

Reinvigorating data protection in schools

28 February 2025

Claire Archibald and Beth Paliga

Why schools need to consider re-energising their data protection programme

It has been a few years now since the flurry of activity by schools to ensure compliance in the wake of the GDPR. But a lot has changed in schools since then.

We had a rush to adopt cloud systems during the pandemic, a huge increase in the numbers of cyber-attacks on schools and a fundamental change in school operations, with newsletters being replaced with parental apps, learning being recorded on edtech platforms and, perhaps most significantly, an increase in the number of parental complaints and resultant subject access requests (SARs).

Add to that new risks of pupil and staff data being used to train artificial intelligence (AI) based systems and data protection concerns continue to grow in significance.

The Information Commissioner's Office (ICO) has made clear the regulatory focus for 2025 is to ensure that:

- Children's personal data is protected.
- SARs are handled correctly.
- Any AI or Biometric processing is risk assessed and data protection risks minimised.

Being more proactive

The Information Commissioner himself, John Edwards, recently wrote a public letter to all organisations, imploring them to be more proactive to prevent data breaches and more responsive when there is a breach. Schools are clearly within scope of this renewed focus.

This spotlight by the regulator was seen in the summer of 2024, when a school was publicly reprimanded by the ICO for failing to comply with the law when installing a facial recognition system in their canteen. They had failed to carry out a Data Protection Impact Assessment before installing the technology.

Schools who similarly adopt innovative technologies, such as biometric or AI projects, but fail to carry out vendor due diligence and data risk assessments run the risk of similar reprimands.

Failure to deal adequately with SARs

Other public authorities have been reprimanded for failure to deal adequately with SARs. The ICO has issued detailed advice on SAR management in schools, after carrying out a comprehensive review of practice in over 300 schools during 2020, but this has not been an area of significant improvement for many schools, despite receiving an increasing number in both volume and complexity.

School leadership and governance should ensure that updating and refreshing compliance processes are included for consideration within their improvement plans. Our series of articles takes these ICO messages and translates them into sensible advice that schools can act upon.

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 Officer Helpline](#)

Key contacts

Claire Archibald
Legal Director

claire.archibald@brownejacobson.com
+44 (0)330 045 1165

Bethany Paliga
Senior Associate

bethany.paliga@brownejacobson.com
+44 (0)330 045 1154

Related expertise

Child protection and safeguarding in schools

Data protection guidance for schools and trusts

Education law