permissions are they asked to give the school concerning the processing, storage, archiving and disposal of their data?	
How often are these permissions refreshed with the alumni?	
How is the alumni data stored?	
Are alumni made aware of where their data is held within the school?	

Is the data shared, if so with whom and are alumni aware of who their data is shared with	
If data is shared with an alumni association/society, foundation or PTA, have you identified who is the data controller?	
If data is shared with another school organisation, is this clearly detailed in the school's privacy notice and a data sharing agreement in place?	
Is data ever transferred outside the UK, by the school or its supplier?	
If a supplier working for the school is provided with personal data, has the school checked the supplier's privacy and processing policies and a data processing agreement put in place?	
Has a privacy impact assessment been carried out for this area of data acquisition, processing, storage and disposal? In particular around sharing data with PTAs, Old Pupil Associations and/or Foundations, and/or around particularly intrusive processing of personal data such as wealth screening.	

Alumni relations and schools' development

If you are working in alumni relations or schools' development, it is highly likely you will be processing personal data of alumni and past parents, and potentially current pupils, parents and staff as well. This could be through storing personal data, sending regular newsletters or invitations to events, processing donations or using publicly available information to research and contact alumni. This (and more) all counts as processing personal data.

Under GDPR, the data controller – be that the school or alumni association/society or both (independently or jointly) – must identify the purpose and lawful basis (or bases) for processing this personal data, document this and share this regularly, to ensure you are respecting the privacy rights of individuals' from your school community.

Please note throughout this section we will refer to 'alumni', however this section relates to all individuals you are engaging with from an alumni relations or development perspective, which could also include past parents, current parents, pupils staff, organisations such as corporates and trusts, and the wider community.

1. **Why is 'direct marketing' important under GDPR?**

   Within alumni relations and schools' development, much of the processing of personal data is for direct marketing purposes. The ICO's definition of direct marketing includes the promotion of an organisation's aims and ideals, as well as the sale of products and services, such as alumni engagement or fundraising. It applies not only to commercial organisations but also not-for-profit organisations such as charities and schools. Advertising or marketing material could include school newsletters, fundraising appeals or campaigning materials.

   You will need to consider what the purpose of your communication is: if it is to promote the aims and ideals of the school and is directed at a specific individual, then this will be classed as direct marketing. Under GDPR, if your school is carrying out direct marketing, you will need: (i) a lawful basis for processing this personal data; and (ii) to comply with PECR. For further information, visit https://ico.org.uk/media/1555/direct-marketing-guidance.pdf

2. **What is PECR and why is it important when talking about GDPR?**

   PECR or the Privacy Electronic Communications Regulations, sits alongside GDPR to give individuals specific privacy rights in relation to electronic communications, including marketing calls, e-mails, texts and faxes. Under PECR, you need to have consent to send direct marketing via electronic communications such as:

   (i) to personal email addresses (but not to "corporate" email addresses – e.g. @company.com, @university.org etc.),
   (ii) by SMS; or
   (iii) to TPS-registered telephone numbers.

   PECR is not new: it has been in existence since 2003. It will remain unchanged under GDPR (although it will be replaced in the future, possibly 2020, by a new e-Privacy Regulation which may do away with the personal / corporate email distinction).

   However, what is new under GDPR is that a higher standard of consent is required: a freely given, specific, informed and unambiguous indication of an individual's wishes (see question 3). Therefore as a minimum, to comply with both PECR and GDPR, it is likely your school will need to **review and in some cases renew its consents** for e-communications. However, schools should **be VERY careful** in this process not to overstate what it needs consent for: for example, postal or (in some cases) telephone marketing can still be carried out under legitimate interests, and so this should be

distinguished in the wording; and administrative "membership" type emails may still be necessary and lawful to send.

Schools must understand that there is a spectrum of risk here in both directions, given strict ICO Guidance about what is "marketing" and low take-up of opt-in.

3. What lawful bases can development and alumni relations' professionals use to process personal data?

Under GDPR there are six lawful bases for processing personal data (see the introduction to this guide). The two most relevant to development and alumni relations are **'consent'** and **'legitimate interest'**, although if your alumni organisation is predicated on membership terms or a fee then there may be arguments to be made under **'contract'** (i.e. that certain communications – member admin, but potentially also invitations to events, magazines and newsletters – are expected member benefits). The latter will not always be straightforward to make out.

CONSENT

4. What is consent?

Under GDPR, consent must be **a freely given, specific, informed and unambiguous indication** of the individual's wishes. GDPR sets a **higher standard** for consent, it means offering individuals a **genuine choice** and you can no longer rely on pre-ticked boxes.

If relying on consent, there are different ways alumni can give their consent, through ticking an 'opt-in' box on a website, completing a form at an alumni event or through a verbal confirmation. Whichever way an alumnus gives their consent, it must be clear what they are consenting to. Likewise, a **record of the consent must be retained**: what they were told, when and how they agreed. Consent cannot be a condition of a service or be bundled up with terms and conditions – therefore from a school perspective **consent cannot be part of a parent contract**. It is perhaps more credible to gather consent as part of "membership terms" of an alumni organisation on leaving the school, because of the more narrow purposes and expectations of what one is signing up to in this way.

Consent can also not be assumed: for example, through the act of giving a donation. There is some scope to assume that someone who has bought a ticket for an event may wish to hear about similar events going forward, but generally this rule (called the "soft opt-in" rule) does not assist in a development context because it requires a sale. Donating or merely keeping in touch does not trigger this rule.

If relying on consent, individuals have certain rights under the GDPR, including the right to withdraw consent at any time; the right to object to direct marketing; the right to erasure when consent has been withdrawn, if consent was what you were relying on to hold their data (but you may need to keep "suppression data" in some cases); the right to restrict how their data is processed; the right to rectification (that their personal data is kept accurate and up-to-date) and the right to access (to request to see what personal data your school holds on them). For further information, visit https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

5. Does consent need to be granular?

In the Guidelines on Consent produced by the Article 29 Working Party and adopted by the ICO, it states that **an individual should have the opportunity to consent**

separately to the different purposes of processing rather than having to consent to a bundle of processing purposes. Therefore, if relying on consent, you will need to consider the different activities your school carries out, the different purposes for processing personal data and if necessary separate out these purposes to obtain consent for each.

For example, you could request consent to send direct marketing e-mails. However, you could not rely on the same consent to then carry out wealth screening via a third-party organisation unless that was clearly and separately indicated. As you are processing personal data for a different purpose, a separate consent would be required; or you might consider a legitimate argument applied to this secondary activity, but that would still have to be transparent (and subject to its own risk assessment).

In conclusion: you cannot say that a "consent" is relevant unless it is specific to the activity and, generally, the medium of contact too (email, telephone or post).

6. What information should you include when capturing consent?

Under the GDPR, one of the conditions of consent is that it is **'informed'**. Therefore, according to the Guidelines on Consent, the following information is required for obtaining a valid consent:
- the data controller's identity or identities, i.e. if both the school and an alumni association/society are data controllers then both must be named;
- what data will be collected/processed; and
- for what purpose, i.e. the processing purpose(s) for which consent is sought (i.e. direct marketing, sharing data with a third party, wealth screening/profiling).

More generally, this needs to be supported by the Privacy Notice, which have must been provided to the individual and will include:
- how can an individual withdraw consent;
- if relevant, the use of data for automated decision-making;
- whether data will be transferred outside of the EEA and what lawful safeguards are in place.

Please note that data processors do not need to be named as part of the consent requirements. However, as transparency is one of the fundamental principles of GDPR, you will still need to share with alumni a list of data processors or categories of data processors, i.e. mail-houses, within your privacy notice.

7. How long does consent last?

GDPR **does not set out any specific time limit on how long consent lasts**: it will depend on what your purpose is for processing personal data, what is reasonably necessary for that purpose, and what you have told individuals in terms of why and how long you will be processing this for.

However, **acquiring consent is not a one-off process** and it does **not last indefinitely**. When acquiring consent from alumni, you will need to clearly state why you are processing their personal data, and how you will use their data. When your purposes for using the personal data are no longer relevant or change, you will either need to delete the data or seek new consent. You will also need to provide alumni with the opportunity to withdraw their consent at any time.

Whilst within the charitable sector there has been a suggestion that consent be reviewed every 24 months, within the context of alumni – where there is likely to be less regular communication but a stronger foundation of relationship – it may be inappropriate to renew consent so frequently. You may decide to renew consent

based on the life-stages of alumni: for example if you organise alumni reunions every ten years, then would this be a good opportunity to renew consent? It is worth asking your alumni what they deem to be a reasonable length of time before renewing consent?
The Guidelines on Consent produced by the Article 29 Working Party recommends that consent is refreshed at appropriate intervals and to comply the GDPR principle of accountability, you document your decision and your reasoning around renewal of consent.

Please bear in mind that there may be other reasons, separate to consent, why you need to keep hold of alumni data: archiving; statistics; legacies; evidence for historic claims; and suppression files (i.e. "do not contact" records). These may not be relevant to development activity, but it should be remembered that a "right to be forgotten" request, expiry or withdrawal of consent, or objection to marketing may not have absolute effect.

8. Can pupils provide consent or should we ask their parents?

The GDPR itself does not specify an age limit for valid consent (the age of 13 cited in some quarters is of specific and limited application).

In the context of development and alumni relations, a natural opportunity to obtain consent – regardless of any "consent" supposedly given by the parent under the parent contract, for example – will be as the pupil leaves the school.

A separate example of when consent would be required might be the use of photographs of pupils for direct marketing purposes: from secondary school age, this is likely to be the pupil's consent you need. In order to gain 'informed consent' from a child, you need to explain clearly how you intend to process their personal data (in this instance how you intend to use their photograph – this should not just include what photo and where it will be used, but also detail such as how long the photo will be used and whether it will be practicable to remove the photo once used (e.g. in a printed publication). This is in order for consent to be truly "informed".

Many schools use leaver forms to gather personal information about pupils before they finish school, and these often seek consent to ongoing communication with pupils once they have left. However it is worth bearing in mind that alongside capturing the pupil's consent, if you are looking to continue to communicate with the parent(s), you will need to consider the lawful basis for processing their personal data moving forward too, and whether their consent is also needed.

9. How should we record consent?

Under the GDPR, there is **an explicit obligation for the data controller to demonstrate an individual has given consent.**

You can develop a method of recording consent that works for your school and this will often be determined by your database provider. However, it is worth noting that in demonstrating consent you should not be collecting any more information than is necessary nor should this information be kept for any longer than is necessary. For example, you may keep a copy of a consent statement, with details of when consent was obtained and the information that was provided, but you would not need to keep copies of every signed consent statement if these are recorded on your database.

Verbal consent is valid under GDPR: but as with written consent, it is necessary to evidence what information was provided when the consent was requested. For example, you could develop a standard verbal consent to share with alumni when they contact you by phone or you meet face to face. You would then need to

reference this standard verbal consent and when this was given against the individual's record in your database.

10. We already have consent in place, do we need to renew our consent?

It will depend on whether your consent complies with the standards as set out under GDPR, i.e. consent must be freely given, specific, informed and unambiguous indication of the individual's wishes.

You are not required to automatically refresh all existing consents in preparation for the GDPR, but it is important to check your processes and records in detail to be sure existing consents meet the GDPR's higher standard. For example, if you do not have a record of an alumnus' consent, then this is presumed consent: under GDPR this is not a valid consent**. Likewise, if your consent relies on an opt-out or pre-ticked opt-in box, this does not meet the GDPR standard of genuine choice. It is likely therefore that where relying on consent, you will need to renew your consents to comply with GDPR**. For further information, visit https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf

11. Can an alumnus withdraw consent?

Yes. Under GDPR, the privacy rights of the individual have been strengthened. **An alumnus has the right to withdraw consent at any time** and also has **the right to object to direct marketing** (which includes fundraising), even if you are relying on legitimate interests (see below). You must have a process in place for handling withdrawal of consent. You can use a suppression list where you store personal data on alumni who have withdrawn their consent: however you must only retain the minimum amount of personal data to identify the alumnus.

LEGITIMATE INTERESTS

12. What is legitimate interests?

Legitimate interests is the most flexible lawful basis for processing personal data and is likely to be most appropriate where you are using personal data in ways that individuals would reasonably expect and where there is a minimal impact on their privacy.

Whereas consent requires an individual to provide an affirmative consent that they want to receive direct marketing from your school, legitimate interests allows a school to consider its own legitimate interests, for example to promote its aims and ideals, and to balance this against the individual's privacy rights – provided that it notifies the individual and gives them the chance to object.

Essentially you can send direct marketing (via certain methods of communication) as long as an individual has not said 'no'. However:

(i) it does not circumnavigate the PECR requirement for consent for electronic communications (subject to the above); and

(ii) under GDPR the principles of transparency and accountability still apply.

Therefore, whilst a definitive 'yes' is not needed when relying on legitimate interests, your alumni must be made aware of and understand why and how the school intends to process their personal data – this can be achieved through regularly sharing a detailed privacy notice with your alumni community (see questions 20630).

It may well be that more than one organisation has a legitimate interest to process personal data, for example an alumni association/society and a school may have a legitimate interest to process the personal data of their alumni. **A legitimate interest can apply to more than one organisation** (e.g. an alumni organisation): however again it will be important to make this clear in your school's privacy notice.

You will also need to provide alumni with the opportunity to essentially 'opt-out'. **If relying on legitimate interests, under the GDPR there is an obligation to tell individuals about their right to object**, ideally at the point of data collection or subsequently in your privacy notice. You must also have a clear process to respond to an individual who does object – current practice is to hold a suppression list and this would be acceptable under GDPR, however you must only retain minimal data to ensure you can respect the alumnus' decision to 'opt-out'.

13. What might be a legitimate interest in the context of alumni and schools' development?

GDPR makes it clear that the purpose of 'direct marketing' is a legitimate interest. However, it is possible to rely on other legitimate interests such as a **'relevant and appropriate relationship'** with the school or a **'reasonable expectation'**.

For example, it is likely your alumni, given their pre-existing relationship with the school, will expect the school to process their personal data to keep in touch with them, their 'relevant and appropriate relationship' with the school means this processing is less likely to be unexpected or unwanted. Equally, if alumni are members of an alumni association/society, the legitimate interest might be that there is a 'reasonable expectation' as a member of this association/society that the alumni association/society and the school (depending on who is/are the data controller(s)), will process their personal data.

It is likely that, provided it limits the activity to permitted marketing methods (postal, non-TPS telephone lines, business or university emails) most schools will be able to build a legitimate interests argument for most ex-pupils and ex-parents in most cases. But whatever the purpose for processing personal data, you will still need to carry out a Legitimate Interest Assessment to demonstrate you have balanced your school's legitimate interests against the privacy rights of your alumni.

14. What is the Legitimate Interest Assessment

A school may choose to rely on legitimate interests to process personal data for direct marketing/development purposes, if they feel that they are processing alumni's personal data in ways they would reasonably expect, which has a minimal impact on their privacy, or where there is a compelling justification for the processing. The ICO have suggested a three-part test, the Legitimate Interest Assessment or LIA to assess whether legitimate interest is the appropriate lawful basis:

- **Purpose test** – what is your school's legitimate interest for processing personal data?
- **Necessity test** – is the processing necessary for this purpose?
- **Balancing test** – do the individual's interests override the school's legitimate interest?

Within the context of alumni relations and development, the legitimate interest for processing alumni's personal data could be:

- **direct marketing** – which is specifically mentioned as a potential legitimate interest under the GDPR, i.e. promoting the school and its activities through regular communications with alumni

- **reasonable expectations** - as members of an alumni society/association there is a reasonable expectation their personal data will be processed
- **relevant and appropriate relationship** – as an ex-pupil, there is a pre-existing relationship with the school and therefore processing of an alumnus' personal data would not be unexpected or unwanted
- **to seek support for a fundraising campaign** – for example, a school cannot afford to fund bursary places unless it raises money therefore it has a legitimate interest or 'purpose' for processing personal data
- **prospect research to support a fundraising campaign** – for example, a school is running a capital campaign and it wants to use prospect research to identify potential major donors who have the capacity to make substantial donations and support this fundraising campaign

The school would then need to determine whether it was necessary to process the alumni's personal data for this purpose – what difference will this activity make to the pupils/school? What is the impact on the school of not carrying out this activity? The school would then need to consider the balancing test is this action particularly intrusive.

For example:

- a school seeking support for a fundraising campaign could decide to send a postal mailing requesting support.

- the school would need to consider whether it was necessary to contact alumni to achieve their purpose, and then balance this purpose against the rights of their alumni. Would their alumni expect to be contacted in this way?

- If the mailing only requires the processing of the names and addresses of alumni already on the school's database, it might consider this a proportionate way of approaching alumni for donations.

- Likewise, if a privacy notice has been shared with alumni which details why and how the school processes their personal data, and alumni have received previous such mailings, it would be reasonable for them to expect future mailings if they have not opted out.

For further information, visit https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

Whilst schools generally only contact individuals who have some sort of existing relationship with the school; alumni, past parents, etc, and therefore there is potentially a legitimate interest to contact them because of their 'relevant and appropriate relationship' with the school, the GDPR principles of transparency and accountability still apply. When carrying out your LIA, you must still consider whether alumni know why and how you are processing their personal data, and you must demonstrate that you have looked at all the relevant factors. For example, if your school has never sent a fundraising ask to alumni and you have not detailed that this is one of the purposes for processing alumni's personal data in your privacy policy, whilst your school may well have a legitimate interest to request support from alumni, and it may be necessary for the school to carry out this fundraising, you will still need to evidence that you have considered the privacy rights of the individuals in question, the balancing exercise to ensure your 'fundraising ask' is not unexpected or intrusive.

Schools can consider gathering evidence which will help them to demonstrate how the legitimate interest test can be satisfied. For example, donor feedback (through surveys, focus groups or informally), the number of complaints, donation histories, etc

can all be used to show whether alumni's individual privacy rights have been considered.

15. Do we need to include an 'opt out' if relying on legitimate interests?

Yes. Having carried out the legitimate interest assessment, you may decide that you have a legitimate interest to process alumni's personal data for direct marketing purposes, but **the individual still has the choice to say 'no' to direct marketing** and you will need to make it clear how they can 'opt out' of further communications.

Under GDPR, an individual has the right to object to processing of their personal data for various reasons, notably marketing. This overrides the school's legitimate interest to send them future communications.

16. How long can we rely on legitimate interest to communicate with our school community?

Whilst again there is **no specific time limit on using legitimate interest** as a lawful basis for processing the personal data of your alumni, age (including the frequency or recency of contact or response from the individual) will form part of the balancing test. You will need to continue to review:

- your purpose for processing personal data
- whether legitimate interest remains the most appropriate lawful basis for this processing
- whether processing this personal data is still necessary
- whether there is reason to think that the individual's wishes or expectations have changed

Through regularly reviewing the lawful basis for processing your alumni's personal data, you will demonstrate your commitment to the key principles of GDPR: transparency, accountability and fair processing.

17. How do we know what constitutes an individual's 'reasonable expectations'?

This is a good question. What constitutes reasonable expectations for one alumnus might be quite different to those of another. The key thing to remember is the principles of transparency and accountability under GDPR. If you are transparent with your alumni, for example you tell them you will be contacting them with donation requests within your privacy policy and you share this on a regular basis with them, then you have demonstrated consideration for your alumni's privacy rights. Other ways of minimising risk here and demonstrating you have considered their rights, might be to hold a focus group of alumni or to include in an alumni satisfaction survey and document what they consider to be reasonable expectations, or to develop a policy around direct marketing that says for example, you will only contact 'lapsed' alumni every ten years to ask them if they want to re-engage with your school. If you make this clear in your privacy notice and share this with alumni, then you are demonstrating both transparency and accountability.

18. What safeguards can we put in place when relying on legitimate interests to minimise the risk to alumni's privacy?

If relying upon legitimate interests, in order to demonstrate your consideration of an individual's privacy rights, it is important to **put certain safeguards in place to evidence your 'balancing test'**.

For example, if relying on legitimate interests to profile potential major donors, safeguards could be put into place to minimise data collection, to limit the use of publicly available material, to restrict sharing of this data, to identify strict retention periods for this data, and to ensure the individual is provided with a copy of your

school's privacy notice (which clearly details how their data has been processed and why) at the first point of contact and how they can object to processing of their personal data. The safeguards you put in place, will depend upon the purpose for processing. If there is a higher risk to an individual's privacy rights or the processing is new, a DPIA (see question 43) is a good way of demonstrating that you have considered and minimised these risks.

LEGITIMATE INTERESTS Vs CONSENT

19. Is there a 'right' lawful basis for processing personal data for alumni relations/schools' development?

There is **no 'single' or 'right' lawful basis for processing personal data** for alumni relations/schools' development. Each school's relationship with their community will be slightly different and therefore your school will need to choose the most appropriate lawful basis for your circumstances. Whichever lawful basis your school intends to rely on, you must determine this before you begin processing personal data and you must include this in your privacy notice.

20. Can we use both legitimate interests and consent or do we have to stick to one lawful basis?

Yes, both are valid lawful bases for direct marketing (subject to PECR). You might decide that you want to move towards consent for specific groups of individuals, for example school leavers, however there may be other groups of alumni where you want to rely on legitimate interests, for example where you have a longstanding relationship with alumni or previous donors. You also may want to use different lawful bases depending on the type of communication you are using (see question 23)

Whichever lawful basis or bases you choose, it is important to get it right, you should not swap to a different lawful basis at a later date without good reason (see question 24). You must determine your lawful basis before you begin processing personal data and include this in your privacy notice, and if using both lawful bases, ensure you have a system to administer this properly.

21. Can we always rely on consent as the lawful basis for processing alumni's personal data?

It is worth bearing in mind that there may be occasions where you cannot rely on consent. For example, you may need to rely on legitimate interests if identifying alumni who are currently not on your school database.

22. Can we always rely on legitimate interests as the lawful basis for processing alumni's personal data?

No. If you are contacting alumni by a personal e-mail address, SMS or using automated telephone calls or a TPS-registered telephone number, you will also need to comply with the Privacy and Electronic Communications Regulations or PECR.

Under PECR, you need to gain consent to send direct marketing via electronic communications such as e-mail, SMS or TPS-registered telephone numbers. With TPS, it is important to note that it is the number and not the individual which is registered with the TPS. As such an alumnus might provide you with multiple telephone numbers, one of which is registered with the TPS, however it may still be possible to use one of the alternative numbers to contact them.

23. What bases can we use for each type of communication?

You can carry out direct marketing to an alumnus:

By post/to a business email address/live telephone call (not registered with the TPS) if an alumnus has given you their affirmative consent or you can demonstrate a legitimate interest (and the alumnus has not objected to receiving direct marketing materials)

By e-mail, text, automated telephone call or live telephone call (to a TPS-registered phone number) if an alumnus has given you their affirmative consent.

(Again it is worth noting the point above, that it is the phone number that is registered with the TPS and not the individual, so an alumnus may have provided you with alternative numbers that you could use if wanting to rely on legitimate interests to process personal data).

24. If we ask for consent and we do not receive a response, can we then rely on legitimate interests?

Unlikely: this is why it is a risk to rush in to an "all opt in" approach. **If you ask an alumnus for their consent and they do not reply, then you do not have their consent to contact them.** It would be difficult to then justify changing your lawful basis for processing personal data to legitimate interests. How would you evidence that you have a legitimate interest to communicate with them if they have not responded to your request for consent?

25. If a school asks an alumnus for their communication preferences, and an alumnus does not tick to say they are happy to receive postal mailings, can you still use legitimate interest to communicate by post with the alumnus?

To use legitimate interest as the basis for processing personal data, you will need to consider the Legitimate Interest Assessment (see question 14). Whilst in this example, it may still be possible to justify a legitimate interest for the school to contact the alumnus and even demonstrate that their processing is necessary, if an alumnus has clearly stated their preference not to receive communication by post, then to send them postal mailings would be acting against the individual's express interests and his or her right to object to direct marketing.

26. What is the 'soft opt-in' and does it apply to schools?

The 'soft opt-in' offers the opportunity to market similar products to existing customers who have not opted out of marketing messages. However, the 'soft-opt in' does not apply to fundraising so schools can only use this in very limited sales contexts – and never for fundraising. For further information, visit https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/

PRIVACY NOTICES

27. What are privacy notices?

Privacy notices (previously often described as "Privacy Policies", "Data Protection Policies" or "Fair Processing Notices") inform individuals about who you are, why and how you will process personal data and who this data will be shared with. All schools should have a clear and accessible privacy notice. For further information about what must be included in your privacy notice, see the 'Draft Privacy Notices' section of this guide for a template privacy notice for schools or visit https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

28. Do we need a separate privacy notice for processing personal data for alumni relations/schools' development purposes?

It is not necessary to have a separate privacy notice for your processing of personal data for alumni relations and development purposes, however you may find that to fulfil the GDPR requirement that privacy notices are concise yet specific, having a specific privacy notice which focuses on just how you process personal data for the purposes of alumni relations and development may be more transparent than including this in the school's organisational privacy notice. See the 'Draft Privacy Notices' section of this guide for a template privacy notice and appendix for alumni relations and development.

It is however important to remember that members of your school community may have multiple relationships with the school, for example an individual may be a parent and an alum, and therefore there must be a consistent and joined up approach to the privacy rights of individuals across the school.

29. How should we share privacy information with alumni?

The ICO suggests a **layered approach**. This means that you share key privacy information with your alumni such as the name of the school and the way you process personal data, with links to more detailed information, and that you consider different ways of sharing this information. You can provide privacy notices through a variety of mediums, face to face, on the phone, through an article in your newsletter, a poster, as part of an e-mail, on your website, etc. It is good practice to use the same medium you use to collect personal data to deliver privacy information, so if collecting information through an online form you should share privacy information as the alumnus is completing the form – not just wait and send it via e-mail afterwards.

In some instances, it may be difficult to communicate privacy information or share a privacy notice, for example when carrying out prospect research to identify a potential major donor. In cases like this, it is important that you share privacy information at an appropriate later date (see question 38). For further information, visit https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/where-should-you-deliver-privacy-information-to-individuals/

30. How often should we share our privacy notice with alumni?

There is no definitive timeframe for how *often* you should share your privacy notice with alumni. Indeed, GDPR says that if a person has already received your relevant privacy information, he or she does not need to receive it again.

However, it is important to review your privacy notice regularly – and if any really substantial changes are made, then these should be communicated to your alumni.

31. What do we do if our alumni association/society also have access to alumni's personal data?

You firstly need to **decide who 'owns' the personal data**, who is the data controller? – or are both organisations data controllers? If so, then independently or jointly? If the school is the data controller and you intend to continue to share personal data with the alumni association/society as a data processer, you will need to create a data processing agreement with the alumni association/society (see section on draft data processing agreements), and detail this in your privacy notice. If the alumni association/society is the data controller, and the school is performing services on its behalf, then the reverse is necessary.

If both the school and alumni association/society are data controllers then you will need to create either a data sharing agreement, or a joint data controller agreement, which clearly states why and how both organisations will process personal data and share this in your privacy notice(s) with your alumni. If you are joint data controllers,

this will require a more comprehensive agreement allocating responsibility, and you will need to make the "essence" of the arrangement available to data subjects. Either way, you may consider using a shared privacy notice or separate ones – but care must be taken to communicate the relationship, and any data sharing between the two organisations, accurately.

FAQs

32. There are alumni on our database and we don't know if we have their consent. Can we still contact them?

If you are unable to demonstrate that you have consent, then you may be able to rely on legitimate interests to contact these alumni by cerain means (you would need to carry out the Legitimate Interest Assessment as detailed above). If you can demonstrate that you have a legitimate interest to contact them, then you could contact these alumni by post or potentially by live telephone call (if telephone numbers are not registered with the TPS). **If you are not sure whether you have their consent to send emails, then do not send them an e-mail direct marketing message** – in fact even an e-mail which asks if they can confirm if they are happy to continue to receive e-mails from you is direct marketing.

Under GDPR, there is an obligation to keep information accurate and up-to-date and therefore you could contact an alumnus via e-mail as part of an administrative data cleansing exercise, but you would need to consider the wording of such an e-mail to avoid this being interpreted as direct marketing. We would consider this approach to be very risky by email, given recent ICO enforcement cases, and better carried out by post.

33. Can we still send communications to alumni which promote our alumni events?

Yes, but this is effectively direct marketing and therefore you will still need to consider your lawful basis for processing personal data. For post or live telephone calls to numbers not registered with the TPS you may be able to rely on legitimate interests or consent (see questions above). For electronic communications (e-mail, text, automated calls, or TPS-registered phone numbers), your school can only send direct marketing communications about alumni events if you have an alumni's consent. There is an argument that paid events could be promoted on a "soft opt-in" basis to those who have previously bought tickets, but again this would be at risk given the ICO's strict attitude (plus a marketing "opt out" would have to have been offered from the outset, which may be hard to prove).

34. An alumnus pays to be part of the alumni association/society either when they join the school as part of their fees or as a pupil leaves the school. Does this change the relationship between the school and the alumnus? Is there a different lawful basis (other than consent and legitimate interest) that we can rely on to process their personal information?

This suggests that there is essentially a 'contract' between the alumnus and the school. This does potentially bring in a new lawful ground.

However, to rely on a 'contract' as the lawful basis to process an alumnus' personal data, the processing must be 'necessary' to fulfil the obligations of the contract. In the case of an alumnus, who may well 'pay' to be part of the school's alumni association, it could be argued that the communications, invitations to events, etc are services or goods expected in return for their membership, so are part of a 'contract' with the school. It could also be argued that these communications are thereby "solicited", which takes them outside of PECR even if they are deemed to be marketing.

However, you would need to consider how you demonstrate that the communications, invitations to events, etc are all necessary to fulfilling the obligations of this contract

with the alumnus. If the processing is only necessary to maintain your business model more generally, this lawful basis will not apply and you should consider another lawful basis such as legitimate interests or consent.

Finally, a paid membership **could** be used as an argument for soft opt in, because a purchase has been made – but the same issues as above arise, plus soft opt-in only works for promoting the same organisation's "similar" goods and services. Schools should again only take this approach on an informed risk basis.

35. Do I need a lawful basis to process a donation from an alumnus

Yes: whilst you may not be carrying out direct marketing, you need a legal requirement to process the donation. However, you will surely have one: and processing a donation is likely to require writing to an alumnus to thank them for their donation. However, if you include further information about your school, which effectively promotes the aims and ideals of the school, you will risk being deemed to be carrying out direct marketing and will need to therefore consider which lawful basis you are relying on.

36. We organised a sponsored event for our alumni and the alumni who took part have given us their sponsorship forms so we can claim Gift Aid. Can we contact all the individuals who have sponsored the alumnus

An individual who sponsors someone they know, is unlikely to expect their personal data to be processed for direct marketing purposes by the organisation who received the donations. It may be that you wish to contact those who have sponsored an alumnus to thank them for their support. However, it would be difficult to argue that they have a realistic expectation to receive direct marketing from the school, unless you have made this clear on the sponsorship form and asked for their consent.

This also applies to online giving websites where individuals' details are captured. On online giving sites, individuals are normally given the choice as to whether they would like to hear from an organisation in the future, and if they agree, the online giving site will share their contact information with you in their reports.

37. How long can we store alumni data?

Under GDPR, **there is no definitive timeframe for storing personal data**. You need to consider whether your purpose for processing the personal data and the lawful basis for this processing, is still valid. This should be reviewed regularly to ensure you can clearly demonstrate that there is still a legitimate interest or valid consent to retain personal data. You must not retain personal data that you no longer need. From a development and alumni relations perspective, it is important to distinguish your alumni records from your pupil records. For example, when a pupil leaves school, whilst there are specific legal obligations to comply with around data retention (please see data retention section of this Guide), much of the personal data held by the school will not be necessary for you to continue your engagement. You must only retain the personal data that is appropriate to your purpose, so this might include contact details, the year they left they school for alumni reunions, their interests to inform invitations to alumni events.

It is important to be transparent with your alumni about how long you will keep their personal data both in your privacy notice and your retention policy. It may well be that you will retain their personal data indefinitely, which can be stated in your privacy notice and retention policy, with the caveat that you will review this on a regular basis to make sure you have a valid purpose and lawful basis to continue to process their personal data.

Finally, under GDPR, there are increased privacy rights for the individual, including the right to erasure and the right to object (including to direct marketing) and you need to have a process in place to respond to such requests from alumni.

38. Can we still carry out prospect research?

Yes. The IDPE benchmarking report recognises the crucial role major gift fundraising plays in schools' development, with schools on average reporting that their two largest gifts per year account for 40-60% of their annual fundraised income. Prospect research is integral to major gift fundraising, as it allows you to identify which members of your community have the propensity and capacity to give. Identifying potential donors is crucial both in terms of prioritising staff time and resources, and for the donor themselves – for example, it would be inappropriate to ask every alumnus for a donation of £100,000 as it is highly unlikely that all your alumni have the capacity to give at this level.

Where possible, you will need to inform alumni before you carry out any prospect research, including both why and how you are processing their personal data and under which lawful basis: consent or legitimate interests. Consent offers the opportunity to be completely transparent as to what prospect research you will be doing and for alumni to actively agree to this. However, it is also possible to rely on legitimate interests if you clearly document your prospect research activity, and share this with your alumni.

If you are researching alumni who are not part of your existing database and therefore potentially have not seen your privacy policy, you will need to ensure you share this with them, when you first make contact (or within 30 days) whichever is sooner. You must also remember to give them the right to object to the use of their personal data.

When carrying out prospect research, consideration should be given as to how much is within an individual's reasonable expectations – for example, there is a difference between researching an employee's description on a company website and someone's personal facebook account. If you're not sure what alumni's reasonable expectations are around prospect research, why not ask them and then document their responses to demonstrate your accountability?

For further information, please see the Institute of Fundraising's Connecting people to causes: a practical guide to research fundraising, in partnership with Bates Wells Braithwaite and More.

39. Can we look at information that is available on professional networking sites such as LinkedIn or information in the public domain, to find out more about an individual before we make an approach?

As detailed in question 38, prospect research supports schools in identifying potential donors and there is a lot of data within the public domain which can support schools in focusing their major gift fundraising efforts. This information can include published materials such as media reports, the rich list, company information, electoral roll, etc as well as information published by the individuals themselves on social media such as facebook, LinkedIn, etc.

Whilst the ICO has stated that GDPR does not stop you accessing information from publicly available sources, it is not 'fair game' to presume just because information is publicly available that you can process it, and potentially use it to your advantage. You still require a lawful basis for processing this personal information and you will need to be transparent with why and how you are processing such research.

For further information, please see the Institute of Fundraising's Connecting people to causes: a practical guide to research fundraising, in partnership with Bates Wells Braithwaite and More.

40. Can we still carry out wealth screening?

Yes. Whether you are sending it to a third party or just using publicly available information, the process of applying any kind of wealth analysis screening is a separate "use" of the data, and so you have to be able to show that it is fair, lawful, and transparent. This means being upfront about how you are processing personal data and telling individuals what you are doing. You also need to consider what your lawful basis for carrying out wealth screening is: consent or legitimate interests. Following the fines issued by the ICO to certain charities, implied consent on the basis that you mentioned it in your privacy policy is unlikely to be sufficient. You will either need demonstrable consent for this particular use or if relying on legitimate interests, you will need to address how you can ensure the balance between the legitimate interests of the school and the privacy rights of the individual. A good starting point is to carry out a DPIA (see question 43) to assess the risk to your alumni's privacy rights, and also to demonstrate your school's commitment to accountability.

The ICO has been very clear that in order to be fair, you must be transparent, and the test of this is likely to be whether you have been detailed enough in the information you have shared, that an individual will not only understand exactly what it is you are doing, but also that they have the right to object and stop this process if they wish.

For further information, please see the Institute of Fundraising's Connecting people to causes: a practical guide to research fundraising, in partnership with Bates Wells Braithwaite and More.

41. An alumnus shares contact details for another alumnus who is currently not on the school database. Can we contact them?

Where possible, encourage the alumnus who is already engaged with the school to ask their fellow alumnus to contact the school directly as this takes away the need to rely on effectively a third party, and allows you to share your privacy notice/consent form with them when they get in touch.

If this is not possible, you would need to consider the impact of contacting the alumnus directly and carry out a Legitimate IAssessment to assess this (as you would not be able to rely on consent in these circumstances). If you can satisfy the LIA, then you could contact the alumnus by post (or telephone if their number is not registered with the TPS) and share your privacy notice/request consent.

42. Under GDPR, can we still carry out due diligence which may include carrying out research on a potential donor?

Yes. Charity law demands that a charity (or school with charitable status) carry out due diligence on potential major donors in order to safeguard the school's reputation and integrity. Schools should have an ethical fundraising policy in place, which includes a procedure for carrying out due diligence on potential major donors, to prevent from money laundering and/or fraud. In this instance it is not appropriate to ask the donor to consent to you carrying out such research as processing of personal data is a necessary legal requirement.

43. What is a Data Protection Impact Assessment (DPIA) and when might we need to use this for alumni relations or development?

A Data Protection Impact Assessment or DPIA can be used to help assess the necessity and proportionality of the processing of personal data in relation to the purpose and risks to an individual's privacy rights. It is likely that you will need to carry out a DPIA if you are looking to process personal data in a different way or to approach a new group of individuals. Within the context of alumni relations and development this could be if you are looking to research and identify alumni who are currently not on your database, to re-approach alumni who you have lost contact with, or if you are considering carrying out wealth screening and have not done this in the past. It is a way of demonstrating that the school has considered the privacy rights of

the individuals involved and carrying out a DPIA demonstrates accountability, one of the key principles of GDPR. For further information, see the DPIA section of this guide.

44. Can we contact an alumnus by e-mail without consent if we have their corporate e-mail address?

Whilst corporates are organisations, their employees are individuals and still have privacy rights in relation to any personal data which specifically identifies them. For example, covering e-mail addresses often include an individual's name, i.e. name.surname@organisation.com.

However, when approaching corporates you may lawfully use legitimate interests to send direct marketing communication by e-mail under the 'corporate subscriber' category of recipient. This will only apply if the individual works for an organisation that falls within the corporate subscriber category of organisation and the purpose of the communication is relevant to the corporate. For example, this could be contacting an alumnus to speak at a business networking event, to mentor a current pupil, or to make a fundraising request directed at the corporate, where the approach is relevant to their work, i.e. a request to a design and print company for in kind support to design and print the school brochure. Even when using the corporate subscriber category, you will still need to satisfy the legitimate interests test and an individual still has the right to ask you to stop using their personal work e-mail address for direct marketing.

For further information, please see the Institute of Fundraising and Fundraising Regulator's GDPR Spotlight on Corporate Fundraising.

45. Is trust fundraising affected by GDPR?

Whilst trusts like corporates are organisations, the individuals associated with the trust will still have privacy rights in relation to any personal data which specifically identifies them. For example, covering e-mail addresses often include an individual's name, i.e. name.surname@organisation.com. As with corporates, there is the potential to rely on the 'corporate subscriber' category to send e-mails without consent (see question 44), if for example these relate to seeking further information from a trust about their grants or to submit a request for support. Please note, the 'corporate subscriber' category would not apply when requesting personal donations, consent would be required if making a personal ask over e-mail, even if using an organisational e-mail address.

You may also need to carry out research on particular trustees of a trust or foundation, to identify those trusts whose objectives and policies best match your school's need. This is processing of personal data and therefore you will need to consider what lawful basis you are relying on to carry out this prospect research (see question 318

For further information, please see the Institute of Fundraising's GDPR Spotlight on Trust Fundraising.

46. Do we have to comply with GDPR if an alumnus has passed away?

GDPR only applies to any information relating to a living individual who can be directly or indirectly identified from it. There is however, a duty of care in respect to the personal data of the deceased and if retaining personal data on an individual who has passed away. It is important to consider what personal data you are retaining, the purpose for doing so and whether you have a valid lawful basis for continuing to store this personal data.

47. Can we contact the family of an alumnus if they have left a legacy to the school?

Yes. In many cases, the administration of an estate where someone has left a legacy, will be carried out by a solicitor therefore there may not be any need to communicate with family members.

If not, a school can write to the family of the legator, as you have a legal duty to carry out the donor's wishes, but you must be careful to focus only on the administration of the legacy. Whilst the family may well want to support the school in the future, any additional requests such as to sign up to the school's newsletter will be viewed as direct marketing and therefore under GDPR, will require a different lawful basis for processing the family's personal data, i.e. consent or legitimate interests.

For further information, please see the Institute of Fundraising and the Fundraising Regulator's GDPR Spotlight on Legacy Fundraising.

48. When do we need data sharing agreements?

You will need a data sharing agreement in place whenever you are sharing personal data between data controllers (this is different to sharing data with a data processor, see question 49). In the context of alumni relations and development, you may be sharing data with your alumni association/society (or your PTA), effectively more than one data controller has access to and is processing a shared data set.

A data sharing agreement should, at least, document the following issues:

- the purpose, or purposes, of the sharing
- who the data will be shared with
- the data to be shared
- how you will ensure data quality – accuracy, relevance, usability etc
- how you will ensure data security
- retention of shared data
- individuals' rights – procedures for dealing with access requests, the rights to object/erasure, queries and complaints
- review of effectiveness/termination of the sharing agreement
- sanctions for failure to comply with the agreement or breaches by individual staff

As with all processing of personal data, you will need to consider which lawful basis you are relying on to share personal data. Where you are sharing data with other organisations this will need to be detailed in your privacy notice and if relying on consent, specific consent is likely to be needed for sharing personal data. Whether relying on legitimate interests or consent, the principle of transparency applies and therefore it is important to share who you will be sharing data with and why.

49. When do we need data processing agreements?

You will need a data processing agreement when you are sharing data with a third party who is processing this data on your behalf. In the context of alumni relations and development, this could be a mail-house or wealth screening company. As data controller, you must ensure you have a data processing agreement in pace with any data processors. This should be a written contract, that details:

- the processor only acts on instructions from the data controller
- demonstrates the appropriate security is in place

As a data controller, even if using a third-party organisation to process personal data you still have ultimate responsibility for the personal data and must carry out the necessary due diligence on third-party data processors to ensure they are compliant with GDPR.

As with data sharing, the principle of transparency applies and therefore it is important to share in your privacy notice who you will be sharing data with and why, or if you cannot be explicit, the types of organisation who will be processing personal data on your behalf and why.

50. Can we share data with volunteers?

Yes, however you will need to consider volunteers in a similar way to third-party organisations, they are effectively data processors. As such, you will need to have some sort of 'contract' in place which is signed by the volunteer to ensure they understand and agree to the restrictions on the use of the personal data. Likewise, you will need to consider there is the appropriate security in place for transferring personal data to volunteers, for example password protection or encryption and that your privacy notice details how and why volunteers process personal data.

51. Outside of GDPR, what other legislation or regulations do I need to consider when working in alumni relations and/or schools' development?

We have already mentioned PECR, the Privacy and Electronic Communications Regulations, which is relevant to direct marketing via certain communications channels (see question 16).

As the majority of schools are registered charities, you will also need to consider charity law and regulation. In the context of development, it is important to recognise the move towards increased monitoring of fundraising, not just of the income raised but of *how* this income has been raised. The CC3 The Essential Trustee, CC20 Charities and Fundraising and Charity Governance Code, provide detailed guidance on the responsibilities of Trustees/Governors, particularly around fundraising. Further information can be found on the Charity Commission website, https://www.gov.uk/government/organisations/charity-commission/about/publication-scheme

Following the Etherington Review into fundraising practice, the Fundraising Regulator was established in 2015, to strengthen the regulation of fundraising. The Fundraising Regulator is responsible for investigating complaints into fundraising practice; operating the Fundraising Preference Service which enables individuals to manage their contact with charities; and developing the Code of Fundraising Practice, which is a set of standards expected of all charitable fundraising organisations across the UK. Further information can be found on the Fundraising Regulator's website, https://www.fundraisingregulator.org.uk/code-of-fundraising-practice/code-of-fundraising-practice-v1-4-310717-docx/

Finally, if your school is carrying out lotteries or raffles as part of your fundraising activity, you will also need to consider whether you need a license for such activity. Further information can be found in the Code of Fundraising Practice (see above) and on the Gambling Commission website, http://www.gamblingcommission.gov.uk/for-the-public/Fundraising-and-promotions/Fundraising/Lotteries-at-events.aspx

SUMMARY

Compliance with the GDPR is not just the responsibility of one department within the school, it requires the whole school to work together, and therefore alumni relations and development professionals must work with your senior leadership team (the IMGO) on this school-wide approach.

Successful alumni relations and development depend on engaging effectively with your alumni and wider community. The GDPR places a greater emphasis on transparency and accountability, and you will need to demonstrate these when building these relationships. GDPR does not stop you from engaging with you community, nor does it stop you from fundraising. It just emphasises the importance of individual's privacy rights and how compliance must become part of your day-to-day relationship building – it does not define it.

Notifying the ICO of a data breach - actions for schools

Under GDPR the guidance on notifying the ICO of a data breach has changed.

This guidance assumes that the criteria for reporting breaches to the ICO are understood - in short, this means that Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is about more than just losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A breach should be reported if it will result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Such matters may separately require a report to the Charity Commission but be careful with which organisation the data protection duty lies as Serious Incident reports are subject to Freedom of Information requests which may, if answered, create a further data or privacy breach if the lines of responsibility are not clear.

FAQs

Do we have to report every data breach?

Not necessarily, although you are certainly expected to record them internally – and it is strongly advisable to include a record of how it was assessed, what steps were undertaken and why the decision was made not to report it. This will be useful later if there are any unanticipated consequences.

The ICO do not want to be appraised of every “Reply All” email, temporary system outage, or every loss of an encrypted device - the intention of the new reporting regime is not to generate more fines and enforcement notices, but (in line with wider government policy) to help the ICO gather statistical data on the patterns of UK data breaches. So, not all reporting of data breaches should be feared: see the ICO's blog here.

What is the threshold and timescale for notifying the ICO?

"*…without undue delay and, where feasible, not later than 72 hours after having become aware of it… unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons*."

As above, this is changing under GDPR. Under the previous regime it was common first to inform the individuals affected, and gauge their reaction, before deciding whether or not to report the breach to the ICO. From 25 May 2018, this will rarely be feasible within the 72-hour timeline allowed for notification, absent a reason for delay. One such reason might previously have included consulting with those affected to assess the likely harm: but under GDPR the

threshold for notifying the ICO is in fact lower than for notifying individuals, hence this is likely to take priority when responding to a data breach.

Schools which have charitable status, should keep in mind that any report made to another regulator ought routinely to be backed up with a report to the Charity Commission and/or the Fundraising Regulator, if appropriate. This tends to result in a very soft, hands-off response for all but the most serious of breaches. It may be in due course that this practice will change in respect of more minor data breach reporting: but until otherwise notified, this should continue as before under GDPR.

What is the threshold and timescale for notifying affected individuals?

"when likely to result in a high risk to the rights and freedoms of natural persons… without undue delay."

Communication of the breach to those affected is only strictly necessary if the likely harm is high risk: whether from embarrassment or loss of privacy, or exposure to fraud. There is both a reputational and a legal sensitivity to how this is handled. Individuals are likely to be increasingly aware of the right to bring group claims. Such claims may be low-value, but a breach in respect of even a single person can be serious if the data is particularly sensitive. It does not follow that every data breach will always give rise to a potential claim, even if harm is caused. A claim for loss or distress may only be brought where it was caused by a contravention of the law by the school: for example, if its data security was inadequate or an employee's unlawful actions were to blame.

What about breaches caused, or suffered, by our suppliers?

You may be liable for breaches affecting your own data which impact your suppliers, notably IT providers, which is one of the reasons it is important to have a robust contract in place. By law they must notify you "*without undue delay*" if they become aware first, but the contract should ideally include a specified period. Any obligation on you to report begins once you are first made aware but the first hours and days are vital to minimising the impact.

What is the practical approach to dealing with a data breach?

A distinction ought to be drawn between an obviously serious breach that triggers a crisis plan (involving potential roles for IT, legal and PR advisers) and a more mundane breach that ought nevertheless to be dealt with as a matter of policy and record. Of course, it can be hard to see the difference before an assessment has taken place.

A step-by-step guide is provided on the next page (but this is a guide, rather than a substitute for a formal plan).

What does the ICO's Guidance say?

The ICO has an expanded section on data breach in its general Guide to the GDPR which is helpful.

The ICO's fuller guidance on data breach management has not been updated for GDPR. It still contains some valuable insights but its emphasis on assessment before notification will bring risks after 25 May 2018. The four elements that it identifies to breach management (*1. Containment and recovery; 2. Assessment of ongoing risk; 3. Notification of breach; 4. Evaluation and response*) remain relevant but should not be taken as a strict order of proceedings. From 25 May, the recommendation must be for early notification, potentially on a provisional holding basis. GDPR allows for phased provision of information, so this may be followed up later (without undue delay) with either (a) fuller updates; or (b) confirmation that the matter is closed and contained without likely harm.

This means that neither the ICO's existing breach self-reporting form (which is quite detailed and requires filling out with care) nor the malicious breach form (which is slightly less exacting) are likely to be suitable for every early notification. The ICO is setting up a telephone reporting

line to sit alongside its online forms and it is to be hoped these will allow for provisional notifications and not be too prescriptive in terms of required fields. In any event schools may wish to prepare their own forms to record internal assessments. Time will tell whether the ICO will accept these as valid reporting tools, but they will have value as internal records (as required by GDPR).

What steps should we take to prevent data breaches?

There are two elements to this question: the "before" and "after". Plenty of sensible steps can be recommended to mitigate the likelihood, and likely impact, of future breaches. However, the risk of a breach can never be eliminated – whether due to sophisticated attacks, human error, or rogue employees – so learning to react is critical. Your school's crisis management and/or business continuity plans should cover major breach incidents but having a data breach specific response plan (with allocated staff) is now on the ICO's GDPR checklist.

(a) Preparatory steps

On top of the crisis plan mentioned above, there is also routine best practice. In terms of basic data security groundwork, making sure school mobile devices and memory sticks are fully encrypted is a quick win. This should be tied in with effective policies on working from home, "bring your own device" protocols, email usage, data retention and secure deletion, information sharing and secure delivery methods, and a meaningful password culture (including managing internal access rights to information which should be on a need-to-know basis).

Policy and structure is just as important as having secure IT. If a breach occurs, schools will be expected to prove that staff training took place and policies were properly notified and enforced. Where schools outsource systems and processes which require use of e.g. pupil data (which again goes beyond IT), they have a legal obligation to secure sufficient contractual guarantees that the data will be handled safely and by competent people.

(b) Remedial steps

Action after the event is also important: policy and systems review, re-training, and – for more major incidents – a review of the causes of the incident and the effectiveness of the school's response.

This is not simply a case of shutting the stable door: nothing improves practices like learning from mistakes and there will be future data incidents. From the ICO's perspective, a key aspect of closing a data breach case is noting the remedial steps taken: and, ideally, schools will be pro-active in telling the ICO what they have done, rather than waiting to be told. When the next incident happens (as it inevitably will) the ICO will look at the school's past record and assess whether lessons were learned and whether any promises made were kept.

STEP GUIDE TO DATA BREACH RESPONSE (*to form part of the school's response plan*)

1. Upon the first employee becoming aware of the breach

- *Am I the relevant person at the organisation? If not, immediately notify that person.*

2. Initial assessment, containment and recovery – first few hours:

    - *How long has the breach been active, what data was involved and how far has it got?*
    - *What immediate steps can be taken to prevent it going further? Consider:*
        - *if a cyber breach, involve the school's IT personnel from the outset;*
        - *if human actor(s) are involved, can they be contacted to give reassurances;*
        - *if e.g. Royal Mail, courier, IT or other contractors are involved, can they assist;*
        - *are specialists needed: forensic IT consultants, crisis management PR, legal etc.*

3. Ongoing assessment of risk and mitigation – first 72 hours (and initial notification where required):

    - *Build up a more detailed picture of the risk and reach of the security breach:*
        - *how many have been affected?*
        - *was any sensitive personal data involved – health, sexual life, crime?*
        - *was financial data involved and/or is there a risk of identify fraud?*
    - *Identify if a crime has been committed and involve police or cyber fraud unit.*
    - *Assess if insurers need notifying (major loss, crime, or possible legal claim(s))*
    - *Decide if the likely risk of harm to the data subjects:*
        - *is sufficient to require a full <u>or</u> preliminary notification to the ICO; and*
        - *is sufficiently serious to require communication to affected individuals*
    - *If not, is this a matter we can document but deal with internally? or*
    - *If so, what can we usefully tell the ICO and/or individuals at this stage?*
        - *e.g. provide fraud or password advice, offer counselling etc.*

4. Ongoing evaluation, monitoring and remediation:

    - *Continue to monitor and assess possible consequences (even if apparently contained).*
    - *Keep the ICO and/or those affected informed as new information becomes available.*
    - *Tell the ICO and/or those affected what you are doing to remediate and improve practice.*
    - *Begin process of review internally:*
        - *how did this happen? What could we have done better?*
        - *would training or even disciplinary action be justified for staff members?*
        - *were our policies adequate, and/or adequately followed?*
        - *if our contractors were involved (e.g. systems providers), did they respond adequately? Do we have any remedies against them if not?*

5. Record keeping and putting outcomes into practice:

- *Keep a full internal record, whether or not the matter was reported or resulted in harm.*
- *Log this record against wider trends and compare with past incidents.*
- *Make sure all past outcomes were in fact put into practice.*
- *Ensure any recommendations made by, or promised to, the ICO are actioned.*
- *Notify the Charity Commission as an RSI, if a charity, at an appropriate juncture (and any other regulatory bodies if necessary).*
- *Review policies and ensure regular (or specific, if required) training is actually completed.*

Serious breaches should be reported to the ICO using the security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach and give advice.

Or, use the security breach notification form, which should be sent to the email address: casework@ico.org.uk
or by post to the ICO office address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

The security breach notification form can be found here:

https://ico.org.uk/media/fororganisations/documents/2666/security_breach_notification_form.doc

PRIVACY IMPACT ASSESSMENT (PIA) TEMPLATE
Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the data collection develops if you need to.

- **Will the data collection involve the collection of new information about individuals?**
- **Will the data collection compel individuals to provide information about themselves?**
- **Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?**
- **Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**
- **Does the data collection involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.**
- **Will the data collection result in you making decisions or taking action against individuals in ways that can have a significant impact on them?**
- **Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.**
- **Will the data collection require you to contact individuals in ways that they may find intrusive?**

Privacy impact assessment template

The template follows the process that is used in the ICO's PIA code of practice. (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)

Step one: Identify the need for a PIA

Explain what the data collection aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.
You may find it helpful to link to other relevant documents.
Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions above).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the data collection and holding.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your data collection management process. You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify what type of personal data you are processing, the key privacy risks and the associated compliance and corporate risks. Larger scale PIAs might record this information on a more formal risk register.

Definition of personal data (Schedule 2):
Data which relates to a living individual who can be identified –
(a) from that data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Definition of sensitive personal data (Schedule 3):
Personal data consisting of information as to -
(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union,
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The eight Data Protection Principles:
1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Principle 1 - Personal data shall be processed fairly and lawfully
Privacy issue
Have you identified the purpose of the project?
Is there a lawful reason you can carry out this project?
How will you tell individuals about the use of their personal data?
Do you need to amend your privacy notices?

The school's main one can be found here (insert hyperlink) Do you have specific ones for your department?

Have you established which schedule 2 conditions for processing apply? (See above)
If sensitive personal data is involved, have you established which schedule 3 conditions for processing apply? (See above)

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
Will your actions interfere with the right to privacy under Article 8 of the Human Rights Act? (http://www.legislation.gov.uk/ukpga/1998/42/contents) If yes, is it necessary and proportionate?
Have you identified the social need and aims of the project?
Are your actions a proportionate response to the social need?

Principle 2 - Personal data shall be obtained only for one or more specified and lawful purposes
Privacy issue
Does your data collection plan cover all of the purposes for processing personal data?
Which personal data could you not use, without compromising the needs of the project?

Principle 3 - **Personal data shall be adequate, relevant and not excessive**
Privacy issue
Is the quality of the information good enough for the purposes it is used?
Which personal data could you not use, without compromising the needs of the project?

Principle 4 - Personal data shall be accurate and, where necessary, kept up to date
Privacy issue
If you are procuring new software does it allow you to amend and / or delete data when necessary?
How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary
Privacy issue
What retention periods are suitable for the personal data you will be processing?
How long will you keep the data for?
Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6 - Personal data shall be processed in accordance with the rights of data subjects
Privacy issue
What process is in place to answer 'Subject Access Requests' (requests for personal data)?

Principle 7 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Privacy issue
Do any new systems provide protection against the security risks you have identified?
What training and instructions are necessary to ensure that staff know how to operate a new system securely?
What training on data protection and / or information sharing has been undertaken by relevant staff?

Principle 8 - **Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection.**
Privacy issue
Will the data collection require you to transfer data outside of the EEA? If yes how does it demonstrate an adequate level of protection?
If you will be making transfers outside the EEA, how will you ensure that the data is transferred securely?

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk Solution(s) Result: is the risk eliminated, reduced, or accepted?
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
(see below for some examples of the potential risks that a PIA could identify)

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?
Risk Approved solution. Approved by ……?
(see below for some examples of the potential actions that could be included in your PIA as ways of reducing the risks to privacy)

Step six: Integrate the PIA outcomes back into the data collection plan

Who is responsible for integrating the PIA outcomes back into the data collection and management plan and updating any data collection management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?
Action to be taken

Date for completion of actions

Responsibility for action

Contact point for future privacy concerns

For further information, visit https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

Privacy Impact Assessment – Guidance

Below are some of the risks to individuals, which you might identify when completing a PIA.

- **Individual risks** Inadequate disclosure controls increase the likelihood of information being shared inappropriately.

- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.

- New surveillance methods may be an unjustified intrusion on their privacy.

- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.

- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.

- Identifiers might be collected and linked which prevent people from using a service anonymously.

- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.

- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.

- Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, presents a greater security risk.

- If a retention period is not established information might be used for longer than necessary.

Corporate risks

- Non-compliance with data protection legislation can lead to sanctions, fines and reputational damage.

- Problems which are only identified after the data collection has launched are more likely to require expensive fixes.

- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.

- Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, is less useful to the business.

- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.

- Data losses which damage individuals could lead to claims for compensation.

Reducing the risks

There are many different steps which organisations can take to reduce risks to privacy rights. Some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Limiting the number of staff who have access to specific data sets, ensuring this is on a need-to-know basis
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's
behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Organisations will need to assess the costs and benefits of possible privacy solutions. Some costs will be financial, for example an organisation might need to purchase additional software to give greater control over data access and retention. These costs can be balanced against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.

The draft privacy notices and their covering note are supplied as draft documents for schools to use as they need to, each will require modification to suits the school's policies and particular circumstances.

XXXX School – Privacy Notice and annexes

The EU General Data Protection Regulation (GDPR) includes rules on giving privacy information to those whose data is held by an organisation (data subjects). These are more detailed and specific than in the DPA and place an emphasis on making privacy notices understandable and accessible. Data controllers are expected to take 'appropriate measures' to ensure that this is the case.

The school interprets this as using very clear language to outline each of the responsibilities for each of the data subject groups.

The GDPR say that the information provided to data subjects about how the school processes their personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

These requirements are about ensuring that privacy information is clear and understandable for data subjects. This privacy notice deals with the overall privacy responsibilities of the school but includes, as annexes the particular notices that apply to parents, pupils under the age of 13, pupils over the age of 13, staff, Governors and alumni. The appropriate annex should be read by the appropriate data subject along with the overarching notice.

Each annex deals with two sources of data, that obtained directly from the subject and, data not obtained directly from the subject. For both sources the Identity and contact details of the data handler (and where applicable, the handler's representative) and the data protection officer (or privacy officer) are provided.

The intention is that each privacy notice is used as a stand alone document, introduced and covered by the paragraphs above.

ANNEX A

Privacy Notice XXXX School – parents (or guardians) of children at the school, or applying to join the school

This annex should be read in conjunction with the introductory paragraphs in the covering document.
The italicised paragraphs in red refer to guidance from the ICO on the compilation of privacy notices.

(The privacy notice should be provided at the time the data was obtained, if it was obtained directly from the data subject.)

This privacy notice will be provided to you at the time your data is being obtained, if it is being obtained directly.

(The purpose of the processing and the legal basis for processing must be clearly stated and the categories of personal data held must be clearly stated.)

Data will be processed for the purposes of responding to requests for information about joining the school and the school will therefore have a "legitimate interest" for processing basic personal data and sensitive personal data. The data the school holds will be the minimum it requires to form and maintain the contract between you and the school.

(Any recipient or categories of recipient must be clear and it should also be clear if data transfer to other countries and the safeguards in place.)

The school will share your data with the following companies who have contracts with the school and who have equalled the school's precautions and systems for dealing with data, these are:

- Catering
- Photographer
- Health care service provider
- IT Contractor
- IT software provider

It is not necessary for data to be shared with other countries. The exception to this will be international trips that the school organises, should this be envisaged for your child, you will be contacted for your consent, the consent will be limited in time and content if it be required.

(*The retention period for the data or the criteria used to determine the retention period.)*

The retention period for pupil data will be until the pupil reaches the age of 25, [and / or be modified by any other legal obligation the school finds itself under.]

(*The existence of each data subject's rights. The right to withdraw consent at any time.)*

You have the right to withdraw your consent to data processing at any time, however this will only apply to certain groups of data for which you have given particular consent.

(*The right to lodge a complaint at any time with a supervisory authority.)*

You can complain at any time about how the school has handled your data, the Information Commissioner is available as follows:

ICO helpline is 0303 123 1113. A template letter, should you need it is at the appended to this notice.

(Where data is not obtained directly, the source from which it was obtained and whether or not it is a publicly available source.)

(For data obtained indirectly, the privacy notice should be provided within a one month (referred to as a reasonable period of time), when the first communication takes place with an individual, or if disclosure is envisaged to another recipient, at the latest, before the information is disclosed.)

We will obtain the data the school requires from you, should we need data from other sources we will contact you within a month.

(Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data.)

We see the provision of personal data as necessary to properly admit you child to the school and to administer, and for the school to fulfil its obligations under the contract once your child is a pupil here.

(The exitance of automated decision making including profiling and the information about how decisions are made, the significance and the consequences.)

There is no automated decision making or profiling involved in this data stream into and through the school.

Appendix

[Your full address]
[Phone number]
[The date]

[Name and address of the organisation]
[Reference number (if provided within the initial response)]

Dear [Sir or Madam / name of the person you have been in contact with]

Information rights concern
[Your full name and address and any other details such as account number to help identify you]

I am concerned that you have not handled my personal information properly.

[Give details of your concern, explaining clearly and simply what has happened and, where appropriate, the effect it has had on you.]

I understand that before reporting my concern to the Information Commissioner's Office (ICO) I should give you the chance to deal with it.

If, when I receive your response, I would still like to report my concern to the ICO, I will give them a copy of it to consider.

You can find guidance on your obligations under information rights legislation on the ICO's website (www.ico.org.uk) as well as information on their regulatory powers and the action they can take.

Please send a full response within 28 calendar days. If you cannot respond within that timescale, please tell me when you will be able to respond.

If there is anything you would like to discuss, please contact me on the following number [telephone number].

Yours faithfully
[Signature]

ANNEX B

Privacy Notice XXXX School – Children at the school over the age of 13.

This annex should be read with the introductory paragraphs in the covering document.
The paragraphs in red refer to guidance from the Information Commissioner's Office (ICO) on the compilation of privacy notices. The red sections are the sections that the ICO needs the school to comply with in its dealings with you.

(The privacy notice should be provided at the time the data was obtained, if it was obtained directly from the data subject.)

This privacy notice will be provided to you at the time your data is being obtained, if it is being obtained directly. This means you get this when the school gets your data from your parents, or within a month.

(The purpose of the processing and the legal basis for processing must be clearly stated and the categories of personal data held must be clearly stated.)

Data will be processed for the purposes of allowing you to make the best of your time at xxxx school. The school will therefore have what is called a "legitimate interest" for processing basic personal data and sensitive personal data. The data the school holds will be the minimum it requires to allow you to thrive in your years here.

(Any recipient or categories of recipient must be clear and it should also be clear if data transfer to other countries and the safeguards in place.)

The school will share your data with the following companies who have contracts with the school and who have equalled the school's precautions, systems and procedures for dealing with data, these are:

- Catering
- Photographer
- Health care service provider
- IT Contractor
- IT software provider

It is not necessary for data to be shared with other countries. The exception to this will be international trips that the school organises, should this be envisaged for you, you will be contacted for your consent, the consent will be limited in time and content if it is required.

(*The retention period for the data or the criteria used to determine the retention period.)*

The retention period for pupil data will be until you reach the age of 25.

(*The existence of each data subject's rights. The right to withdraw consent at any time.)*

You have the right to withdraw your consent to data processing at any time, however this will only apply to certain groups of data for which you have given particular consent.

(*The right to lodge a complaint at any time with a supervisory authority.)*

You can complain at any time about how the school has handled your data, the Information Commissioner is available as follows:

ICO helpline is 0303 123 1113. A template letter, should you need it is at the appended to this notice.

(Where data is not obtained directly, the source from which it was obtained and whether or not it is a publicly available source.)

(For data obtained indirectly, the privacy notice should be provided within a one month (referred to as a reasonable period of time), when the first communication takes place with an individual, or if disclosure is envisaged to another recipient, at the latest, before the information is disclosed.)

We will obtain the data the school requires from you, should we need data from other sources we will contact you.

(Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data.)

We see the provision of personal data as necessary to properly manage your time at XXXX school and for the school to fulfil its obligations to you.

(The exitance of automated decision making including profiling and the information about how decisions are made, the significance and the consequences.)

There is no automated decision making or profiling involved handling this data.

ANNEX C

Privacy Notice XXXX School – Governors of the school.

This annex should be read in conjunction with the introductory paragraphs in the covering document.
The italicised paragraphs in red refer to guidance from the ICO on the compilation of privacy notices.

(The privacy notice should be provided at the time the data was obtained, if it was obtained directly from the data subject.)

This privacy notice will be provided to you at the time your data is being obtained, if it is being obtained directly.

(The purpose of the processing and the legal basis for processing must be clearly stated and the categories of personal data held must be clearly stated.)

Data will be processed for the purposes of responding to requests for information about joining the Board of the school and the school will therefore have a "legitimate interest" for processing basic personal data and, if necessary, sensitive personal data. The data the school holds will be the minimum it requires.

(Any recipient or categories of recipient must be clear and it should also be clear if data transfer to other countries and the safeguards in place.)

The school will share your data with the following companies who have contracts with the school and who have equalled the school's precautions, systems and procedures for dealing with data, these are:

- IT Contractor
- IT software provider

It is not necessary for data to be shared with other countries. The exception to this will be international trips that the school organises, should this be envisaged for you, you will be contacted for your consent, the consent will be limited in time and content if it is required.

(*The retention period for the data or the criteria used to determine the retention period.)*

The retention period for data on Governors to be held will be 25 years.[or as detailed in the school's retention policy].

(*The existence of each data subject's rights. The right to withdraw consent at any time.)*

You have the right to withdraw your consent to data processing at any time, however this will only apply to certain groups of data for which you have given particular consent.

(*The right to lodge a complaint at any time with a supervisory authority.)*

You can complain at any time about how the school has handled your data, the Information Commissioner is available as follows:

ICO helpline is 0303 123 1113. A template letter, should you need it is at the appended to this notice.

(Where data is not obtained directly, the source from which it was obtained and whether or not it is a publicly available source.)

(For data obtained indirectly, the privacy notice should be provided within a one month (referred to as a reasonable period of time), when the first communication takes place with an

individual, or if disclosure is envisaged to another recipient, at the latest, before the information is disclosed.)

We will obtain the data the school requires from you, should we need data from other sources we will contact you first.

(Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data.)

We see the provision of personal data as necessary to safeguard you and the school as it will allow the necessary checks to be made.

(The exitance of automated decision making including profiling and the information about how decisions are made, the significance and the consequences.)

There is no automated decision making or profiling involved in this data stream into and through the school.

Annex D

Privacy Notice XXXX School – alumni

This annex should be read in conjunction with the introductory paragraphs in the covering document.
The italicised paragraphs in red refer to guidance from the ICO on the compilation of privacy notices.

Routine contact with alumni will be by surface mail, email will only be used as a method of contact if the individual alums gives consent to be contacted in this way.
(The privacy notice should be provided at the time the data was obtained, if it was obtained directly from the data subject.)

This privacy notice will be provided to you at the time your data is being obtained, if it is being obtained directly.
(The purpose of the processing and the legal basis for processing must be clearly stated and the categories of personal data held must be clearly stated.)

Should you give consent data will be processed for the purposes of maintaining an accurate record of those who were educated at xxxx school. The school will process only the minimum personal data to achieve this purpose.

(Any recipient or categories of recipient must be clear and it should also be clear if data transfer to other countries and the safeguards in place.)

The school will not share your data with any companies associated with the school.

It is not necessary for data to be shared with other countries.

(*The retention period for the data or the criteria used to determine the retention period.)*

The retention period for alumni data will be unlimited as long as the school believes it has a relationship to serve with the alum.

(*The existence of each data subject's rights. The right to withdraw consent at any time.)*

You have the right to withdraw your consent to data processing at any time, however this will only apply to certain groups of data for which you have given particular consent.

(*The right to lodge a complaint at any time with a supervisory authority.)*

You can complain at any time about how the school has handled your data, the Information Commissioner is available as follows:

ICO helpline is 0303 123 1113. A template letter, should you need it is at the appended to this notice.

(Where data is not obtained directly, the source from which it was obtained and whether or not it is a publicly available source.)

(For data obtained indirectly, the privacy notice should be provided within a one month (referred to as a reasonable period of time), when the first communication takes place with an individual, or if disclosure is envisaged to another recipient, at the latest, before the information is disclosed.)

We will obtain the data the school requires from you, should we need data from other sources we will contact you first.

(Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data.)

Annex E

Privacy Notice XXXX School – employees of the school, or applying to join the school

This annex should be read in conjunction with the introductory paragraphs in the covering document.
The italicised paragraphs in red refer to guidance from the ICO on the compilation of privacy notices.

(The privacy notice should be provided at the time the data was obtained, if it was obtained directly from the data subject.)

This privacy notice will be provided to you at the time your data is being obtained, if it is being obtained directly.

(The purpose of the processing and the legal basis for processing must be clearly stated and the categories of personal data held must be clearly stated.)

Data will be processed for the purposes of responding to requests for information about joining the school and the school will therefore have a "legitimate interest" for processing basic personal data and sensitive personal data. The data the school holds will be the minimum it requires to form and maintain the contract between you and the school.

(Any recipient or categories of recipient must be clear and it should also be clear if data transfer to other countries and the safeguards in place.)

The school will share your data with the following companies who have contracts with the school and who have equalled the school's precautions and systems for dealing with data, these are:

- Health care service provider
- IT Contractor
- IT software provider
- DBS Clearance provider

It is not necessary for data to be shared with other countries. The exception to this will be international trips that the school organises, should this be envisaged for you, you will be contacted for your consent, the consent will be limited in time and content if it be required.

(*The retention period for the data or the criteria used to determine the retention period.)*

The retention period for employee data will be until …….., [and / or be modified by any other legal obligation the school finds itself under.]

(*The existence of each data subject's rights. The right to withdraw consent at any time.)*

You have the right to withdraw your consent to data processing at any time, however this will only apply to certain groups of data for which you have given particular consent.

(*The right to lodge a complaint at any time with a supervisory authority.)*

You can complain at any time about how the school has handled your data, the Information Commissioner is available as follows:

ICO helpline is 0303 123 1113. A template letter, should you need it is at the appended to this notice.

(Where data is not obtained directly, the source from which it was obtained and whether or not it is a publicly available source.)

(For data obtained indirectly, the privacy notice should be provided within a one month (referred to as a reasonable period of time), when the first communication takes place with an individual, or if disclosure is envisaged to another recipient, at the latest, before the information is disclosed.)

We will obtain the data the school requires from you, should we need data from other sources we will contact you within a month.

(Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data.)

We see the provision of personal data as necessary to properly employ you at the school and to administer, and for the school to fulfil its obligations under the contract once you are an employee here

(The exitance of automated decision making including profiling and the information about how decisions are made, the significance and the consequences.)

There is no automated decision making or profiling involved in this data stream into and through the school.

The draft letter for suppliers with access to school data is for schools to use as needed, although it may require modification to suit your school's particular circumstances.

The ISBA Member School

The suppliers with access to school data x March 2018

General Data Protection Regulations – School Data, its handling and security

You will be aware that the General Data Protection Regulations (GDPR) comes into force on 25 May2018. The school has been putting plans in place for this change and, as part of its preparation, the school needs to be reassured that each of its suppliers, who have a responsibility for processing, storing and disposing of school data, has the appropriate policies, procedures and safeguards in place.

As your company processes data on behalf of the school, would you forward a copy of the following documents:

a. Your privacy statement covering how your company deals with data as a whole.
b. The privacy impact assessment that assesses the risk your company poses to the security of the data from the school.
c. The training records for the staff involved in handling the data.

These will be held by the school as part of its Data Management Organisation and will not be shared with any third party.

If you have any questions on the above please let me know, otherwise I look forward to receiving the documents.

……..

Bursar

XXXX School – Information Sharing Agreement (ISA)

This Information Sharing Agreement (ISA) defines the arrangements for processing data between xxxx School and the travel company named in the right-hand box below.

Parties to the agreement: Full name and address of the travel company:

School Address	

The following information about students and staff:

- Medical / dietary needs
- [ ] Tour – Full Name and Date of Birth

is being shared by xxx School to enable the travel company named above to organise a school trip for our students and staff for trips travelling between 01/01/2018 and 31/12/2018.

- The information is shared securely with [ ] Limited.
- The information will be stored securely by [ ] Limited.
- [ ] Limited will not pass any details on to any other organisation, unless agreement has been obtained from xxxx School and providing the sharing is to help make the trip possible.
- [ ] Limited agrees to destroy the data once the trip and all related matters have been concluded.

This agreement must be formally approved and signed by both parties before any information sharing takes place. Both parties will ensure that the ISA and any associated documents are known and understood by all staff involved in the process.

Originating organisation:

Name of organisation: XXXX School

Name:

Partner organisation:

Name of travel company:

Name:

Position:

Signature:

Signature on behalf of [ ]:

Date:

Date:

Xx xxxxxxx 2018

Ref:

Dear Parents

Further to the trip briefing held on xx xxxxx(date), I attach a summary of the points raised and discussed, together with a document covering travel, hotel and key locations to be visited and researched.

I would also like to take this opportunity to confirm the Data Protection agreement we have with ABC Travel Limited who have helped organise this trip. It has been agreed that we can share information with ABC Travel, with regards medical/dietary needs and the full name and date of birth of each pupil, but only if they fulfil the following conditions:

- The information is shared securely with ABC Travel Limited.
- The information will be stored securely by ABC Travel Limited.
- ABC Travel Limited will not pass any details on to any other organisation, unless agreement has been obtained from XXXX School and providing the sharing is to help make the trip possible.
- ABC Travel Limited agrees to destroy the data once the trip and all related matters have been concluded.

If you wish to discuss any of the above further with me, please do not hesitate to contact me.

Yours sincerely

Guidelines on the Storage and Retention of Records and Documents

GDPR and document retention

GDPR does not fundamentally change the principles for length of document retention – it is still a question of relevance and purpose, as well as data security.

It does, however, have stricter rules about use and storage of personal data generally with the practical effect of requiring more dynamic, efficient and secure storage systems. Notably:

- All information held by schools needs to be justifiable, by reference to its purpose;
- Schools must be transparent and accountable as to what they hold;
- Schools must understand and explain the reasons why they hold data – which also means keeping records that explain how decisions around personal data are made;
- Schools must be prepared to respond more quickly to subject access requests;
- Schools must be able to amend, delete or transfer data promptly upon any justified request, or otherwise be prepared to explain why they will not;
- It should be possible to audit how your personal data was collected and when; and
- Sensitive data must be held securely, accessed only by those with reason to view it, and schools should have an "appropriate policy document" as to why it is needed.

In practice these purposes must be explained to those affected – parents, pupils, ex-pupils, staff – although that is not to say a school's specific data retention periods need to be public. However, under GDPR the basic principles and the rationale behind them do need to be communicated as part of the school's Privacy Notice.

The GDPR requirement on organisations to document their processing activities (i.e. to keep a record of what they do and why) is separate from the considerations of this note, which deals with questions of how long to retain the data itself, and why. The ICO has produced guidance around the documentation process.

IICSA, child protection and document retention

In the light of the Independent Inquiry into Child Sexual Abuse (IICSA), former Chair Dame Lowell Goddard's forceful statements, and various high-profile safeguarding cases, all independent schools will be aware of the emphasis currently being placed on long-term, lifetime or even indefinite keeping of full records relating to incident reporting. Many will be extending this rule to all personnel and pupil files on a 'safety first' basis.

This section has been drafted in full awareness of these considerations. **It is strongly recommended in the current climate that schools do not embark on a policy of deleting historic staff and pupil files, or any material potentially relevant for future cases, even if it has been held for long periods already. Data protection issues should never put child safety at risk, nor take precedence over the general prevention and processing of safeguarding claims.**

What should also be emphasised is that the present focus on safeguarding does not mean that existing laws in respect of data protection or confidentiality are now in suspension, nor that schools may not still be liable for breaches of data protection legislation (such as retaining personal data longer or in greater volume than *is necessary for its purpose*, or a failure to keep the data accurately or safely).

Schools will already find legal support for lifetime retention of adequate and accurate records where they are of potential relevance to historic cases. However, schools should be aware that the longer they hold large amounts of personal data, the more onerous their exposure is to subject access rights (individual requests for data) and data breach. Sensitive personal data of employees or pupils, including allegations of a sexual or criminal nature (whether proven or not), or details as to physical or mental health, should be kept securely and shared

or accessible only on a need-to-know basis – for example, where a competent authority reasonably requests such information citing lawful grounds.

Some Designated Safeguarding Leads (DSLs) and local authorities advise that when schools pass on a child protection file to a new school, as required whenever a pupil is being transferred, they should delete their own copy. Whilst this may be appropriate for maintained schools, for independent schools in the current environment – in light of IICSA's statement and possible future claims against the school – it is a clear risk to delete any records of incidents that occurred while the pupil was at the school, or any information that was relevant to what action the school took (just as it would be for a pupil leaving the school at the normal academic age). Schools must balance that risk against any risk of seeming to demur from local authority advice or guidance.

In due course we expect more settled guidance from the relevant authorities on striking this balance. In the meantime, the threat of historic abuse claims is to be weighed against that of relatively minor data protection contraventions. In such circumstances it would be very inadvisable to start disposing of historic insurance, pupil and personnel files except where no living person could bring a claim; and if practical resources mean that it is not feasible to conduct a thorough review, then schools should in the current climate err on the side of retention, rather than disposal, of staff and pupil files.

The purpose of this note

Schools will generally seek to balance the benefits of keeping detailed and complete records – for the purposes of good practice, archives or general reference – with practical considerations of storage, space and accessibility. However, whilst independent schools are not as directly regulated as state maintained schools, there are still legal considerations in respect of retention of records and documents which must be borne in mind. These include:

- statutory duties and government guidance relating to schools, including for safeguarding;
- disclosure requirements for potential future litigation;
- contractual obligations;
- the law of confidentiality and privacy; and (last but by no means least relevant)
- the GDPR and Data Protection Bill will inform (although not prescribe) minimum and maximum retention periods, as well as what to keep and who should be able to access it.

For example, the General Data Protection Regulation (GDPR) and the Data Protection Bill, will allow for longer retention for archiving, that will be useful for some aspects of school record-keeping, but subject to limitations and safeguards about what is necessary and in the public interest

Striking a balance

Even justifiable reasons to keep certain records, such as child protection records, for many years after pupils or staff leave the school will need to be weighed against an individual's privacy rights. The longer potentially relevant personal data is retained, and the more sensitive material is kept on file, the greater the administrative burden on schools, in terms of both secure storage and individual subject access rights.

Steps a school can take to support its retention policies are (a) communicating the reasons for the policy in Privacy Notices and staff or parent contracts; and (b) ensuring any records necessary to keep long-term are kept very secure, accessible only by trained staff on a need-to-know basis.

Meaning of "record"

In these guidelines, "record" means any document or item of data which contains evidence or information relating to the school, its staff or pupils. Some of this material, but not all, will contain personal data of individuals.

An obvious example of personal data would be the Single Central Record or a pupil file; however, a "record" of personal data could arise simply by holding an email on the school's systems.

Many, if not most, new and recent records will be created, received and stored electronically. Others (such as Certificates, Registers, or older records) will be original paper documents. The format of the record is less important than its contents and the purpose for keeping it.

Digital records

Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data – or any large quantity of data – should as a minimum be password-protected and held on a limited number of devices only, with passwords provided on a need-to-know basis and regularly changed. Where 'cloud storage' is used, consider what data needs to be made available in this way. If personal information kept in this way is sensitive, or held in large quantities, digital encryption is advisable.

Emails (whether they are retained electronically or printed out as part of a paper file) are also "records" and may be particularly important: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, however, the format is secondary to the content and the purpose of keeping the document as a record.

It is also worth remembering that a digital document's original metadata may indicate the date of its creation, its author or the history of its changes: so it is important that this information is preserved.

Paper records

Paper records are most often damaged by damp or poor storage conditions; but as well as applying common sense (i.e. dry, cool, reasonable ventilation, no direct sunlight; avoid storing with metals, rubber or plastic which might deteriorate or damage the paper), security is also vital – especially if the materials contain legally or financially sensitive data, as well as personal data.

Under the forthcoming data protection legislation, paper records are only classed as personal data if held in a "relevant filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible, and thus searchable as a digital database might be. By way of example, an alphabetical personnel file split into marked dividers will likely fall under this category: but a merely chronological file of correspondence may well not.

However, when personal information is contained on print-outs taken from electronic files, this data has already been processed by the school and falls under the forthcoming data protection legislation. Remember: data protection legislation is only one consideration in retaining records, so it is preferable to keep paper documents ordered and accessible.

A note on "personal data"

Some records will contain information about individuals e.g. staff, pupils, consultants, parents, contractors – or indeed other individuals, whether they are a part of the school or some other third party (for example, another school). Particular legal requirements will therefore come into play.

That type of information is likely to amount to "personal data" for the purposes of the forthcoming data protection legislation and therefore be subject to data protection laws which *may*, in places, conflict with aspects of these 'document retention' guidelines. Neither the statutory time limits by which legal claims must be made, nor the precise stipulations of private contracts or governmental organisations (e.g. the Disclosure and Barring Service, the 'DBS'), were necessarily drawn up with data protection law in mind.

For example, the forthcoming data protection legislation requires that personal data is only retained for as long as necessary – that is, necessary for the specific lawful purpose (or purposes) it was acquired. This will of course vary and may be either shorter or longer than the suggested document retention period, according to context. This is a nuanced area which may therefore require tailored, specific advice on a case-by-case basis.

As a general rule, statutory legal duties – or the duty to report to safeguard vital interests – will 'trump' data protection concerns in the event of any contradiction. Certain personal data may legitimately need to be retained or disclosed subject to a private contractual duty (e.g. under a parent contract).

However, a higher standard would apply to the processing of "*sensitive* personal data". By way of example a contractual duty, or other legitimate interest of the school or third party, would not of itself justify the retention or sharing of sensitive personal data – but 'protection of vital interests' might. Sensitive personal data includes data relating to an individual in respect of their health, race, religion, sexual life, trade union membership, politics or any criminal proceedings, offences or allegations.

Archiving and the destruction or erasure of records

All staff should receive basic training in data management – issues such as security, recognising and handling sensitive personal data, safeguarding etc. Staff given specific responsibility for the management of records must have specific training and ensure, as a minimum, the following:

- That records – whether electronic or hard copy – are stored securely as above, including if possible with encryption, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable;
- That important records, and large or sensitive personal databases, are not taken home or – in respect of digital data – carried or kept on portable devices (whether CDs or data sticks, or mobiles and handheld electronic tablets) unless absolutely necessary, *in which case* it should be subject to a risk assessment and in line with an up-to-date IT use policy;

- That questions of back-up or migration are likewise approached in line with general school policy (such as professional storage solutions or IT systems) and not individual *ad hoc* action;

- That arrangements with external storage providers – whether physical or electronic (in any form, but most particularly "cloud-based" storage) – are supported by robust contractual arrangements providing for security and access;

- That reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and – in the case of personal data – necessary for the purposes for which it is held (and if so, that it is accurate and up-to-date); and

- That all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely – with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them.

This is particularly important in respect of the school's specific legal obligations under the forthcoming data protection legislation. However, they amount to common sense rules even where personal data is not directly involved.

A note on litigation

One consideration in whether it is necessary or desirable to keep records is possible future litigation. Generally speaking, a school will be better placed to deal with claims if it has a strong corporate memory – including adequate records to support its position, or a decision that was made.

Ideally, therefore, records would not be disposed of until the limitation period for bringing a claim has passed. For most contracts that will mean 6 years from any breach (or 12 years in case of, say, a witnessed deed), but the date to start counting from is the last day of the period under contract. Where there has been early termination, this will be the relevant date to apply (once the appeal process has been concluded): but for pupils, limitation periods will only apply from the age of 18 years.

The period of 6 years also applies to many claims outside contract (such as fraud, mistake or negligence). For discrimination cases it is usually only 3 months. In the case of personal injury, and some other negligence claims, it is 3 years. However, if the harm is only discovered later – e.g. 'latent' damage, or some unseen injury – then the timer only starts from the point of discovery: subject, in the case of latent property damage, to a 15-year backstop.

In some cases, the prompt may be the end of a calendar year, so for the purpose of this guidance a contingency is generally built in (e.g. 7 years where the statutory limitation is 6 years).

Finally, limitation periods may be disapplied altogether by courts in the case of certain crimes or associated breaches of care (e.g. historic abuse), whether a charge is brought by the police or a school is sued under a private claim. It is not always possible to try a case where the evidence is inadequate, including due to a lack of corporate memory (eg records and witnesses). However, as recent cases and IICSA (the Independent Inquiry into Child Sexual Abuse) have shown, authorities will expect to see a full and proper record and inferences may be drawn otherwise.

Often these records will comprise personal or sensitive personal data (e.g. health or criminal allegations). In such instances, even justifiable reasons to keep records for many years will need to be weighed against personal rights. Recent 'historic' cases in the field of child protection make a cautious approach to record retention advisable and, from a forthcoming data protection legislation perspective, make it easier for a school to justify retention for long periods – even the lifetime of a pupil. The most important steps a school can take to support such a policy are (a) having adequate policies explaining the approach, including notices in both staff and parent contracts; and (b) ensuring any long-term records worth keeping are kept very secure, accessible only by trained staff on a need-to-know basis.

Insurance documents will not be personal data and relevant historic policies need to be kept for as long as a claim might arise.

The risks of longer retention

Notwithstanding the legal grounds and (in some cases) imperatives to do so, the longer potentially relevant personal data is retained, and the more sensitive material is kept on file, the greater the administrative and storage burden on schools. This also increases the amount of material in respect of which schools must be accountable to data subjects (e.g. information requests, "right to be forgotten" requests), and the consequences of data security breaches become more serious.

Schools must take professional advice and decide for themselves where to draw the line in retaining data for these purposes: some may err on the side of caution and retain; others will apply a clear system for filleting pupil or personnel files, or indeed email folders, down to the information they think is likely to be relevant in the future. However, this is a decision that should always be made mindful of risk and knowledge of where historic incidents may have occurred or future complaints may arise.

It is also vitally important that all staff bear in mind, when creating documents and records of any sort (and particularly email), that at some point in the future those documents and records could be disclosed – whether as a result of litigation or investigation, or because of a subject access request. The watchwords of record-keeping are therefore accuracy, clarity, professionalism and objectivity.

A note on secure disposal of documents

For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Skips and 'regular' waste disposal will not be considered secure.

Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed.

Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information.

How to use the table of suggested retention periods

The table at the end of this guidance document has three main functions:

- it should help schools and staff identify the key types of document concerned.

- it should focus attention on any particular issues associated with those types of document.
- finally – and this needs to be emphasised – it acts as an outline guide only.

Note that, except where there is a specific statutory obligation to destroy records, it is misleading to present (or apply) any guidance as if it constitutes prescriptive time 'limits'. Figures given are not intended as a substitute to exercising thought and judgment, or take specific advice, depending on the circumstances.

Indeed, the essence of this guidance can be boiled down to the necessity of exercising thought and judgment – albeit that practical considerations mean that case-by-case 'pruning' of records may be impossible. It is accepted that sometimes a more systemic or broad-brush approach is necessary, which is where the table comes in.

TABLE OF SUGGESTED RETENTION PERIODS

Type of Record/Document	**Suggested [1] Retention Period**
SCHOOL-SPECIFIC RECORDS	
• Registration documents of School	Permanent (or until closure of the school)
• Attendance Register	6 years from last date of entry, then archive.
• Minutes of Governors' meetings	6 years from date of meeting
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS	***NB – this will generally be personal data***
• Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).
• Examination results (external or internal)	7 years from pupil leaving school
• Pupil file including: o Pupil reports o Pupil performance records o Pupil medical records	ALL: 25 years from date of birth (subject to where relevant to safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the pupil).
• Special educational needs records (*to be risk assessed individually*)	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)

<u>INDIVIDUAL PARENT RECORDS</u> • Contact details for parents and other next of kin, i.e. emergency contact details	***NB – this will generally be personal data*** Duration of pupil's time in school (potential to keep beyond if notified accordingly of change of lawful basis for processing personal data (please see below)
<u>INDIVIDUAL ALUMNI/PAST PARENT RECORDS</u> • Contact details for alumni/past parents • Communication records • Prospect research on alumni/past parents	***NB – this will generally be personal data*** Lifetime of alumni/past parent (subject to review of consent/legitimate interest)
<u>SAFEGUARDING</u> • Policies and procedures • DBS disclosure certificates (if held) • Accident / Incident reporting	***NB – please read notice at the top of this note*** Keep a permanent record of historic policies <u>No longer than 6 months</u> from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself. Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available. [2]

• Child Protection files	If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely. If low level concerns, with no multi-agency act – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).

CORPORATE RECORDS (where applicable)	**e.g. *where schools have trading arms***
• Certificates of Incorporation	Permanent (or until dissolution of the company)
• Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum – 10 years
• Shareholder resolutions	Minimum – 10 years
• Register of Members/Shareholders	Permanent (minimum 10 years for ex-members/shareholders)
• Annual reports	Minimum – 6 years
ACCOUNTING RECORDS [3]	
• Accounting records (*normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state*) [NB specific ambit to be advised by an accountancy expert]	Minimum – 3 years for private UK companies (except where still necessary for tax returns) Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place Internationally: can be up to 20 years depending on local legal/accountancy requirements
• Tax returns	Minimum – 6 years
• VAT returns	Minimum – 6 years
• Budget and internal financial reports	Minimum – 3 years

CONTRACTS AND AGREEMENTS	
• Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments*)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
• Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS	
• Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.
• Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
• IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS	***NB this will contain personal data***
• Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (but not DBS certificate itself: 6 months as above)
• Contracts of employment	7 years from effective date of end of contract
• Employee appraisals or reviews	Duration of employment plus minimum of 7 years
• Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims.
• Payroll, salary, maternity pay records	Minimum – 6 years
• Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme
• Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
• Immigration records	Minimum – 4 years
• Health records relating to employees	7 years from end of contract of employment

INSURANCE RECORDS	
• Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
• Correspondence related to claims/ renewals/ notification re: insurance	Minimum – 7 years
ENVIRONMENTAL, HEALTH & DATA	
• Maintenance logs	10 years from date of last entry
• Accidents to children [4]	25 years from birth (longer for safeguarding)
• Accident at work records (staff) [4]	Minimum – 4 years from date of accident, but review case-by-case where possible
• Staff use of hazardous substances [4]	Minimum – 7 years from end of date of use
• Risk assessments (carried out in respect of above) [4]	7 years from completion of relevant project, incident, event or activity.
• Data protection records documenting processing activity, data breaches	No limit: as long as up-to-date and relevant (as long as no personal data held)

FOOTNOTES:

1. General basis of suggestion:

   Some of these periods will be mandatory legal requirements (e.g. under the Companies Act 2006 or the Charities Act 2011), but in the majority of cases these decisions are up to the institution concerned. The suggestions will therefore be based on practical considerations for retention such as limitation periods for legal claims, and guidance from Courts, weighed against whether there is a reasonable argument in respect of data protection.

2. The High Court has found that a retention period of 35 years was within the bracket of legitimate approaches. It also found that it would be disproportionate for most organisations to conduct regular reviews, but at the time of writing the ICO (Information Commissioner's Office) still expects to see a responsible assessment policy (eg every 6 years) in place.

3. Retention period for tax purposes should always be made by reference to specific legal or accountancy advice.

4. Be aware that latent injuries can take years to manifest, and the limitation period for claims reflects this: so keep a note of all procedures as they were at the time, and keep a record that they were followed. Also keep the relevant insurance documents.

Subject Access

What is a "Subject Access Right" (SAR)?

Both the Data Protection Act 1998 (DPA) and, from 25 May 2018, the General Data Protection Regulation (GDPR) provide for a right enjoyed by all individuals – including parents, pupils, staff (past, present and prospective) – to know what personal data about them is being held and used by organisations (including schools), and broadly for what purpose, where it came from, and who else might receive it. This is subject to certain limitations and exemptions.

Please note that the SAR is not the same as a parent's statutory right to receive a copy of their child's educational record under the Education Act 1996, which is sometimes cited by parents but does not apply to independent schools.

Why should we be concerned?

The definition of personal data is wide and includes correspondence, emails, minutes, reports, results, databases, lists and expressions of opinion. Given that independent schools have close relationships with pupils and parents, a good deal of personal data of this kind will be accumulated over the career of a pupil. Usually, individuals are also entitled to a "permanent copy" of the personal data held. In practice, this involves considerable effort, and can sometimes result in delicate or embarrassing disclosures and difficult decisions around the application of appropriate exceptions. Only repetitious requests, without allowing a reasonable time since the previous SAR, can safely be ignored.

The SAR right is wide in scope and has no time limitation. Schools can expect to incur considerable time and costs in responding fully, and – from 25 May 2018 – will no longer be able to charge even a token fee, except in limited cases.

What are the formalities needed for making – or recognising – a valid SAR?

Very few: a SAR must be made in writing but does not have to mention the DPA or GDPR (or use any of the technical jargon of the law of personal data), provided it is clear the requester wishes to access information about themselves held by the school. It can be validly made to anyone in the organisation, including online, and the effect (and period for responding) is the same. Schools can however request any information reasonably required to confirm the identity or authority of the requester, or in order to locate the data sought (if this is not immediately obvious, with e.g. CCTV footage), before responding. Schools can ask requesters to use a specific "form" but cannot insist on this.

Informal requests may be very narrow, in which case the school can consider it on its own terms (rather than assume a full SAR) but still need to be mindful of the SAR rules, including to take care around the information of others.

Can a SAR be made on another's behalf?

Yes, provided the school is satisfied that the third party is genuinely acting on the individual's behalf – for example, by their solicitor, or a family member. Children have exactly the same rights to make a SAR as adults, and indeed strictly speaking those rights belong to the child (and not the parent). However, a person with parental responsibility would normally exercise those rights on behalf of a child too young to understand the nature of the request (usually meaning under twelves). A child of any age can also ask a parent or third party to make a SAR on their behalf.

If there is any doubt, it will always be reasonable to request a direct or signed "authority" from the individual (e.g. the pupil). It is good policy to do this as a matter of course with parental requests about secondary school age pupils.

What are the time limits for compliance?

GDPR requires a response within a calendar month, starting with the date on which the SAR is received (or the date on which the information referred to above is received, if later – though this should not be used to artificially extend the deadline). It is recommended that the school does not delay in starting the process, and keeps the requester informed. With GDPR, the response time is shorter than the 40 calendar days under the existing Data Protection Act of 1998, which itself has often proved very tight for larger requests.

It is not a serious contravention of the law to take longer, but it is a technical breach and may be used to criticise the school. In general, it is better to get the disclosure "right" than to hurry and risk failing to make proper redactions.

What needs to be searched? Can we be proportionate?

All electronic systems under the school's control, which may include personal devices or email accounts where used on school business (by e.g. peripatetic music teachers or governors), and any "filing system" as defined by the GDPR. There is some encouragement in recent case law to suggest searches may be subject to proportionate considerations and the GDPR suggests that "*manifestly unfounded or excessive*" requests can be ignored or fairly charged for.

Under the DPA, SARs included hard copy records only to the extent they were sufficiently well-organised to give easy access to specific information about an individual. The GDPR arguably tightens this rule, but we await ICO Guidance.

What information has to be disclosed?

A SAR only provides access to the individual's own "personal data". Case law suggests that this is widely defined to include anything that "relates to" an identifiable, living individual (which means it includes initials, nicknames, job titles and so on). All the same, it is worth remembering that the right only relates to personal data, not whole documents. An entire email chain will not always be personal data of someone mentioned in the subject line, for example.

Some requesters will expect full document disclosure of anything of interest to them but do be mindful that very often this may relate to their complaint without relating to them personally: it could be merely factual or procedural.

What if the information identifies other people?

Where personal data about the person making a SAR also constitutes "personal data" about another person (a "third party"), a data controller is not obliged to disclose this mixed data in response to a SAR unless either (a) the third party has consented or (b) it is "reasonable", taking into account all the relevant circumstances, to disclose without consent. Otherwise, factors will include the third party's views, any harm or distress that may come to them, and their expectations of confidentiality – but the data controller must disclose as much of the requester's personal data as they can without unreasonably identifying the third party. Schools need to be aware that [under the current draft Data Protection Bill] it will always be assumed reasonable to disclose where that other person is a social worker or education worker, which will include from 25 May 2018 teachers (and other staff) of an independent school.

Real care needs to be taken in this area, as disclosure of information which also relates to a third party may be undesirable and may even give rise to a breach of confidence or data protection towards that other person.

Are there any other exemptions to the Subject Access right?

Yes. For example, information may be exempt from disclosure if it:

- is *legally privileged* (but this is not always easy to argue in quasi-legal processes like school complaints;
- records the intentions of the school in *negotiations* with the individual making the SAR;

- consists of a *confidential reference* given by the school (though not currently confidential references received by the school – although this wording is more ambiguous under the draft DPA 2018);
- consists of *exam or test answers* or *exam results* before the allotted publication time;
- is held for purposes of *management planning* (e.g. redundancy planning);
- would prejudice the prevention and detection of *crime* if disclosed (e.g. in live investigations);
- might cause serious harm or distress in limited *social work* contexts.

What are the consequences of non-compliance with a SAR?

Data protection legislation is enforced by the Information Commissioner's Office (ICO) and the Courts. Individuals who are unsatisfied with an organisation's response to a SAR may complain to the ICO, which will generally investigate and (usually, having given the organisation a chance to state its case) give its view on whether the organisation has complied with the law. In some cases, the ICO may simply ask the organisation informally to re-consider, with no further consequences (though it will keep a record of the matter, which could have an impact on how future complaints are dealt with). Individuals may also make an application to court to enforce the request, which is at the court's discretion and is of course more expensive for all involved.

Formal enforcement action is rare, but if the ICO makes a recommendation (including to disclose), schools are well advised to comply to avoid the ICO using its stricter powers.

Is there any formality to disclosing the data?

Strictly, it does not matter how the data is delivered as long as it is intelligible to the requester – it could be compiled in a table or single document or scanned or photocopied from originals and sent digitally or by hard copy. In practice, care must be taken to ensure it is delivered securely (with effective redactions). The best way to effect safe delivery is by agreeing a time and method with the requester. Post, even by recorded delivery, is less secure than a courier – which in turn is less secure than collecting or delivering in person. Ordinary email is less secure than an encrypted transfer, and so on. The suitability of delivery will depend on the sensitivity, volume and nature of the data. CCTV may require careful thought and offering to show the person footage on-site may be safer than sending out copies.

GDPR sets out additional information about data and rights for inclusion in the cover letter with the data. Care must be taken to get this right, and use the letter to manage fairly the requester's expectations about what they are getting.

Where can we get more information?

The ICO has published extensive guidance on the Subject Access right and most recently updated its pre-GDPR "Subject Access Code of Practice". For further information, visit https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/).

Subject access requests

Does the school have a policy for processing subject access requests?	
Following the request how is it responded to?	

What is contained in the communication concerning data and what form does the communication take?	
Does the communication contain an explanation of the process and the grounds on which a request can be refused?	

Cyber Security

Read the “Guide for Small Charities” written by the NCSC.

Back up data – know where, how, when and what is being backed up.

Using the Cloud – read the NCSC Cloud Security Guidance.

Install and turn on anti-malware software.

Review your **cyber security** measures: see the NCSC and Cyber Aware government websites Control USB drives (and memory cards).

Switch on your firewall.

Mobile devices – switch on password protection, keep the device up to date.

Make sure lost or stolen devices can be tracked, locked or wiped.

Don’t connect to wi-fi hotspots.

General Data Protection Regulation (GDPR) Checklist – What Schools Need to Know and Do…….

Action	Take into Account	Completed (Yes/No)
Register with the ICO and pay the data protection fee	The legal requirement to register and notify your activities to the ICO on a central register will be abolished, but a provision in the Digital Economy Act means it will remain a legal requirement for data controllers to pay the ICO a data protection fee. These fees will be used to fund the ICO's data protection work. As now, any money the ICO receives in fines will be passed directly back to the Government. Please see the ICO's blog here.	
Identify a compliance lead within your school	Your school is unlikely to require the formal appointment of a 'Data Protection Officer' by law as it currently stands under GDPR but you will need someone within your school to take responsibility – whatever their job title. Data compliance is a Senior Leadership Team issue and involvement from the Head, Bursar, governing body as well as staff in IT, HR, marketing and development roles will be crucial to driving this forward and ensuring your school's compliance. It goes far beyond just the school's IT set-up.	
Read the Information Commissioner's (ICO) guidance	The ICO's 'Preparing for the GDPR: 12 steps to take now' is a **must** read, along with the checklist it has recently added to its self-assessment toolkit. Throughout this guide, we refer to specific sections of the ICO website to provide further support and guidance to support you in moving towards GDPR compliance.	
Conduct a data audit	Assessing the data your school holds and identifying its weak areas can be done using the ISBA's template data audit grid available here. Think about where your data comes from, whether individuals are aware of what personal data you hold and how you process this. Have you identified a lawful basis for processing personal data? Are your existing consents (particularly parental or alumni consents) valid under the new GDPR? If relying on legitimate interests have you carried out a legitimate interest test? or are you fulfilling a contractor or employment obligation?	
Review contracts and data sharing agreements where necessary	You will need to look at all your school contracts: parent and staff contracts (where certain consents are captured and your data collection forms too for pupils applying, joining and for alumni); third party contracts - certainly where there is a data security consideration such as IT services, hard copy and digital storage but you'll need to even review your contracts with cleaning contractors. You'll also need to review your school's data sharing agreements (look at where you're sharing data with third parties such as your school's alumni organisation, mailing houses or cloud host and consider whether you need specific data processing contracts).	

Review policies and procedures relating to data protection	Schools will need to adapt references to related documents, if separate, such as: • if they wish to have a separate data protection policy for staff; • IT policies: Acceptable Use and/or eSafety and/or Remote Working / Bring Your Own Device; Data Breach procedures; • Anti-Bullying and Safeguarding Policies (including where monitoring software is used, or where the school has adopted a policy for recording low-level concerns); • Retention of Records (you can see the ISBA's template and guidance note here); • Any policy on taking, storing and using images of children (see the ISBA's template policy here), or biometrics and/or CCTV (see the ISBA's template CCTV policy here); and • Data collection forms or consent forms and any associated privacy wording.	
Review and re-issue your Privacy Notice (s)	One of the core principles of the GDPR is "transparency", meaning an emphasis on how data controllers tell data subjects how they use their personal data, in clear and concise language. There are three things your school's privacy notice **must** include: • Where schools are relying on legitimate interests as a basis for processing, these must be individually listed as part of the Privacy Notice; • If there are new data subject rights that need to be notified to individuals; and • Privacy Notices aimed at children need to be in a language suitable for children of that age. Schools should provide the Privacy Notice to parents (and obtain an indication that they have read it) with the parent contract and/or acceptance form when accepting a place at the school (this would also apply to prospective parents/pupils). You can see the ISBA's template Privacy Notice here. Schools need to draw the policy to the attention of pupils directly, for example within the school rules or pupil handbook. When pupils leave, remind them of the Privacy Notice while collecting any relevant consents to stay in touch with them as Alumni. Schools should also: • Place an up-to-date version of the Privacy Notice on the school's website, suitably integrated with other policies (e.g. by hyperlinking). • Review and update the Privacy Notice annually, to ensure it still accurately reflects the school's use of personal data. • Re-issue the Privacy Notice to all those affected when substantial amends have been made.	

	• Provide copies of the Privacy Notice to all Data Subjects either before the school begins processing, or within a reasonable time (and not more than one (1) month) thereafter (this will include existing parents, pupils, staff, alumni, etc). • Consider related documents – e.g. if your school has a separate Privacy Notice for Alumni activity, whether or not via a legally separate organisation; or for other Trusts, Trading Companies or Associated Bodies. Please note that a school may be able to cover a group of related concerns within the same Privacy Notice, but this requires careful thought as to how data is collected and what individuals are told, papering up data sharing arrangements, and Privacy Impact Assessments (PIAs) – as well as how these facts are conveyed in Privacy Notice itself, identifying all those bodies it is intended to cover. The Privacy Notice will also need to be consistent with any references to confidentiality, parent/pupil rights and how personal data is used in the school's Parent Contract.	
Consider your lawful basis for processing personal data - get consents where necessary or carry out legitimate interest tests	The GDPR requires you to clearly state which lawful basis you are relying on to process personal data. From a pupil or current parent perspective, you are likely to be relying on contract whilst for alumni or past parents you are likely to be relying on legitimate interest or consent. With regards to consent, the GDPR sets a higher standard for consent, which must be freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent under the GDPR requires some form of clear affirmative action. The ICO says that silence, pre-ticked boxes or inactivity does not constitute consent. Consent must also be verifiable - this means that some form of record must be kept of how and when consent was given. It's important for schools to note that individuals have a right to withdraw consent at any time. It may not always be practical for your school to rely on consent. You can instead, use an alternative legal basis to consent, where processing is necessary for your school's legitimate interests. To show "compelling" legitimate interests as the legal basis for processing personal data, means your school needs to know (and tell people) why and how they are processing personal data from the outset and to include this in your privacy policies and other outward-facing wording. But be aware: the more intrusive the activity the harder it will be to rely on legitimate interests. and although flagged in the Privacy Notice, will need additional notification outside the Privacy Notice, or consent from the relevant individual to fully comply with GDPR. For example: **Direct Marketing**: Strict rules apply to "direct marketing" (which includes communications promoting the "aims and ideals" of the school or another organisation, as well as e.g. communications	

	about fundraising), especially where it is sent by electronic means (e.g. email or SMS). Schools are very likely to need consent from the intended recipient of any electronic direct marketing and fundraising, and then will need to rely on consent or legitimate interests for other forms of communications. For further information, -please see the section of this guide on development and alumni relations, or the ICO's guidance on direct marketing here. **Examination Results**: A school may need to separately inform pupils and parents (and provide an opportunity to raise any objections) where it intends to publish exam results other than on an anonymous basis (e.g. if released to the media or on a publicly accessible notice board). For further information, please see the ICO's guidance here on the publication of exam results. **Monitoring emails, internet and telephone usage**: Strict rules also apply to monitoring of pupil internet use, emails and calls (except where this is done on an anonymous basis, e.g. to monitor email or internet traffic within the school as a whole). In particular, the "interception" of communications (which will usually include. opening unread emails or listening to or recording calls) can only be done for narrow purposes unless both sender and recipient have consented. The ISBA's template Privacy Notice assumes that schools will cover these issues primarily in an IT: acceptable use policy, which is certainly best practice, but where (for example) legitimate interests is being relied upon then this will need to form part of the Privacy Notice. **Using Special Category Personal Data**: As well as flagging it in the Privacy Notice, schools may need explicit consent to hold and use this type of personal data – unless one of a number of narrow, situation specific conditions apply. In respect of biometrics in particular, the Protection of Freedoms Act 2012 introduced new rules governing the use of biometric information in schools (which now needs to be notified to parents and pupils, and parental consent obtained). **Unexpected or intrusive uses of images of pupils**: certain uses, such as CCTV or group school photography for use in the school's own "community" media (its magazines or intranet), can be covered off as part of contractual or legitimate interest grounds, if properly notified. However, other more intrusive uses, particularly in external media (website, press release, prospectus), may be better dealt with by consent: especially where a child is identified by name or especially prominently featured, or in swimming or games clothes. Please see the ISBA template policy on taking, storing and using images of children here for further information, but schools are encouraged to develop their own policy on this issue. This is not an exhaustive list, and schools are encouraged to consult ICO guidance, and where necessary take specialist legal	

	advice, on their wider data protection responsibilities and the lawful bases for processing personal data.	
Conduct Privacy Impact Assessments (PIAs) where appropriate	Your school should conduct a PIA before embarking on any new major projects or policy changes (say, a fundraising campaign, IT restructure or update to your privacy policy). This could be as simple as a meeting (properly minuted) or a short report, but key to GDPR compliance is to plan around privacy from the outset and evidence your school's decision-making process. For further information, please see the section of this guide on PIAs or the ICO's code of practice here.	
Review cyber security at your school	If the personal data which you are responsible for has been encrypted as a result of a cyber-attack and you are unable to restore that data then the ICO could be of the view that you have not taken appropriate measures to keep it secure and have therefore breached the Regulation. The National Cyber Security Centre has a useful '10 steps' guide available here and the Government has also published Cyber Essentials guidance here.	

The ISBA has produced a range of new and updated documentation to prepare schools for the implementation of GDPR. Many of these are linked in the content above but to view all the guidance produced please visit the ISBA reference library at: https://members.theisba.org.uk/reference-library.aspx