GDPR FOR SCHOOLS

Processing SEND data under the GDPR

How does the GDPR affect the way schools gather, share and retain SEND information? **Jack Procter-Blain** outlines what you need to know.

Schools are expected to comply with the new General Data Protection Regulation (GDPR), ensuring that the information they process is kept secure at all times.

A school's processing of information pertaining to special educational needs and disabilities (SEND) should be consistent with its processing of other types of personal data. Your privacy notice is a good way to be transparent about how and why you use data, and SEND information is no exception.

What is SEND data?

SEND data would include:

- details of a child's special educational need or disability
- educational provision arrangements (e.g. individual education plan)
- medical information as relevant to a child's SEND
- details of ECHP annual reviews
- details of the services provided to support a child with SEND.

Lawful basis

The lawful basis for processing SEND data is that schools have a duty to comply with statutory obligations (as set out in the SEND Code of Practice), chiefly to provide appropriate care and support for pupils with SEND. Where the processing of data is necessary to comply with a statutory obligation, this is sufficient grounds for processing the data lawfully.

Retaining and sharing data

Under current regulations, SEND information falls into the category of information that, as part of a pupil's record, a primary school passes on to secondary schools by the start of the academic year. These files can be kept electronically or in hard copy. If a school passes on files by post, this should be done by recorded delivery.

As explained in the IRMS Information Management Toolkit for Schools, schools are advised to retain SEND information for at least 25 years from the date of birth of the pupil. This is so that, if a 'failure to provide a sufficient education' claim is brought against them, they would not be disadvantaged as a result of having destroyed personal data. This recommendation is unlikely to change under the GDPR.

Once a primary school has passed over a pupil's record to the receiving secondary school, and the transfer has been acknowledged, the primary school should not keep duplicate copies of any files – electronic or hard copy – unless there is a specific reason for doing so (such as ongoing legal action). It is not sufficient for a primary school to retain copies of information simply because 'it's what we've always done' – always ask 'Why do we need to keep this data?'

Creating a data retention policy will be a good way to set out the length of time for which you intend to retain different types of personal data, including SEND data.

Obtaining consent

If you have already made clear that the school's lawful basis for processing personal data is to serve legitimate interests, and such intention is made clear in the school's privacy notice, there will be few circumstances in which you will need to seek explicit parental or guardian consent in order to process SEND data.

For example, you will not need to obtain a parent's written consent before you share a child's data with trusted external bodies such as your local authority, or request exam access arrangements, as both are mandated in the Code of Practice.

Communicating with stakeholders

Schools are expected to work closely with parents, health and care services, and commission specialist services when necessary to providing for pupils with SEND. In complying with the GDPR, the onus is on schools to ensure technical safety at all times in the transferring of pupils' personal data.

Before continuing to share SEND data with third parties such as a speech therapy provider, the school would need the provider to confirm in writing that they are GDPR compliant and keep a record of this. This would apply to any third-party organisations that provide services on the school's behalf, such as:

- speech and language therapists
- educational psychologists
- occupational therapists
- outreach services
- Youth Offending Teams
- clinical commissioning groups (CCGs)
- child and adolescent mental health services (CAMHS)
- any other third-party organisations that provide services on the school's behalf.

After that it would be up to the school to decide the safest way to transfer the information. If the recipient is using a secure email address, it is not strictly necessary to use email encryption.

Conclusion

The processing of SEND information should be subject to the same precautions as other forms of personal data. Schools should only obtain, share and retain this data where there is a lawful basis to do so. Individuals should be aware of how their data is being used and why it is being kept.