The General Data Protection Regulation (GDPR) is nearly here but it doesn't end on 25th May. Compliance will need to be improved upon over time as schools and everyone else get to grips with the new rules and ways of working within the new data ecosystem. This isn't an exhaustive guide to becoming compliant but should give you a practical overview of some of the key considerations.

**Useful links:**
- DfE GDPR for Schools Video
- 'Talking with Staff on GDPR', DfE Blog

**Disclaimer:** This is an informative guide to GDPR using research from reputable sources, including the ICO and the DfE. This is not legal advice.

### Awareness and Culture

GDPR affects everyone in the school; for compliance to be in effect and the rights of all individuals in the school protected, a culture of data protection awareness needs to be established and maintained by all members of staff.

"All staff should be aware of what personal data actually is, what 'processing' means in the broadest form and what their duties in handling personal information are. They should be aware of the processes by which they are permitted to use that information, and be clear of the scope of the permitted usage of that data. They should be engaged with the risks around data getting into the wrong hands, and their responsibilities regarding responding to a data breach. The job roles that might warrant this level of training include catering staff, welfare supervisors, library staff, cleaners, first aiders etc."

**Source:** 'Data protection: a toolkit for schools', DfE, April 2018.

It's also worthwhile to note that awareness extends to students too; teachers and parents will need to continue to educate children on the importance of protecting their personal data and staying safe online.

**Useful links:**
- GDPR in Schools (GDPRIS) - [Awareness for All Staff](#)
- 'School Lesson Plans and Resources', ICO
- 'Posters, stickers and e-learning', ICO
The 6 Principles of the GDPR

1. Personal data shall be processed **lawfully, fairly and in a transparent manner** in relation to individuals;

2. Personal data shall be collected **for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. Personal data shall be **adequate, relevant and limited to what is necessary in relation to the purposes** for which they are processed;

4. Personal data shall be **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. Personal data shall be **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed**; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

6. Personal data shall be **processed in a manner that ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. ”

**Source:** The GDPR: Chapter II, Principles, Article 5, ‘Principles relating to processing of personal data of the GDPR’. Page 35.

Types of Data

**Business**
GDPR does not apply to business data since it isn't personal e.g. school name, school address, office@schoolname.sch.uk etc.

**Personal**
GDPR applies to personal data, which is any data at all that can identify a person e.g. names, email addresses, ID numbers etc. If in doubt the ICO's guide from the Data Protection Act still applies.

**Special category**
GDPR's classification of especially sensitive data that requires even more protection, since processing it may carry more risk of impacting upon an individual's rights and freedom. The GDPR defines this special category data as:

“personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation”

**Source:** The GDPR: Article 9, ‘Processing of special categories of personal data’. Page 38.

However, the DfE confirms there are additions to this definition:
“Within education, we do process some sensitive information about children that is not set out in the legislation as a ‘special category personal data’. Notably information about children’s services interactions, free school meal status, pupil premium eligibility, elements of special educational need information, safeguarding information and some behaviour data. We consider it best practice that when considering security and business processes about such data, that they are also treated with the same ‘high status’ as the special categories set out in Law.”


Difference between Controllers and Processors

A **controller** determines why and how personal data will be processed. A school itself as an organisation is the data controller, rather than a specific person.

A **processor** processes personal data on behalf of a controller. Schools will have a range of processors in the form of organisations and suppliers who process data in working with them.

“If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.”

Source: [Key Definitions](https://www.ico.org.uk/), The ICO.

Legal Bases for Processing

There are six legal bases for processing data and any data processor must have a valid lawful basis in order to process personal data in accordance with it. Data processors may use more than one for different types of data they process for different individuals. What basis or bases they are using should be clearly detailed in a Privacy Policy. The six bases are:

1. The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;

2. Processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

3. Processing is necessary for compliance with a **legal obligation** to which the controller is subject;

4. Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;

5. Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;

6. Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms.

Our GDPR Commitment & Work

At Satchel, we are working to ensure that we review all of our current processes and behaviours to ensure that we meet the updated regulations.

As part of our GDPR compliance work:

- Internal processes are continually being updated with the full support of our executive team.
- We are auditing both our on-site and cloud data management procedures to ensure we meet all regulations.
- We are ensuring that we facilitate control of personal data for all individuals whose data we hold.
- We have appointed a Data Protection Officer and GDPR project manager.
- All staff are being trained on any new processes that are implemented as part of becoming GDPR compliant.

Ensuring the safety and security of our users is of the utmost importance to us, and data protection and privacy is an integral part of this. We want all individuals who use our services to get the most out of them while having the peace of mind that we have their best interest at heart.

If you have any questions or comments surrounding this, please don't hesitate to send us an email to gdpr@teamsatchel.com and we'll get back to you as quickly as we can.

Full details are available on our GDPR Compliance page and Privacy Policy.