

The General Data Protection Regulation (GDPR) is a new data protection regulation that will apply in the UK from 25 May 2018. GDPR applies to 'controllers' and 'processors'. The definitions are broadly the same as under the Data Protection Act 1998, the controller says how and why personal data is processed and the processor processes data on behalf of the controller. **The school is the data controller.** **Anyone who processes data on behalf of our school is a data processor.**

GDPR applies to personal data. That is, any data that can be used to identify a person. For example, pupil records, governor records, contact lists, parents/carer records. **The person who the data is about is called the data subject.**

Under the GDPR, the data protection principles set out the main responsibilities for the school. These are that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals. There must be a recorded legal basis for processing the data, for example evidenced consent, or a legal obligation, part of a contract or the vital interests of the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The school cannot collect the data for one reason and then use it for another.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The school must only collect the information needed for the purpose we are using it and must not collect excess information just in case.
- The data must be kept accurate and up to date.
- The personal data must not be kept for longer than necessary. The data must have a retention period and then be deleted once that retention period has expired.
- Personal data must be held securely using appropriate technical or organisational measures to prevent unauthorised processing, accidental loss, destruction or damage.

Article 5(2) requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with the principles". The school must be able to demonstrate that it is complying with these data protection principles.
--