General Data Protection Regulation (GDPR)

On 25 May 2018 a new data protection law will come into force across all of Europe – the GDPR (General Data Protection Regulation). Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA). However, there are new elements and significant enhancements.

The GDPR contains principles for good management of personal data, rather than specific rules on how you must do things. It doesn't set out record retention periods or particular security measures that need to be put in place.

Main principles

The GDPR sets out the key principles **that all personal data must be processed in line with.**

- **Data must be:** processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected

There are also **stronger rights for individuals** regarding their own data.

- **The individual's rights include:** to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all

The main changes are:

- Schools must appoint a data protection officer, who will advise on compliance with the GDPR and other relevant data protection law
- Privacy notices must be in clear and plain language and include some extra information – the school's 'legal basis' for processing, the individual's rights in relation to their own data
- Schools will only have a month to comply with subject access requests, and (in most cases) can't charge
- Where the school needs an individual's consent to process data, this consent must be freely given, specific, informed and unambiguous
- There are new, special protections for children's data
- The Information Commissioner's Office must be notified within 72 hours of a data breach
- Organisations will have to demonstrate how they comply with the new law
- Schools will need to carry out a data protection impact assessment when considering using data in new ways, or implementing new technology to monitor pupils
- Higher fines for data breaches – up to 20 million euros. However, the Information Commissioners Office has said it will use it powers "proportionately and judiciously"

Personal data is information that relates to an identifiable living individual that is processed as data. Processing amounts to collecting, using, disclosing, retaining or disposing of information. The data protection principles apply to all information held electronically or in structured paper files. The principles also extend to educational records – the names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

Preparing for the GDPR

The DfE has produced a Data Protection Toolkit, which sets out nine steps to prepare for GDPR. The nine steps are:

1. Raising awareness

In schools, the key people are those who have responsibility for managing or dealing with personal data. Depending on how your school is organised, this will probably be senior leaders, IT technicians, data managers and potentially administrative staff. It will also include governors/trustees, who are likely to have overall responsibility for your compliance with data protection law.

2. Creating a high level data map

Work out what personal data you hold, where it came from, and who you share it with. Start by documenting where the riskiest and most sensitive data is. This is information which could cause detriment to an individual if the data was lost or seen by someone who shouldn't see it (for example, cause them distress, embarrassment or to suffer some form of discrimination).

In schools the riskiest data is usually:

- Confidential information on staff and pupil records
- Safeguarding information
- Information that is taken away from the school premises, such as information on laptops, personal electronic devices or paper records that are transported from one place to another

Your governing board's working practices will need to be considered too. Think about:

- What documents governors have access to and whether these contain any personal data
- How governors get access to these documents
- Whether information is sent to personal email addresses
- Whether governors take information off the school site

Personal data may be stored in a wide range of places, including your IT systems, laptops, personal devices, paper records, USB sticks or other portable storage devices, email accounts, and staff members' homes.

3. Turn your data map into a data asset register

In simple terms, a data asset register is a long list of all the different data assets you have in your school, with some supplementary information about each of them. Different organisations will go down to different levels of detail here depending on their complexity and maturity. As a minimum, doing this for all assets that hold personal level data is required.

4. Documenting the reasons for processing data

Under the GDPR, there are 6 'lawful bases' (or reasons) that a school can use to justify why it needs to process data. Look at the personal data you hold and identify which lawful basis/bases applies to how you process the data. Then, document this and update your privacy notices to explain your lawful basis/bases.
Check that you seek, record and manage consent in accordance with the rules. An example of where you may need to seek consent is for the use of a child's picture on the school website. However, the school probably won't need to seek consent that often – there needs to have a lawful basis (legal reason) for processing personal data, and consent is just 1 of the 6 reasons. Only use consent where none of the other bases apply as the standard for getting consent is very high, and individuals can say no or withdraw it at any time.

5. Documenting how long you need to retain information

When preparing the GDPR Toolkit, it was found that there is "inconsistency in local practice in terms of data retention periods requested of schools, notably around safeguarding data. Follow your local best practice so long as it remains justifiable".
In Essex, schools tend to base their retention schedule on the one set out in the Information Management Toolkit. Your school should have a Records Management Policy which will refer to the retention of documents.

6. Reassurance and risks

Your processes need to:

- Include systems to verify individuals' ages and gather parental or guardian consent for any data processing activities
- Be communicated in clear and plain language – especially any processes that refer to children's data, so that a child can easily understand them

Minimisation is a key thing to think about:
Think about the minimum amount **of personal data** that is needed to get the job done. If an external consultant is coming in to look at progress of pupils in primary schools, then if month of birth or term of birth would do the job, there's no justification for passing on date of birth. Think also about the **minimum amount of people that need access to personal data.** People should only see the personal data they need to see to perform their role.

Your schools has procedures in place to detect, report and investigate personal data breaches. **If you think there might have been a data breach, report this to your Data Protection Officer.**

A data breach you need to report might involve:

- A non-anonymised dataset being published on the school website
  including the GCSE results of children eligible for the pupil premium
- Safeguarding information being made available to unauthorised people
- The theft of a school laptop containing non-encrypted personal data about pupils

7. Decide on your Data Protection Officer role

Schools need to appoint a data protection officer (DPO). This person must:

- Have an understanding of data protection law
- Report directly to the highest management level of the school
- Not have any conflicts of interest between their existing role and the DPO role (so, for example, the head of IT should not be the DPO as they are responsible for implementing the IT system, and the DPO will be responsible for checking the system's compliance with the GDPR)

8. Communicate with data subjects

Your privacy notices at the moment will probably say who you are, why you process information and what you do with it. By May 2018 you must have added information such as:

- Your legal basis for processing
- Notice of the individual's right to make a complaint to the ICO (as the 'supervisory authority')
- Notice of other rights in relation to access and correcting inaccurate data

The school has published a Privacy Notice for staff which sets out how your personal information is used by the school.

9. Operationalise Data Protection and keep it living

Ensure that data protection and risk management is a core and regular part of decision making and risk management practices within the school.
It is good practice to record and investigate every data breach, however small. An analogy here might be the 'accident log book'. Whilst a child grazing a knee may be minor in isolation, if each incident is reported and a trend around a piece of playground equipment is spotted, some remedial action might be appropriate. And so it is with data protection: if a particular system or process is identified as regularly having minor incidents by the Data Protection Officer, they and the school can mitigate the risk. They can only do this if a 'report it always' culture exists and is encouraged.

Safeguarding and GDPR

"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need". (Page 21 DfE Toolkit)

Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place".
"All data on the safeguarding file potentially forms part of an important story that may be needed retrospectively for many years. The elements of a pupil file (name, address) that are needed to identify children with certainty are needed to be retained along with those records [until at least 25 years old]". (Page 61 DfE Toolkit)

The school should have clear, practical policies and procedures on information governance for staff and governors, and should check that these are understood and followed.

These should include:

- Data Protection Policy
- Staff Code of Conduct – the Essex HR model includes use and control of data – *this has been updated in March 2018*
- Governors Code of Conduct
- Privacy notices for staff and parents/pupils
- Record Management Policy *(not mandatory, but good practice)*

Staff and governors need to know and understand

- What personal data they manage in school on a day to day basis
- How to manage, keep and dispose of data
- The school's procedures in relation to pupil records, email, social media, taking photos in schools, mobile technology and the school website
- When they are allowed to share information with others and how to make sure it is kept secure when shared.

This briefing paper relates to the introduction of the GDPR – to develop the staff understanding of data protection and information management, follow up with the additional 7-minute staff meetings:

- Information sharing
- Data management and Information security
- Data protection principles

Two other useful video clips for staff training

GDPRiS Training: GDPR Awareness for School Staff
https://www.youtube.com/watch?v=4yPxs4D9u_c

GDPR for schools – introduction to GDPR
https://www.youtube.com/watch?v=HevlI3zqc44

Additional guidance and further reading

- EPHA website – dedicated page https://essexprimaryheads.co.uk/info-and-documents/data-protection/
- DfE Data Protection: a toolkit for schools
- Data Protection Officer checklist (EPHA website)
- Individuals' rights – difference between Data Protection Act and GDPR (EPHA website)
- Information Commissioner's Office https://ico.org.uk/
- ICO Data Protection guide for schools
- Information Management Toolkit for Schools 2016
- Information sharing advice for safeguarding practitioners March 2015
- Essex Schools Infolink https://schools-secure.essex.gov.uk/data/information-governance/Pages/DataProtectionAct1998.aspx