idpe
institute of development
professionals in education

What do you need to do if you suspect a data breach?

IDPE corporate partner Blackbaud discovered and stopped a ransomware attack on its systems in May. After discovering the attack, their Cyber Security team successfully prevented the cybercriminal from blocking system access and fully encrypting files; and ultimately expelled them from their system. Prior to locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from their hosting environment. The cybercriminal did not access credit card information or bank account information.

What should your school do if you suspect a data breach?

1. Assess the risk

Firstly, it is worth establishing whether in fact a data breach has occurred. If a data processor such as your database provider experiences a data breach, they have a duty under data protection legislation to inform the data controller (the school) of this incident, without undue delay. If you are aware of a data breach and have not been contacted by your data processor, it would still be prudent to check with your data processor whether data from your school has been involved.

From a schools' perspective, it is also important to consider who is the data controller? The school, your alumni association, the foundation? Or are there joint data controllers? This is important as it impacts who is responsible for assessing whether the breach should be reported and which individuals should potentially be notified.

2. Notify the ICO

Not all data breaches need to be reported to the ICO – it depends on whether the data breach is likely to result in a risk to individuals' rights. If your school decides to report the data breach to the ICO, this should be done without undue delay, where feasible no later than 72 hours after you became aware of it.

3. Notify your community

In some cases it may not be necessary to share information about a data breach with your community. Notification to the individuals whose data is involved needs to be considered, but under GDPR there is a higher threshold for this. You are only required to inform your community, where the breach is likely to result in a 'high risk' to individuals such as the sharing of bank details or special category data. However, it can sometimes be prudent to inform individuals even where the legal threshold has not been met, is it better for your school that it is seen to be transparent and proactive?

Current advice from the ICO is that if schools are aware of the recent Blackbaud data breach and think that this may have impacted their supporters' personal data, where applicable, they should be notifying individuals to make them aware of the situation. Otherwise they must maintain records documenting the rationale behind any decision they make not to inform individuals.

Every school communicates with their community in a different way, therefore consider the most appropriate way for your school to inform individuals who have potentially been impacted. For some this may be a public statement on your website, for others this may be a personal letter or e-mail explaining the circumstances of the breach – remember to offer your community a point of contact within the school to find out more if they are concerned.

Schools should provide an initial response to any individual who raises concerns with them, outlining whether an investigation is being conducted into the matter and any steps that have been put in place to mitigate risk. Individuals can be informed that Blackbaud has reported a data breach incident to the ICO.

4. Notify other relevant parties

Charity Commission
A report to the ICO would, for charities, also necessitate a serious incident report to the Charity Commission. Whilst there is no fixed deadline to report a serious incident to the Charity Commission, this should be done promptly.

Action Fraud
Cyber crime is any criminal act dealing with computers and networks, including a data breach, therefore it is important to consider whether you need to report the data breach to Action Fraud.

Insurers
As data breaches and cyber attacks are now part of the new norm, your school may have cyber liability insurance to protect and mitigate exposure to such risks.

Senior leadership
Finally, don’t forget to keep your senior leadership informed. Your governing body in particular are not only responsible for how much you fundraise but how you fundraise, and will need reassurance that the necessary steps have been taken to minimise risk as a result of the data breach.

5. Record the process

Each school affected by a third-party data breach, must carry out its own independent assessment to determine whether there has been a data breach of the data they hold. Even if you conclude that a data breach is low risk and that you do not need to notify the ICO, it is important to keep a record of the incident and what steps were taken.

6. Seek advice

If you are unsure whether there is a data breach or of the process you should follow around assessing risk and notifying the relevant bodies/individuals, then do seek legal advice.

Please note, Blackbaud have informed all organisations that have been affected by the recent ransomware attack. However, if you require any further information, please contact your Blackbaud Customer Success Manager or customersuccess@blackbaud.co.uk.

If your school is a Blackbaud customer and has been affected by this, you can join IDPE’s LinkedIn group and find out how others are responding.