General Data Protection Regulations (GDPR)

What is the GDPR?

Originally enacted in 2016, the EU General Data protection Regulations (GDPS) come into force on 25 May 2018 and will affect schools.

The United Kingdom's withdrawal from the European Union does not affect the introduction of the GDPR at all.

The Information Commissioners Office (ICO) has prepared a useful guide for schools with clear advice and how to prepare for the regulations. A full copy of the guide can be found at:

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

The GDPR is a set of guidelines for the collection and processing of personal information of individuals within the EU; it will come into effect in the UK from 25 May 2018, taking the place of the DPA, and will not be affected by the UK's decision to leave the EU.

The GDPR applies to the following:

- **Data subject** – an individual who is the subject of personal data
- **Data controller** – a person who determines the purposes and way that data is processed (The School or MAT)
- **Data processor** – any person who processes data on behalf of the data controller

Personal data

Under the GDPR, personal data has a more detailed definition; information such as online identifiers (e.g. IP addresses) will now be classed as personal data. The regulations apply to both automated personal data and manual filing systems where personal data can be accessed.
Personal data must be:

- Processed lawfully and fairly.
- Collected for specified and legitimate purposes.
- Accurate and relevant.
- Kept in a form which permits the identification of data subjects for no longer than is necessary.
- Processed in a way that ensures full security of the data

Schools data is regulated by GDPR.

Lawful reason for processing data

The school must have a lawful reason for processing data. For the vast majority of information the school processes (Pupil details, Assessment, Safeguarding, SEND) the school will not need to seek permission to do this as it has a legal reason for collecting the data. For some non-core activities e.g. use of images in promotional materials consent must be given.

When consent is required it **must** be:

- Freely given, specific, informed, an unambiguous indication of an individual's wishes, a form of firm confirmation or positive opt-in, such as ticking boxes on a webpage.

Consent **cannot** be obtained from the following:

- Silence, pre-ticked boxes or inactivity

Under GDPR it will not be acceptable for schools to assume that no objection implies consent.

Individuals' rights

The GDPR has created new rights for individuals, whilst strengthening some that existed under the DPA; these rights are:

1. **The right to be informed**
   This includes the schools obligation to provide fair processing information, usually in the form of a privacy notice. The DfE have published a template – DCC will provide additional information. *(This applies to all data – that for which consent is required and data which schools must legally process).*

2. **The right of access**
   Where an individual has requested access to their personal data (known as a Subject Access request) the school must provide a copy of the information free of charge; however, if the request is manifestly unfounded or excessive, a reasonable fee may be charged.

   This information must be provided within one month of the request. If you refuse a request, you must tell the individual why and inform them of their right to complain to the supervisory authority.

3. **The right to rectification**
   All individuals are entitled to request their personal data to be rectified if it is inaccurate or incomplete.

   Requests must be responded to within one month from the date the request was received, or extended to two months if the request is complex.

4. **The right to erasure**
   This enables an individual to request the removal of personal data where it is no longer required for the process it was originally obtained for.

   Requests can be refused for reasons such as compliance with a legal obligation or to exercise the right of freedom of expression and information, this will probably apply to some school data – seek legal advice. SIMS are currently working on modules to make some of this possible.

5. **The right to restrict processing**

Individuals have the right to 'block' or suppress the processing of personal data. In an instance where processing is restricted, you may store the personal data; however, you may not process it any further.

Circumstances that will require the restriction of processing personal data include:

- When an individual has challenged the accuracy of the personal data – processing should be restricted until accuracy is verified.
- When an individual has objected to processing that had been necessary for the purpose of legitimate interests, you may consider whether your organisation's legitimate grounds override this.
- If the processing is unlawful and the individual has requested restriction instead of erasure.
- If your organisation no longer requires the data, but the data is needed by the individual to defend or carry out a legal claim.

Individuals must be informed when you lift a restriction on processing.

6. The right to data portability

This allows individuals to obtain and reuse their personal data for their own purposes; they are able to move, copy or transfer personal data easily, in a safe and secure way. Schools routinely transfer data when a child moves.

7. The right to object

Individuals may object to processing based on legitimate interests. Organisations must stop the processing unless they can provide legitimate grounds that would override the interests, rights and freedoms of the individual, or if the processing is for the exercise or defence of a legal claim.

Individuals may also object to having their data processed for direct marketing purposes. In both instances mentioned here, individuals must be informed of their rights in your privacy notice, and at the first point of contact. This is unlikely to apply to schools.

8. Rights to automated decision-making and profiling

The GDPR ensures that individuals' data is protected against the risk that a potentially damaging decision is made without human intervention. Rights to automated decision-making and profiling will not be used in school settings.

Processing pupils' data

The GDPR has introduced new provisions that are intended to enhance the protection of children's personal data. Where services are offered directly to a child, privacy notices must be written in a clear, age-appropriate way.

The GDPR states that a pupil under the age of 13 (Law still in parliament) cannot give consent for themselves – consent must be obtained from a person holding 'parental responsibility'.

Consent from a parent or guardian is not required where the processing is related to preventative or counselling services that are offered directly to a pupil.

Accountability and governance

Under the GDPR, you are expected to put comprehensive, but proportionate, governance measures in place that minimise the risk of data breaches. An organisation can demonstrate its compliance with the new accountability principle in the following ways:

- Implementing internal data protection policies, such as staff training or reviews of internal HR policies
- Maintaining relevant documentation and processing activities
- Appointing a DPO
- Implementing measures that meet the principles of data protection by default, including data minimisation and transparency
- Using data protection impact assessments (DPIAs) where appropriate

DPIAs are tools that can help organisations identify the most effective way to comply with data protection obligations and meet individual's expectations of privacy.

DPIAs can address more than one project and should contain:

- A description of the processing operations and the purposes.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures currently in place to address risk.

If your organisation has less than 250 employees, you must maintain records of activities related to higher risk processing, such as:

- Processing personal data that could result in a risk to the rights and freedoms of an individual.
- Processing of special categories of data or criminal convictions and offences.

If your organisation has more than 250 employees, you must maintain additional internal records of your processing activities.

Examples of the information that must be recorded include the name and details of your organisation (including information of other controllers and the DPO), the purposes of processing and the categories of the recipients of personal data.

Data Protection Officer (DPO)

Under the GDPR, a DPO must be appointed for a school, or across a MAT

Organisations may appoint a single DPO to act for a group of schools, or swop DPO between schools so one business manager acts as a DPO for a neighbouring school. Examples of the DPO's tasks include informing and advising the organisation and its employees about their obligations to comply with the GDPR, and monitoring the organisation's compliance.

A DPO is not required to have any specific qualifications; however, they should have professional experience and knowledge of data protection law. Headteachers or SBMs should not be appointed due to conflict of interests.

Special Category Data

There are some types of data that need to be treated more carefully as a breach will have more serious consequences. These will relate to medical, safeguarding,

religious, some employment information and data relating to ethnicity or sexuality. Schools will need to protect this information more carefully.

Information Asset Log

Schools need to know what data they keep and where it is stored and who has access. When data is processed by a third party (iTrack, Lexia, Parent Pay etc.) schools should have information from that third party to show that they process data on behalf of the school and to confirm that the schools data is being safely processed. Many organisations are now producing information explaining how they are GDPR compliant.

Data Retention

Schools should have a system for ensuring data is not kept for longer than required. The Schools Record Management Toolkit http://irms.org.uk/page/SchoolsToolkit) has useful information about data retention periods.

Data Breaches

Organisations will be required to report data breaches that are likely to result in a risk to the rights and freedoms of individuals to the relevant supervisory authority and, if necessary, the individuals affected.

A breach notification must contain:

- The nature of the personal data breach, including the categories and approximate number of individuals, as well as personal data records concerned.
- The name and contact details of the DPO or other contact point where more information can be obtained.
- A description of the likely consequences.
- A description of the measures taken, or proposed to be taken, to deal with the breach.

The relevant supervisory authority (e.g. the ICO) must be notified of the breach within **72 hours** of the organisation becoming aware of it. If the breach is serious enough to require notification to the public, it is the responsibility of the organisation to do so without delay. Failure to report the breach could result in a fine.

To prepare for breach reporting, you should ensure that staff understand what a data breach would be and that you have an internal breach reporting procedure in place. Due to the tight timescales with breach reporting, it is vital that you have strong breach detection, investigation and internal reporting procedures in place.