DATA PROTECTION REVIEW 2017: AUDIT GRID FOR ISBA (Farrer & Co, May 2017)

TYPE OF DATA	IS THIS SENSITIVE PERSONAL DATA?	SOURCE	IS INDIVIDUAL AWARE YOU HOLD THEIR DATA, AND WHY?	LEGAL BASIS FOR HOLDING DATA	WHAT DO YOU DO WITH THE DATA? AND – WHAT MIGHT YOU WANT TO USE DATA FOR?	DO YOU SHARE DATA WITH ANYONE ELSE?	HOW IS DATA HELD?	IS DATA EVER ARCHIVED / DESTROYED?	IS DATA EVER TRANSFERRED / USED OUTSIDE UK?	ANY SPECIFIC CONCERNS?
		Often individual him/herself, but not always	*And, if so, how?*	*If consent: attach / reference any form. What is the scope of that consent?*	*Obviously key – and for matching up against any consent/notification by the individual*	*For example : contractor (this may be as "data processor"), volunteer, consultant, social services, police, etc. – and PTA, alumni associations*	*Paper-based; electronic; what security standard applied?*			*Any thoughts not covered by other questions*
Employee / permanent staff personal details, including details of pay / remuneration and basic / contact information for family members *[elaborate a little what this consists of]*	Yes, potentially – for example recording mental and physical health details.	Employees (when first employed and/or updated via HR department from time to time?)	[Yes – via contract of employment / internal data protection policies? What about how disciplinary or health concerns etc. are recorded?]	[Consent via contract of employment / internal data protection policies; *are full details of your data use included?*] *[Legal exemptions for employers where they have specific duties or obligations]*	[Process it for [*employee welfare, appraisal, remuneration*] purposes in line with contract of employment and/or internal data protection policies?]	Yes, potentially – where required / necessary: (1) healthcare, social and welfare organisations; (2) trade associations; (3) employment / recruitment agencies; [in line with contract of employment / internal data protection policies?]	On internal CRM system? *[Is this segregated by country / entity in your co. group / otherwise?]* *[include more detail]*	[Yes – "archived" after [X] years, but still accessible] *[include more detail]*	[Yes – when players are on tour etc] *[include more detail]*	Very possible that some employees have signed different forms of contract and/or incorporating different data protection policies. *[include more detail]*
Consultant / contractor personal details, including pay / remuneration			External / public-facing privacy policy [*provide link*]							
Prospective pupils / parents										
Current students / pupils	Yes, potentially – for example recording mental and physical health details, safeguarding file.		[Student / Pupil Handbook, joining forms, parent contracts, general data collection forms, and related policies e.g. Privacy Policy]							
Alumni / ex-pupils / **ex-parents**	[unlikely for marketing uses – but perhaps for historic accident or safeguarding records]		[Previous versions of Student Handbook, leaving forms, parent contracts and policies and forms and other related policies] Bespoke privacy policy used by alumni group(s)? [*provide link*]	[Consider legal grounds for longer retention of safeguarding records, accident reports etc.] [consider legal grounds for marketing to alumni] [Consider PECR, Privacy & Electronic Communication Regulations - consent is needed for certain communication, i.e. e-mail, TPS, SMS]	e.g. do you conduct wealth screening? Will you send magazines / newsletters?	e.g. alumni association (if separate entity), mailhouse / printers, etc			e.g. storage of data on US cloud system, processing of data by US-based company, etc	
Parents / those with parental responsibility	[contact details / bank accounts but also emails / complaints]		Parent contracts and policies and forms. External / public-facing Privacy Policy [*link*]			e.g. other parents as part of PTA business				

[Other categories of data?]										

Please note: *this is a suggestion for conducting a preliminary information asset audit, and not a full compliance kit for the General Data Protection Regulation. Categories and text entries are likewise provided as suggestive only and this is not a substitute for seeking legal advice and/or appointing a compliance lead at your school.*

How to use this grid

This grid is not a complete “turn-key” solution for GDPR compliance and nor is it a substitute for tailored advice. Just as importantly, it is not intended as a substitute for serious thought and investigation. The rows and columns, and the sample text populating some of these grids, are suggestions not prescriptions: asking more questions is to be encouraged. Schools should take full ownership of the issue, with the compliance lead at your school reporting at a management and trustee level but getting buy-in from all staff. You should not hesitate to add to or refine the matrix where it seems appropriate or adds value. The grid may only be a starting-point that triggers ideas or a preferred different approach that suits your school, but it is intended to ask some of the necessary questions to set you on the road to 25 May 2018.

If you need further advice or guidance, either in how to use the grid or what to do when it is complete, please contact IDPE.