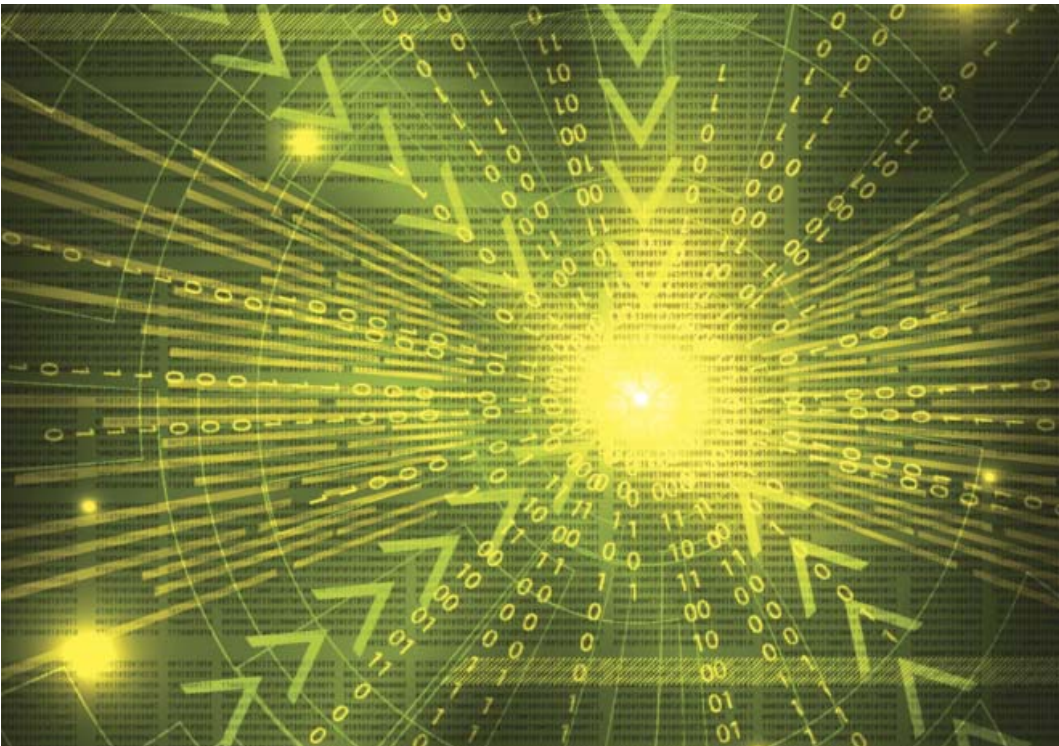
Getting ready for GDPR

A guide to the General Data Protection Regulation



The General Data Protection Regulation

Wherever information is stored, individuals and organisations need to be mindful of the importance of data security and privacy.

The Data Protection Act 1998 provides a legal framework of responsibilities on organisations (including schools and colleges) and employers, and rights for individuals (including teachers) with regard to ensuring privacy and confidentiality.

From 25 May 2018, the Data Protection Act (DPA) will be replaced by the General Data Protection Regulation (GDPR). These new EU regulations are intended to strengthen and unify the safety and security of all data held within organisations, including schools and colleges.

The GDPR will fundamentally change the way schools and colleges manage data and information and will bring increased responsibility to ensure all data is managed in the right way.

The GDPR does not prescribe how teachers should abide by the principles. However, what is clear is that a transparent e-safety policy is vital to ensure all key stakeholders know what they need to do to remain compliant.

Wherever members encounter any issues or have concerns about the use of personal data, they should contact the NASUWT for help and advice.

Introduction

Many of the General Data Protection Regulation (GDPR) concepts and principles are the same as under the Data Protection Act (DPA 1998) requirements. However, there are new elements and significant enhancements, so schools and colleges will have to do some things for the first time and some things differently.

The GDPR places greater emphasis on the documentation that schools and colleges must keep to demonstrate their accountability.

It will also require schools and colleges to review how they manage data protection.

This guidance highlights the initial steps school and college leaders should take to prepare for the GDPR which will apply from 25 May 2018.

Awareness of the regulation

Implementing the GDPR could have significant implications, especially for larger and more complex organisations, and compliance may be difficult if preparations are left until the last minute.

Designated Data Protection Officer

All maintained schools are required formally to designate a Data Protection Officer (DPO) who should lead this process. If schools and colleges have yet to appoint or designate responsibility for data protection, it is recommended that this is done as soon as practicable because the GDPR will impose significant additional compliance requirements. For some schools or colleges (i.e. maintained and most likely academies) the designation of a DPO will become a mandatory requirement in any event.

The role of DPO is a specific technical and administrative position. It requires no knowledge of teaching and there is no requirement for teachers to undertake any element of this role. If NASUWT members are asked to take on additional tasks because of the GDPR or data protection, they should contact the NASUWT immediately.

Information held by the school or college

Schools and colleges must document the personal data that is held, where it came from and who it is shared with. It may be necessary to organise an information audit across the school or college in connection with the implementation of the GDPR.

The GDPR requires a school or college to maintain records of its processing activities. For example, if inaccurate personal data is held and shared with another organisation, the other organisation will have to be informed about the inaccuracy so it can correct its own records. Schools and colleges will not be able to do this unless a record of personal data is held, showing where it came from and who it is shared with. The DPO will be responsible for supporting the school or college to achieve compliance in this area.

Data controllers will have to demonstrate their compliance and prove that they are taking data protection seriously by implementing a range of accountability measures. These are explained below.

1. Privacy Impact Assessments

The GDPR will expect some Privacy Impact Assessments (PIAs) to be undertaken. PIAs require schools and colleges to document:

- what kind of personal information will be collected;
- how it is collected, used, transmitted and stored;
- how and why it can be shared; and
- how it is protected from inappropriate disclosure at each stage.

2. Pseudonymisation

This term refers to the technique of processing personal data so that it can no longer be attributed to a particular data subject without cross-referencing it with further information. The further information must be kept separate and subject to enhanced security measures to ensure that the data subject cannot be identified.

3. Data protection audits

Schools and colleges should review and document the personal data they hold, identify the source and who it is shared with.

Data protection audits are used to map how personal data enters and leaves school and colleges and can be used to measure the degree to which the school or college complies with the law and identify 'red flags' which require urgent attention.

4. Data protection policy reviews

The GDPR will mean that schools and colleges will need to review their policies, particularly those relating to data protection. Data protection policies for pupils and parents should already explain an individual's legal rights and how those rights can be exercised. Because the GDPR amends those rights, school and college policies will also have to be amended.

Any policies also intended to be read by children will have to be explained in clear non-technical language and in a way that can be easily accessed and readily understood by the intended audience.

5. Staff data protection training

Schools and colleges will continue to be subject to an obligation to take steps to keep personal data secure. The provision of staff data protection training will continue to be expected. Schools and colleges will need to ensure that new staff receive data protection training before they have access to personal data and that existing staff receive regular refresher training.

Schools will be criticised and potentially liable if they have failed to ensure that all staff who handle personal data have received data protection training.

Communicating privacy information

Schools and colleges should review current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

GDPR requires schools and colleges to provide additional information to individuals about how their data is used.

Schools and colleges are already legally required to provide information to individuals (including staff, pupils and parents) about how their personal data is collected, stored and used. This is commonly provided through a privacy notice. GDPR expands the list of information which has to be provided to individuals. Some information has to be communicated in all cases (mandatory privacy notice information) whilst certain information is provided in specific cases (e.g.

if the school or college intends to process the personal data for different purposes than those that existed at the time of collection). Notwithstanding the volume of information that now needs to be included in a privacy notice, schools and colleges will be expected to provide this in a concise, transparent, intelligible and easily accessible way.

Information that schools and colleges will be expected to provide will include:

- identity and contact details for the data controller (school or college);
- the purpose and legal basis of processing personal data;
- with whom the personal data is shared;
- how data is protected when transferred outside the EU;
- length and criteria for retention of data;
- full legal rights of individual data subjects;
- right to complain.

Legal grounds for processing personal data

GDPR sets out conditions that must be met for the processing of personal data to be lawful.

Personal data may be processed:

1. with consent;
2. where the processing is necessary for a contract; or
3. where the processing is necessary for compliance with a legal obligation.

GDPR requires schools and colleges to publish the legal grounds for processing personal data and, if necessary, explain it to staff, pupils and parents.

For example, it is likely that the legal ground for processing pupil or staff images for identification purposes (i.e. Information Management Systems or for use on identification badges) will be because the processing is ***necessary***. In contrast, the legal ground for using pupil or staff images for school or college marketing and on the school/college website will be with ***consent***.

Some individuals' rights will depend on the legal basis for processing personal data. For example, individuals will have a stronger right to have their data deleted where consent is used as the legal basis for processing.

Schools and colleges must explain the legal grounds for processing personal data in a privacy notice or when answering a subject access request.

Consent

GDPR requires that schools/colleges must obtain consent prior to processing data in relation to staff, pupils or parents. To meet the GDPR requirements regarding consent, personal data must meet the following tests:

- **freely given:** The consent must be freely given and capable of being withdrawn at any time. It must be as easy for an individual to withdraw their consent as it was to provide it in the first place;
- **specific:** Separate consents must be obtained for different processing operations. Under GDPR there is a presumption that consents should be separable from other written agreements;
- **fully informed:** Schools should clearly communicate to individuals what they are consenting to and of their right to withdraw consent;

- **consent must be unambiguous and be a positive indication of agreement:** consent will no longer be presumed or inferred from silence, inactivity or pre-ticked boxes.

Schools and colleges are not required to automatically refresh all existing consents in preparation for the GDPR.

Schools and colleges should review how they gather, record and manage consent and whether any changes are needed.

Schools and colleges must have simple ways for people to withdraw consent.

Individuals' rights

The legal rights that individuals have under GDPR include the right to:

- **access data held about you**;
- **have inaccuracies about you corrected**;
- **have information held about you erased ('right to be forgotten')**;
- **stop direct marketing**;
- **prevent automated decision-making and profiling**;
- **data portability** (schools and colleges will have to provide requested information electronically and in a commonly used machine-readable format).

The right to data portability is new. It applies:

- to personal data an individual has provided to a school or college;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

Right of subject access

The GDPR will allow individuals to ask the school or college to give them a copy of their personal data together with other information about how it is being processed; this is called a Subject Access Request (SAR).

Under GDPR, the rules for handling SARs will change.

- Information must be provided for free in most (but not all) cases.
- Manifestly unfounded or excessive requests can be charged for or refused.
- The deadline for processing of information is reduced from 40 calendar days to 'within 1 month'. This deadline can be extended in certain cases.
- Additional information must be supplied, e.g. the school and college data retention periods and the right to have inaccurate data corrected.
- If a school or college wishes to refuse a SAR, it will need to have policies and procedures in place and demonstrate why it has refused a request.

Personal data breaches

Schools and colleges will have to adopt internal procedures for detecting, reporting and investigating a personal data breach.

The GDPR introduces mandatory breach notification to the Data Protection Authority, Information Commissioner's Office (ICO) and, in some cases, affected individuals. Breaches which are likely to result in an individual suffering damage must be reported, e.g. breaches that could result in identity theft or where an individual's confidentiality has been breached. Schools and colleges must have systems in place to detect and investigate all breaches and maintain an internal breach register.

Where schools and colleges detect a breach which is subject to mandatory reporting rules, it must be reported no later than 72 hours after becoming aware of it.

Where a breach has to be reported to affected individuals, this must be done without 'undue delay'.

Non-compliance can lead to administrative fines of up to £8,847,500 or 2% of annual turnover.

Children's Rights

The GDPR identifies children as 'vulnerable individuals' deserving of 'special protection'.

The GDPR introduces some child-specific provisions, most notably in the context of legal notices and the legal grounds for processing children's data.

All schools and colleges will need to address the new requirements when writing notices which must be child-friendly.

The main provision is that where services are offered directly to children aged under 16, parental consent will be required.

The school or college will be required to make reasonable efforts to verify that appropriate consent has been provided.

The NASUWT is the only union that is pursuing industrial action to protect teachers and headteachers from excessive workload associated with the use of data management and information processing systems.

The DPO will be responsible for supporting the school or college to achieve compliance with the GDPR. It is not expected that this should impact teacher workload, and if members are being expected to undertake administrative activities in relation to the GDPR, they should contact the NASUWT immediately.

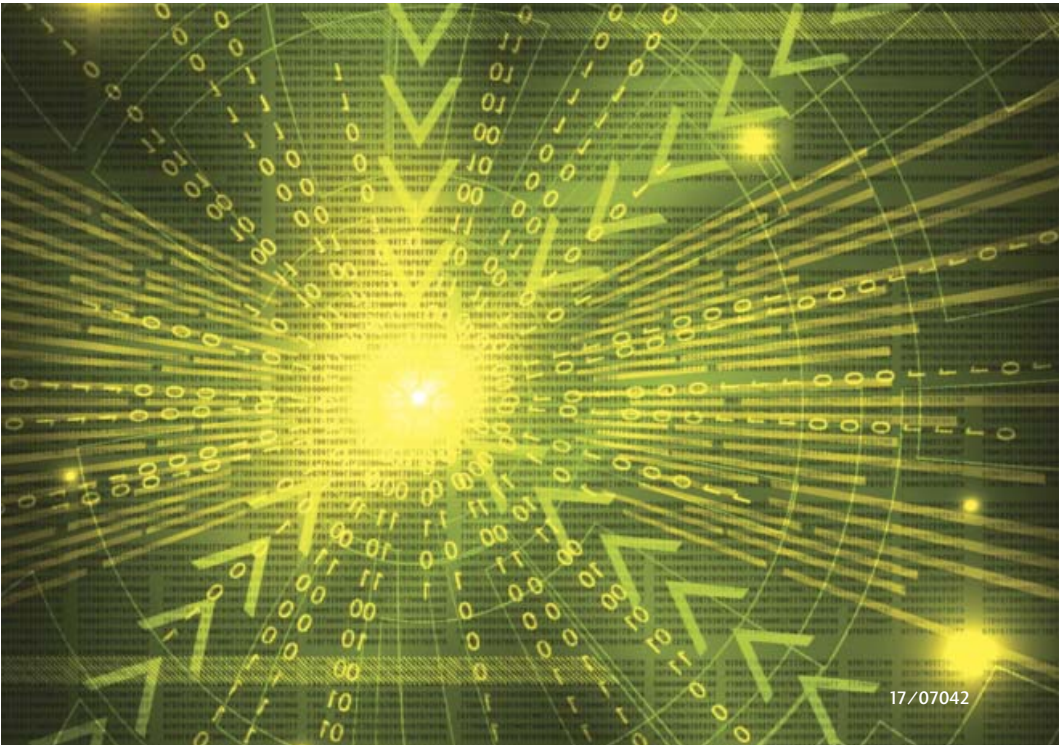
Because the GDPR amends existing data rights, existing school and college policies will also have to be amended. The NASUWT would expect to be consulted by employers on any changes to school or college policy on data protection in relation to staff.

Wherever members encounter any issue or have concerns about the use of personal data, they should contact the NASUWT for help and advice.

03330 145550
advice@mail.nasuwt.org.uk
www.nasuwt.org.uk

NASUWT
The Teachers' Union

Tel: 03330 145550
Email: advice@mail.nasuwt.org.uk
Website: www.nasuwt.org.uk



17/07042