Browne Jacobson

Mitigating the impact of school data breaches

11 March 2025 Claire Archibald and Dai Durbridge

The Information Commissioner's Office (**ICO**) has launched a new campaign urging organisations to recognise the real-world impact of data breaches and improve the way breaches are managed.

This campaign follows new figures published by the ICO, which revealed 55% of UK adults reported having had their data lost or stolen, with 30% of them experiencing emotional distress as a result. However, 25% said they received no support from the organisations responsible.

Schools hold vast amounts of highly personal and sensitive information about pupils, parents and members of staff and there can be devastating consequences for individuals involved if there is a data breach in a school.

Most data breaches in schools are relatively low level and any risk of harm arising from the breach is reduced by taking prompt, sensible steps to deal with the breach. However, this is not always the case. More serious breaches do occur in schools.

Serious school data breaches

This is consistently reflected the high volume of reports made to the ICO each year– photographs of looked-after children in their school uniform published online or in the local press, highly confidential safeguarding logs being displayed on electronic whiteboards in classrooms, addresses of families who have fled domestic abuse being disclosed to former partners, details of allegations a pupil made against a member of staff being circulated to all staff – these are all real examples of breaches that have occurred and have caused a huge amount of distress to the affected individuals.

As part of its campaign, the ICO has published further guidance on communicating with empathy after a data breach. In the guidance, the ICO asks organisations to step up and do better to recognise the importance of data breaches including:

- Quickly assessing the risks to individuals when there is a data breach, including reporting the incident to the ICO and affected individuals where appropriate.
- Acknowledge what has happened with the individuals affected by the breach. Be human and accessible in your communications with the individuals. Defensiveness is likely to further damage relationships.
- Share the ICO's guidance with individuals affected by a breach and direct affected individuals to appropriate external support organisations if required e.g. the NCSC for cyber-attack related breaches or where domestic abuse victims are at risk, organisations such as Refuge.

What can schools do better?

Schools should consider whether existing data breach procedures are sufficient and what improvements can be made to ensure that communications are empathetic and recognise the real risk of harm that has occurred, including making a swift apology and ensuring that victims are directed to appropriate support where necessary. Of course, schools should also be taking action to improve data protection compliance to avoid any harm occurring in the first place including:

- Ensuring good data protection compliance is demonstrated from your senior leadership team.
- Engaging with all staff about the importance of data protection on a regular basis. Training content should be updated regularly to include key issues learnt from publicised cases and the school's own data breaches and any near misses which have occurred.

- Monitoring data protection compliance – it is not enough to simply have data protection policies and procedures. Schools should have evidence of periodic checks (such as on records accuracy, staff awareness and walk arounds) to ensure policies are being complied with.
- Post-incident, work empathetically with staff to collectively learn lessons from the incident.
- Recording and then properly reviewing all suspected breaches and near misses so that schools can assess root causes, and areas of risk or patterns to avoid such incidents happening again.

Further information and support

We're here to help. We offer a range of expert support to help you ensure you to ensure data protection compliance for your school, including:

- Data protection support pack
- Expert-led CPD for Data Protection Officers
- Empower DPO mentoring programme
- Staff data protection and cybersecurity online compliance training
- Data Protection Office Helpline

Key contacts

Claire Archibald

Legal Director

claire.archibald@brownejacobson.com

+44 (0)330 045 1165

Dai Durbridge

Partner

dai.durbridge@brownejacobson.com

+44 (0)330 045 2105

Related expertise

Child protection and safeguarding in schools

Data protection and privacy

Data protection guidance for schools and trusts

Education law

HR services for schools and academies