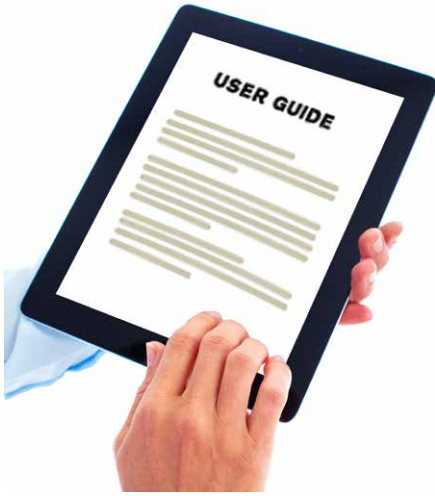


THE ESSENTIAL SCHOOL GUIDE TO GDPR

Published by Schools Week



The general data protection regulations (GDPR) aren't just for schools; they apply to every European organisation that handles personal data.

The aim of the new law is to return control to individuals by allowing them to request deletion or disclosure of their data and the onus is on organisations to provide evidence of their data storage activities.

There isn't any detailed specific guidance available for anybody (it would be impossible to document every possible scenario), so organisations must decide how best to apply the generic GDPR rules to themselves before the deadline of May 25.

So what are schools meant to do?

Firstly: don't panic! Most schools already keep records in line with some GDPR requirements. You'll just need to set some time aside to ensure you're meeting the rest of them.

The Information Commissioner's Office (ICO) is the official authority on GDPR in the UK. It says there are 12 steps to compliancy. Let's see how schools can approach them:

GDPR awareness

Engage with your local governing body, the senior leadership team, and trustees where appropriate, to make everyone aware of the deadline and what the requirements are for your school. Ensure

buy-in from the SLT for implementation of new policies, processes and procedures – as well as all staff.

Information you hold

For most schools, this will be the biggest challenge. Start by documenting your internal systems and identify where personal data is stored in both physical and virtual files. For digital documents, a good inventory tool such as NetSupport DNA will highlight these for you. Then create a list of the software used across the school (including teacher-selected apps) and delegate one to each staff member, to check they are GDPR compliant and what data they are extracting from your users.

Communicating privacy information

Upload an updated privacy policy to all school websites and circulate new versions of policies to affected staff. If you have the appropriate software, you can ensure these are seen and read via tracking and acknowledgement tools.

Individuals' rights

Ensure your policies reflect individuals' rights and, where appropriate, that unions are advised. Also, ensure you can handle scenarios such as a teacher requesting what information the school is holding about them. Devise procedures to find, delete and disclose the relevant data.

Subject access requests

Have a well-defined process for this and make it accessible for staff and parents on the school website. Ensure the process is manageable: only promise what you can deliver.

Lawful basis for processing personal data

It's actually very clear what data schools have and why they hold it, so this shouldn't be an area of huge concern. Schools should, however, check the ICO guidance on this to verify everything is covered.

Consent – is yours up to date?

Ensure the consent obtained from staff and parents meets the GDPR standard.

But, most importantly, keep a record of all of them.

Children: age verification and consent

Most schools already have systems in place to record these. If yours doesn't (which is highly unlikely), you'll need to address this.

Data protection officers

This is still a grey area, and especially difficult for smaller schools, as the DPO needs to be one step removed from the staff and students so they can process data impartially – and few local authorities can provide money to fill the role externally. Discuss this with SLT, governors or other schools who may be able help. For MATs, a suitably qualified or informed trustee may be a practical solution.

Data breaches

A data breach can mean anything from staff leaving a memory stick in a PC overnight, to leaving an unlocked device on a train. Firstly, make sure all staff are aware of the requirement to report any breach, regardless of size, to your appointed data protection officer within 72 hours. Secondly, track and record data breaches, perhaps via a spreadsheet or a software tool. Provided that the breach is recorded and schools can show evidence data wasn't accessed, they will avoid fines.

'Data Protection by Design' and 'Data Protection Impact Assessments'

Refer to the ICO's guidance on Data Protection by Design and Data Protection Impact Assessments and ensure key stakeholders are suitably trained and informed.

International

If you operate in the EU, ensure the same rules apply as in your UK organisation.

Remember: evidence is key and preparation now will set you up for the future, as the GDPR is an ongoing requirement. Start now, and you'll be on your way to becoming a GDPR-compliant school.