

GODALMING LEARNING PARTNERSHIP

Information Management Policy & Records Retention Schedule

Sept 2026

Policy prepared after training sessions with the IRMS and using a recommended model as a basis.

Document control		**POLICY LEVEL:** Non-Statutory	
Approved by	Governing Body	Approved Date	Oct 2026
Portfolio	Data Protection	Next Review	Sept 2026
Published Location	School Website / Internal /		
Version Number	Date issued	Author	Update information
2.0	Sept 2026	R Dunnage	Second Published Version: Reflects IRMS Guidance Feb 2020, Environmental Information Regulations 2004 and Data (Use and Access) Act 2025. Replaces internal review procedure with a general data use and access request Complaint Procedure and clarifies some guidance. Updated Retention Schedule bespoke to GLP.

This policy has been written with consideration given to schools' working practices. By adopting this Godalming Learning Partnership model policy, schools reduce their policy management workload.

Contents

1. Introduction 3

2. Definitions 3

3. Legal Framework and related Policies 3

4. Responsibilities 4

5. Storage and security 4

6. Email 5

7. Confidentiality 6

8. Information Audit 6

14. Retention Schedule 8

15. Disposal of Data 8

16. Transferring Pupil Records 9

17. Monitoring and Review 9

Appendix 1 ..... Error! Bookmark not defined.

Appendix 2 ..... Error! Bookmark not defined.

1. Introduction

1.1. **Witley C of E Infant** school is committed to maintaining the confidentiality of information we hold about pupils, parents, staff and volunteers. In line with the requirements of the General Data Protection Regulation (GDPR), the GLP has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were originally intended.

1.2. This policy outlines how information will be processed, stored, accessed, monitored, retained and disposed of, to meet the Trust's statutory requirements to comply with the General Data Protection Regulation and other relevant statutory legislation.

1.3. Information assets (or 'records') are defined as all documents and materials, regardless of format, which facilitate the activities carried out by the Trust. These records may be created, received and maintained in hard copy or electronically (including emails).

1.4. The school will manage records in line with the Records Retention Schedule, to ensure that it can meet Freedom of Information requests and respond to data subject access requests under the UK GDPR and other financial or legal requirements.

1.5. The retention periods are based on the latest guidance from the Information Records Management Society (IRMS) and are not an exhaustive list of records that may be kept by schools. Where the IRMS has not provided guidance for disposal methods or retention periods, good practice recommendations have been provided. The school will consult the GLP Data Protection Officer for further guidance, when necessary.

2. Definitions

2.1. 'Headteacher' refers to the role of Head of School, Headteacher and Executive Headteacher

2.2. 'School' refers to Witley Cof E Infant school

2.3. 'Pupil' refers to all pupils on roll

3. Legal Framework and related Policies

3.1. This policy has due regard to the following legislation and guidance including, but not limited to, the following:

- UK General Data Protection Regulation (2018)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- The Education (Independent School Standards) Regulations 2014 (with reference to educational record)
- Information Records Management Society 'Information Management Toolkit for Schools' 2020

3.2. The following policies and documents also apply

- Online Safety Policy
- Cyber Security Policy
- Data Protection & GDPR Policy
- Privacy Notices

- Acceptable Use Policy (Staff)
- Code of Conduct for Staff
- Safeguarding and Child Protection Policy
- HR Policies including Grievance, Disciplinary and Capability

4. Responsibilities

4.1. **Witley C of E Infant** school has a corporate responsibility to maintain its records and records management systems in accordance with legislation.

4.2. The GLP Data Protection Officer is responsible for providing guidance and advice on good records management practice and promoting compliance with this policy. Such guidance is formulated within the context of existing school policies and guidelines regarding data protection, national legislation and sector-wide standards.

4.3. The Headteacher is responsible for ensuring this policy is implemented and that all records are stored securely, in accordance with the retention periods outlined, recorded, and are disposed of correctly.

4.4. The Headteacher may delegate to the Data Protection Lead in their school the responsibility for maintaining the information asset register (IAR) and the record of processing activity (RoPA) in accordance with per Article 30 of GDPR and steps 2–5 of the Department for Education (DfE) Data Protection Toolkit for Schools. The GLP's Information & Documentation Processing Record template fulfils the requirements of these two documents.

4.5. It is essential that all records have an identified Information Asset Owner (IAO) whose responsibility it is to ensure records are managed in accordance with school's Data Protection Policies and the GDPR.

4.6. The Data Protection Officer will provide support and guidance to schools to ensure the Information & Documentation Processing Record is kept up to date. Maintaining the Record is not a one-off activity and the document needs to be regularly reviewed.

4.7. Records containing Personally Identifiable Information (PII) must be identified in the school's Information & Documentation Processing Record to ensure the school meets its obligations under GDPR to have a current data map. For example, 'HR records' would be entered, outlining the data fields, the purpose for processing/ retention, the IAO, location, and retention. This information must be reviewable by the school's Data Protection Lead to ensure that data sources are managed in line with policy and can be identified in the event of a Data Subject Access Request.

4.8. All staff are responsible for ensuring that any records for which they are responsible or which they process are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

4.9. The school's onboarding and offboarding procedures will ensure managed access to systems and records. This should include limits on how users access the resources, which user actions can be performed, and what resources users can access.

4.10. As individuals in schools often have access to personal or sensitive data, training will be provided to ensure that they are aware of the associated risks, their responsibilities (including confidentiality responsibilities), and the consequences of unauthorised access or disclosure. Training will be given to staff, volunteers and contractors and a record of their training maintained.

5. Storage and security

5.1. As a general principle, the GLP favours electronic storage of information, in order to:

a) assist data sharing where appropriate

b) ensure access to information by authorized users

c) ensure availability of information in the event of disaster recovery or business continuity

d) minimise duplication of data e.g. information stored in a school's management information system will not also be printed and stored in a paper file except for those contact and health details required for the Emergency Plan.

5.2. The school's Acceptable Use of ICT Facilities and Internet Agreement for Staff details measures to ensure safe and secure storage and access to electronic records and should be read in conjunction with this policy.

5.3. Schools must ensure that key information is securely stored and can still be accessed in the event of a data breach including loss of access due to fire or flood or malware, to limit any loss or theft of data.

5.4. It is strongly recommended that schools store key information in DfE approved enterprise-level cloud storage such as Microsoft Office or G Suite, to ensure access in the event of school closures.

5.5. Confidential paper records must be kept in a locked filing cabinet, drawer or safe, with restricted access. They must not be left unattended or in clear view when held in a location with general access.

5.6. Use of memory sticks is strongly discouraged. Schools must liaise with their IT Manager if exceptional circumstances require them to be used, such as large image files, and any memory stick must be encrypted with secure password access.

5.7. All electronic devices must be password-protected to protect the information on the device in case of theft.

5.8. All members of staff are provided with their own secure login and password which must not be divulged to anyone else.

5.9. All staff members should implement a clear desk policy to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.

5.10. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of school containing sensitive information should be supervised at all times.

5.11. The physical security of the school's buildings and storage systems, and access to them, is reviewed by the School Business Manager, the Designated Safeguarding Lead and the DPO to evaluate the risks of vandalism, burglary or theft, safeguarding risk or data security and provide guidance on measures to reduce risk accordingly.

6. Email

6.1. Staff and governors must not use their own personal email addresses for school purposes.

6.2. The consequences of an e-mail containing sensitive information being sent to an unauthorised person can result in a fine of up to £17.5 million or restrictions on processing from the Information Commissioner, along with adverse publicity for the school. Confidential or sensitive information should be sent by a secure encrypted e-mail or data transfer system. Personal information (such as a pupil's name) should never be used in the subject line of an e-mail.

6.3. Circular emails to parents should by preference be sent using third-party communication systems to ensure security of recipients. The school uses **Arbor** for this purpose. Where emails must be sent, they must be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

6.4. E-mail systems are commonly used to store information which should be stored somewhere else. E-mail and attachments that needs to be kept should be identified by content, for example: *Does it form part of a pupil record? Is it part of a contract? Does it relate to an employee?* They should then be saved into an appropriate electronic filing system. Where the text of the e-mail adds to the context or value of the attached documents,

it may be necessary to keep the whole e-mail. Information contained within e-mails may need to be transferred or logged in the appropriate place (e.g., the management information system (MIS) or behaviour management system). Once this is done, the original should be deleted.

6.5. The retention period for keeping information held as email files should correspond with the types of records found in the Records Retention Schedule below.

6.6. All staff should adopt best practice guidance and routinely delete emails over 12 months old. This will assist greatly in reducing the amount of information potentially disclosable in the event that a subject access request is received. It is essential to apply the same review and deletion principles to the emails in the SENT folders as well as INBOX folders.

7. Confidentiality

7.1. It may be appropriate to label records or archives as 'Confidential'. This does not exempt the record from being admissible under the Freedom of Information Act 2000.

7.2. The school takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

7.3. E-mails may be disclosed in response to a Freedom of Information or Subject Access Request and in legal cases. Electronic messages can be legally binding.

7.4. Before sharing data, staff must always ensure that:

- They have consent from data subjects to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

8. Information Audit

8.1. The Data Protection Officer will conduct an information audit on an annual basis with the school's Data Protection Lead (School Business Manager) against all information held by the school to evaluate the information each is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. The audit may involve interviews or questionnaires with key operational staff to identify information and information flows which may include the following:

- Paper documents and records
- Electronic documents and records
- Databases
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information
- Archives and archive logs

9. Data Gathering and Storage

9.1. Information will only be gathered and stored for specified purposes.

9.2. in order to be able to respond to requests for information the school will implement effective records management practices to enable staff to identify whether data is held and, if it is, locate it quickly and easily.

9.3. Administrators and managers are strongly recommended to create electronic filing systems (folders) which reflect the categories below in order to ensure efficient management of records on an ongoing basis and timely disposal

as required.

9.4. Where information is held in third party systems e.g. ARBOR, there is no requirement to also hold a paper copy and the duplication of records is not considered good practice.

9.5. All records must be securely stored. Schools must risk assess those records held only in paper format, assessing the risks of loss of access, for example through fire or theft, in particular those records of a confidential nature, such as personnel records and consider appropriate back up.

9.6. Electronic records must be backed up whether through DfE approved enterprise-level cloud storage such as Microsoft Office 365 or GSuite

10. Publication Scheme

10.1. The school will adopt and publish the appropriate model publication scheme, as recommended by the DfE, Information Commissioner and approved by school governors.

11. Dealing with Requests for Information

11.1. Theoretically any request for information is a request under the Freedom of Information Act, however this school has taken the decision that it will not consider any request that forms part of the normal pattern of work to be a Freedom of Information request. Only those requests which are considered to be outside the normal remit of the service provided will be recorded as Freedom of Information requests.

11.2. The school will assist applicants in making their request to have access to information held by the school.

11.3. Assistance will be given to applicants whose requests need to be transferred to another public authority (e.g. school, council, hospital).

11.4. The school will exercise its duty to confirm or deny the existence of requested data, subject to any exemptions that may apply.

11.5. The school aims to supply data requested within 20 working days (or in line with the Information Commissioner's current policy during school holidays), subject to any exemptions that may apply, and the estimated cost of complying with the request falling within the current defined charge limit.

11.6. If a response will take longer than 10 working days to complete, an acknowledgement will be sent to the person making the request, informing them when the information will be supplied.

11.7. There is no charge for making a Freedom of Information Act request. However, if we estimate that it would cost more than £450 (calculated at 18 hours work at a flat rate of £25 per hour) to retrieve the information, we are entitled to refuse your request. The rules on charging and fees are set out in section 12 of the Act and in the Freedom of Information and Data Protection Appropriate Limit and Fees Regulations 2004.

11.8. We may charge for photocopying and other direct costs. The first £15 of photocopying will be undertaken free of charge, and after that we may charge you 10 pence per page. We will always let you know in advance if there are costs associated with your request that we will look to recover.

11.9. A designated member of staff will be responsible for ensuring requests are fulfilled within the stipulated deadline and recording details of the request on the school's Information Requests Record.

11.10. Persons requesting data will be supplied with a copy of our complaints procedure upon request. Any complaints regarding Freedom of Information requests must firstly be addressed by the school. If, once we have had opportunity to reconsider our decision, we believe the initial response was correct, the applicant shall be entitled to take the matter to the Information Commissioner's Office and, ultimately, to an Information Tribunal.

11.11. Copies of data supplied will be retained for two years from the date it was put into the public domain.

12. Applying Exemptions

12.1. A full list of exemptions can be found at the Information Commissioner's website. There are two types of exemption – absolute and qualified. In practice there are very few which are likely to be applied by the education sector.

12.2. The decision to apply absolute exemptions will not be taken by individual members of staff but by a constituted group of at least three of the following: a governor, Headteacher, Deputy Headteacher, Data Protection Officer.

12.3. The decision to apply qualified exemptions will not be taken by individual members of staff but by a constituted group of at least three of the following: a governor, Headteacher, Deputy Headteacher, Data Protection Officer. Even if the group decides information should not be disclosed, a public interest test will be carried out when applying qualified exemptions, to decide whether the public interest in disclosure outweighs the objection to disclosure. If it does the information must be disclosed.

12.4. Advice will be sought from the Local Authority'sr Legal Services if there is any doubt as to whether information should be disclosed.

13. Logging Requests Received

13.1. The school will keep a record of all requests received for monitoring purposes, noting:

- the date the request was received,
- name and contact details of the person or organisation making the request
- the date the request was fulfilled or refused,
- the reason for any exemption being applied,
- the reason for any failure to meet the 20 day deadline.

14. Retention Schedule

14.1. The retention schedule refers to records, regardless of the media in which they are stored.

14.2. Managing records against the retention schedule is deemed to be "normal processing" under the UK General Data Protection Regulation, Data Protection Act 2018, Data (Use and Access) Act 2025 and the Freedom of Information Act 2000. Members of staff should be aware that once a Freedom of Information request is received or a legal hold imposed, then records disposal must be stopped.

14.3. Some of the retention periods are governed by statute; others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the General Data Protection Regulation, Data Protection Act 2018, Data (Use and Access) Act 2025 and the Freedom of Information Act 2000.

14.4. Managing records using these retention guidelines will be deemed to be "normal processing" under the legislation mentioned above. If a record series are to be kept for longer or shorter periods than those laid out in this document, the reasons for this need to be documented in each school's Information & Documentation Log.

15. Disposal of Data

15.1. All paper records produced through the day-to-day operations of the school containing personal identifying information must be disposed of by secure destruction e.g. via crosscut shredder.

15.2. Where the Retention Schedule mentions SECURE DISPOSAL, this must be via a confidential waste disposal service which provides confidential waste bins, or via crosscut shredder.

15.3. All schools must keep an electronic log of archived records, held and managed by the school Data Protection Lead. The log must record the date and method of secure destruction of records due for destruction at the

end of the requisite retention period.

15.4. Data Protection Leads are responsible for risk assessing whether records normally due for destruction, e.g. complaints records, should be retained for longer and recording this on the archives log.

15.5. School IT technicians can provide support and guidance to schools regarding secure disposal of computer and electronic records through approved recycling services.

16. Transferring Pupil Records

16.1. Where a pupil transfers to a new school, it is vital to ensure swift transfers of information to the new school to ensure appropriate decisions can be made regarding a pupil, using relevant and accurate information.

16.2. The pupil record should not be weeded before transfer, unless any duplicates or records with a short retention period have been included; these can be removed and securely destroyed.

16.3. The following should be transferred to the next school within 15 school days of receipt of confirmation that a pupil is registered at another school:

- Common Transfer File (CTF) from the School Information Management System via the school2school system, when used
- Any elements of the pupil record, held in any format, not transferred as part of the CTF
- Special Educational Needs & Disabilities (SEND) or other support service information, including behaviour, as only limited information may be included in the CTF

16.4. Child protection information must be securely delivered as soon as possible by the Designated Safeguarding Lead (DSL) or a member of their team to their equivalent at the new school.

16.5. Schools must ensure the information is kept secure and traceable during transfer. Pupil records should not be sent by post, even Special Delivery. They may be delivered or collected in person, with signed confirmation.

16.6. If held electronically, records may be sent to a named contact via secure encrypted email, or other secure transfer method.

16.7. If the pupil is transferring to an independent school or a post-16 establishment, the existing school should transfer copies of relevant information only and retain the original full record as the last known school.

16.8. If a request is received to transfer the pupil record or other information about a pupil to a school outside of the European Union (EU), the school must seek written consent from the parent prior to forwarding any information to the new school and should retain a copy of the original full record as the last known school.

17. Monitoring and Review

17.1. This policy will be reviewed every two years by the GLP Data Protection Officer or when best practice guidance is updated.

End

Appendix 1

General data use and access request Complaints Procedure

This guide explains how:

- members of the school community can raise concerns or complaints about how the school has managed their personal information or handled their Subject Access Request (SAR) under the UK GDPR and Data Protection Act 2018 and the Data (Use and Access) Act 2025.
- how members of the school community and the general public can raise concerns or complaints about how the school has managed their request for information under the Freedom of Information Act (2000) (FOI) or Environmental Information Regulations 2004 (EIR).

1. When to Use This Procedure

1.1. Use the procedure below if you have made a **Subject Access Request (SAR)** and**:**

- You have not received a response within **one calendar month**.
- You believe the SAR response is incomplete, inaccurate or you think information was wrongly withheld or redacted.

1.2. If you have made a request for data under the Freedom of Information Act (FOI) or Environmental Information Regulations (EIR) and:

- You have not received a response within **20 working days.**
- You believe the response is incomplete, inaccurate or you think information was wrongly withheld or redacted.

1.3. If you have a concern or complaint about how the school collects and processes personal data

2. How to Make a Complaint

Please contact the school using this electronic form: General data use and access request Complaints Form (Witley C of E Infant School) – Fill in form

3. School Response

The school will aim to respond in full **within 30 calendar days** for general data protection or SARs complaints **and within 20 working days** for FOI and EIR complaints. If we need more time, we will let you know.

3.1. The review of your complaint will be dealt with in a fair and impartial manner. As such, the review will be undertaken by a panel of 2, made up of a senior member of staff and/or governor(s) who did not deal with your original request.

3.2. The panel will be supported by the Data Protection Officer to ensure correct understanding of Data Protection and FOI and EIR legislation.

3.3. The panel will make a fresh decision based on all available evidence at the date of your request. As part of this process, the panel may need to consult with the member of staff that provided the information originally.

3.4. The panel will make a decision about the validity of any exemptions applied, and whether the school has complied with its statutory duties.

3.5. The panel will inform you of the outcome of the review, giving a full explanation within the specified timescales.

4. Escalation

4.1. Step 1: Data Protection Officer

If your concern or complaint remains unresolved **after 31 days** for general data protection or SARs **and after 21 school days** for FOI and EIR complaints., contact our Data Protection Officer (DPO) Rachel Dunnage: DPO@godalminglearning.org.uk

4.2. Step 2: Information Commissioner's Office

If your concern has not been resolved by the Data Protection Officer after a further calendar month, you can complain to the Information Commissioner's Office (ICO) in the following ways:

- Personal information - Make a complaint about how an organisation has used your personal information | ICO
- Freedom of Information requests: FOI and EIR complaints | ICO

5. Timescales

- Complaint acknowledgment: **within 15 days**.
- Complaint internal investigation and response: **within 30 calendar days** for general data protection or SARs **and within 20 school days** for FOI and EIR complaints. There may be reasons we need to extend our investigation; if we need more time, we will let you know.
- Complaint escalation to DPO: **after 31 calendar days** for general data protection or SARs **and after 21 school days** for FOI and EIR complaints.
- Complaint escalation to ICO: **after two calendar months.**

6. Contact details:

- School: office@witley.surrey.sch.uk
- Data Protection Officer: Rachel Dunnage, DPO@godalminglearning.org.uk
- Information Commissioner Office: T: 0303 123 1113. For more ways to get in touch see: How you can contact us | ICO

Appendix 2

Records Retention Schedule April 2026

Our Records Retention Schedule can be viewed on the Data Protection page of our school website here