The PGS Storage and Retention of Records & Documents Policy (external)

The PGS Storage and Retention of Records and Documents Policy

Background

This policy has been drafted to comply with the UK General Data Protection Regulation (UK GDPR).

It recognises that the regulation does not fundamentally change the principles for length of document retention and that the principles of storage and retention remain related to relevance and purpose, as well as data security.

The key principles followed are as follows:

- All information held needs to be justifiable, by reference to its purpose
- The school will:
    - be transparent and accountable as to what it holds
    - understand and explain the reasons why it holds data – which also means keeping records that explain how decisions around personal data are made
    - be prepared to respond to subject access requests within the new time frames
    - be able to amend, delete or transfer data promptly upon any justified request or otherwise be prepared to explain why we will not
    - be able to audit how personal data is collected and when
    - Ensure that sensitive data will be held securely and accessed only by those with reason to view it.

The school also recognises that the Independent Inquiry into Child Sexual Abuse (IICSA) and various high-profile safeguarding cases have placed emphasis on long-term, lifetime or even indefinite keeping of full records related to incident reporting. We recognise therefore that Data Protection issues should never put child safety at risk, nor take precedence over the general prevention and processing of safeguarding actions. We specifically recognise that sensitive personal data of employees or pupils, including allegations of a sexual or criminal nature (whether proven or not), or details as to physical or mental health, should be kept securely and shared or accessible only on a need-to-know basis; for example, where a competent authority reasonably requests such information citing lawful grounds.

The school aims to balance the benefits of keeping detailed and complete records for the purposes of good practice, archives or general reference with practical considerations of storage, space and accessibility. In this context we recognise that there are legal considerations in respect of retention of records and documents which must be considered. These include:

- statutory duties and government guidance relating to schools, including for safeguarding
- disclosure requirements for potential future litigation
- contractual obligations
- the law of confidentiality and privacy
- the Data Protection Act ("DPA") 2018 and the UK General Data Protection Regulation (UKGDPR)

Appendices 1-3 of this policy (available to staff or on request from the School's Data Protection lead, the Bursar) gives details of the recommended retention periods for the retention of 'Records and Documents'. This guidance is drawn up and published by the IRMS (Information Records Management Society) of which the School is a member at the date of publication:

- Appendix 1 gives an overview index and link to the sections of the Retention Schedule.
- Appendix 2 gives an overview of the sub-categories of types of data
- Appendix 3 gives the full detail of the Retention Schedule.

What is a 'Record' or 'Document'

In this policy a 'record' means any document or item of data which contains evidence or information relating to the school, its staff or pupils. Some of this material, but not all, will contain personal data of individuals as defined in the DPA.

An obvious example of personal data would be the Single Central Record or a pupil file. However, a 'record' of personal data could arise simply by holding an email on the school's systems.

Many, if not most, new and recent records will be created, received and stored electronically. Others (such as Certificates, Registers, or older records) will be original paper documents.

The format of the record is less important than its contents and the purpose for keeping it. There are various forms of records detailed below:

- Digital records

Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data, or any large quantity of data, is password-protected~~,~~ with passwords provided on a need-to-know basis and regularly changed. Where 'cloud storage' is used data is also password protected. Access to many school systems that hold data also makes use of multi-factor authentication.

Emails (whether they are retained electronically or printed out as part of a paper file) are treated as 'records'.

- Paper records

Under the DPA, paper records are only classed as personal data if held in a 'relevant filing system'. This means organised and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible and thus searchable as a digital database might be. By way of example, an alphabetical personnel file split into marked dividers will likely fall under this category: but a merely chronological file of correspondence may well not.

When personal information is contained on print-outs taken from electronic files, this data has already been processed by the school and falls under the DPA.

Archiving and the destruction or erasure of Records

The following applies to the archiving and destruction or erasure of all school records:

- Records whether electronic or hard copy are stored securely. If possible, they will be stored with encryption, so that access is available only to authorised persons and that they are available when required and (where necessary) are searchable
- The School's policy is for cloud-based digital storage, so where relevant and possible, downloading data is discouraged as it should be viewed in situ in the cloud. However, if it is necessary then downloaded records and data are managed in line with this policy.
- The school's Acceptable Use Policy (AUP) is to be followed at all times
- That arrangements with external storage providers, whether physical or electronic (in any form, but most particularly "cloud-based" storage) are supported by robust contractual arrangements providing for security and access
- That reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and, in the case of personal data, necessary for the purposes for which it is held (and if so, that it is accurate and up-to-date)
- That all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them.

Secure disposal of documents

For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Skips and 'regular' waste disposal will not be considered secure.

Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed.

Where third party disposal experts are used they will be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information.

The PGS Storage & Retention of Documents Policy	
Date Approved	26th June 2025 (Senior Management Team)
Date Reviewed	16th June 2025 (School Business Meeting)
Next Review Date	Summer Term 2026
Policy author (SMT)	Bursar
Status	External
Report	ICT and Data Report
Review Schedule:	Every 3 years

Ph4100925

Appendix 1

IRMS Schools Toolkit – Index with Hyperlinks to Retention Schedule sections

(see also detailed Index in Appendix 2 which details sub-categories of data-types, and Appendix 3 which provides the full Retention Schedule)

(available to school staff or on request)