FEDERATION OF GORING AND STOKE ROW CHURCH OF ENGLAND PRIMARY SCHOOLS

DATA PROTECTION POLICY

Policy reviewed and agreed by:	Finance and Resources Committee
Date:	September 2026
Next review:	September 2028

Status and purpose. This policy sets out the Federation's arrangements for complying with UK data protection law and for protecting the personal data of pupils, parents/carers, staff, governors, volunteers, visitors and other individuals whose information the Federation processes. It should be read with the Federation's Privacy Notices, Data Retention Policy, Digital Technology, Online Safety and Acceptable Use Policy, Freedom of Information Policy, safeguarding policies, complaints procedure and relevant operational procedures.

1. Legal framework

This policy is based on the following legal and regulatory framework:

- UK General Data Protection Regulation (UK GDPR), as amended by the Data (Use and Access) Act 2025 where applicable.
- Data Protection Act 2018.
- Freedom of Information Act 2000 (FOIA), including the distinction between FOI requests and requests for an individual's own personal data.
- Relevant education legislation and statutory requirements governing the collection, use, sharing and retention of pupil and workforce information.
- Information Commissioner's Office (ICO) guidance and codes of practice.

2. Scope

This policy applies to all personal data processed by or on behalf of the Federation, whether held electronically, on paper, on school systems, on devices, in email, in cloud services or by third-party providers. It applies to all staff, governors, volunteers, trainees, contractors and anyone else authorised to process personal data for the Federation.

To conform with the requirements of GDPR (General Data Protection Regulation) all data is handled according to the terms of our Privacy Notice. A copy of this is available on our school website.

3. Key definitions

Personal data: Information relating to an identified or identifiable living individual.

Special category data: More sensitive personal data, including racial or ethnic origin, health, biometric data used for identification, and other categories specified by law.

Processing: Any operation performed on personal data, including collecting, recording, storing, using, sharing, altering and deleting it.

Data controller: The organisation that determines the purposes and means of processing personal data. The Federation is the data controller for the processing described in its privacy notices.

Data processor: An organisation or person processing personal data on the Federation's behalf.

Personal data breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Subject access request (SAR): A request by or on behalf of an individual for access to their personal data under the right of access.

4. Data protection principles

The Federation will process personal data in accordance with the UK GDPR principles. In practice, this means that personal data will be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept for no longer than necessary, in line with the Federation's Data Retention Policy and retention schedule;
- processed securely, using appropriate technical and organisational measures; and
- managed in a way that enables the Federation to demonstrate compliance with its obligations (accountability).

5. Lawful basis for processing

Before processing personal data, the Federation will identify and document an appropriate lawful basis. Depending on the purpose, this may include legal obligation, public task, vital interests, contract, legitimate interests where applicable, or consent. Consent will not be used where another lawful basis is more appropriate. Where consent is relied upon, it must be freely given, specific, informed and unambiguous and it must be possible to withdraw it.

For special category data, the Federation will identify both an Article 6 lawful basis and an appropriate Article 9 condition, and will document any additional requirements under the Data Protection Act 2018 where applicable.

To conform with the requirements of GDPR (General Data Protection Regulation) all data is handled according to the terms of our Privacy Notice. A copy of this is available on our school website.

6. Transparency and privacy notices

The Federation will provide clear and accessible privacy information explaining who it is, what information it processes, why it processes it, its lawful bases, who information is shared with, retention arrangements and individuals' rights. The Federation maintains separate Privacy Notices for Pupils and Staff. These notices must be kept aligned with this policy and reviewed when processing arrangements or legal requirements change.

The Federation will ensure that the school websites contain current contact details for the Data Protection Officer.

7. Roles and responsibilities

Governing Board: Provides oversight, ensures that appropriate arrangements and resources are in place, and receives assurance about compliance, significant breaches and data protection risks.

Executive Headteacher: Has overall operational responsibility for implementing this policy and ensuring staff understand their responsibilities. The Executive Headteacher ensures that significant incidents and risks are escalated appropriately.

Data Protection Officer (DPO): Provides independent advice and monitoring, advises on DPIAs and compliance, supports staff training and awareness, acts as a contact point for individuals and the ICO, and monitors compliance. The DPO must be able to operate independently and must have sufficient resources to perform the role.

School leaders and administrators: Ensure data is handled securely, requests and incidents are escalated promptly, records are maintained and retention arrangements are followed.

All staff, governors and volunteers: Must keep personal data confidential, use it only for authorised purposes, follow this policy and related procedures, complete required training, and report suspected breaches immediately.

8. Records management and retention

The Federation's Data Retention Policy provides the framework for keeping and disposing of records. Staff must use the Federation's retention schedule and must not retain personal data indefinitely simply because it may be useful. Where a record is no longer required and no legal hold or other lawful reason applies, it must be securely destroyed or deleted.

The current Data Retention Policy already identifies responsibility for records management, requires an internal breach register and refers to a Data Protection Policy. This policy therefore forms the overarching data protection framework and should be read alongside the retention schedule.

9. Information security

- Access to personal data must be limited to people who need it for their role.
- Passwords and authentication information must be kept secure and must never be shared.
- Personal data must be transferred using secure and approved systems and methods.
- Paper records containing personal data must be stored securely and disposed of confidentially.

To conform with the requirements of GDPR (General Data Protection Regulation) all data is handled according to the terms of our Privacy Notice. A copy of this is available on our school website.

- Devices and systems must be protected with appropriate access controls, updates, encryption and other security measures appropriate to the risk.
- Staff must not use personal email accounts, unauthorised cloud storage, removable media or consumer applications to process Federation personal data unless specifically authorised and appropriately risk assessed.
- Where technology or AI tools are proposed, data protection and privacy risks must be considered before personal data is entered or uploaded.

10. Data sharing and third-party providers

Personal data will only be shared where there is a lawful basis and the sharing is necessary and proportionate. The Federation will consider the nature of the information, the recipient, the purpose, the risks and any relevant statutory duty before sharing.

Where a third party processes personal data on the Federation's behalf, the Federation will ensure that an appropriate written contract or other lawful arrangement is in place and that the processor provides sufficient guarantees regarding security and compliance. Staff must not commission or use new systems or services that process personal data without following the Federation's procurement, safeguarding and data protection checks.

11. Data Protection Impact Assessments (DPIAs) and privacy by design

Data protection will be considered at the planning stage of new or substantially changed processing. A DPIA will be completed before processing that is likely to result in a high risk to individuals' rights and freedoms, and may also be used for other significant projects where it is proportionate and helpful. The DPO must be consulted where a DPIA is required or undertaken.

Examples that may require careful assessment include new monitoring technologies, significant changes to online services, use of emerging technologies or AI involving personal data, large-scale processing of special category data, and processing that could create significant risks to pupils or staff.

12. Individual rights

The Federation will support individuals in exercising their data protection rights, subject to applicable legal exemptions and restrictions. These include, where applicable, the rights to be informed, access personal data, rectification, erasure, restriction of processing, objection and rights relating to automated decision-making and profiling.

The Federation will consider requests involving children carefully, including whether the child is mature enough to understand their rights and whether another person has authority to act on the child's behalf.

13. Subject Access Requests (SARs) – procedure

A SAR can be made verbally or in writing and does not need to use the words 'subject access request', refer to the UK GDPR or be sent to a particular person. Any member of staff who receives a request that appears to ask

To conform with the requirements of GDPR (General Data Protection Regulation) all data is handled according to the terms of our Privacy Notice. A copy of this is available on our school website.

for an individual's personal data must pass it promptly to the School Office/DPO in accordance with the Federation's SAR procedure.

1. Recognise and record the request. Record the date received, the requester, the data subject, the scope of the request and the member of staff responsible for coordinating it.
2. Acknowledge the request and, where necessary, seek proportionate evidence of identity or authority to act for another person. Do not routinely demand excessive identification.
3. If the request is unclear, the Federation may seek clarification where reasonably necessary. Where the law permits the response period to be paused while clarification is awaited, the Federation will record the date and correspondence.
4. Identify the systems, files, emails, paper records and other sources likely to contain the individual's personal data and carry out a reasonable and proportionate search.
5. Review the information before disclosure. Consider information relating to other people, legal professional privilege, safeguarding and other applicable exemptions or restrictions. Seek advice from the DPO where required.
6. Prepare the response in clear and accessible language. Provide the personal data and the required supplementary information.
7. Provide the information securely. Electronic information should normally be provided in a commonly used electronic format unless another format is requested or appropriate.
8. Respond without undue delay and normally within one month of receipt of the valid request. In complex cases or where there are multiple requests, the response period may be extended by up to a further two months where the legal conditions are met; the requester must be informed within the required timeframe.
9. Keep a record of the request, searches, decisions, exemptions relied upon, correspondence and the date and method of response.
10. If the request is refused in whole or in part, explain the reasons where required and advise the requester of their right to complain to the ICO and/or use the Federation's complaints process as appropriate.

Requests for a pupil's education record are a separate access right under education regulations. Where a request concerns both a person's own personal data and other official information, the Federation will separate the request and consider the relevant parts under data protection and FOI law. The ICO confirms that a request for the requester's own personal information should be treated as a SAR even if the requester calls it an FOI request.

14. Personal data breaches – procedure

All suspected personal data breaches must be reported immediately. Examples include sending personal data to the wrong person, loss or theft of records or devices, unauthorised access, accidental publication, inappropriate sharing, or a cyber incident involving personal data.

1. Report immediately to the Executive Headteacher, School Office and/or DPO. Do not delay reporting while trying to establish whether the incident is serious.
2. Contain the incident where possible. For example, recall or delete a wrongly sent message, restrict access, change compromised credentials, recover records or isolate an affected system.

To conform with the requirements of GDPR (General Data Protection Regulation) all data is handled according to the terms of our Privacy Notice. A copy of this is available on our school website.

3. Record the incident in the Federation's breach register, including what happened, when it happened, the types and amount of personal data involved, who may be affected, what has been done to contain it and who has been informed.
4. Assess the likely risk to the rights and freedoms of individuals, considering the nature and sensitivity of the data, the number of people affected, the circumstances of the breach, and potential consequences such as distress, discrimination, identity fraud or safeguarding risk.
5. The DPO/appropriate senior leader will determine whether the breach must be notified to the ICO. Where notification is required, it must be made without undue delay and, where feasible, within 72 hours of the Federation becoming aware of the breach. If all information is not yet available, an initial notification should not be unnecessarily delayed; further information can be provided later.
6. If the breach is likely to result in a high risk to individuals' rights and freedoms, the affected individuals will be informed without undue delay, unless a lawful exception applies.
7. Document the decision about whether or not to notify the ICO and/or affected individuals, including the risk assessment and reasons.
8. Investigate the cause, identify lessons learned and implement proportionate corrective or preventative action. Significant incidents will be reported through the Federation's governance arrangements.

The Federation will keep a record of all personal data breaches, including those that do not meet the threshold for reporting to the ICO.

15. Relationship with the Freedom of Information Policy

The Federation must distinguish between requests for official information under FOIA and requests for an individual's own personal data under data protection law. If a request asks only for the requester's own personal data, it should be handled as a SAR. If it asks for both the requester's personal data and other recorded information, the Federation will consider the two parts under the appropriate legal regime.

16. Complaints and concerns about data protection

Individuals should normally raise concerns about the Federation's handling of their personal data with the School Office, Executive Headteacher or DPO. The Federation will investigate concerns appropriately and explain the outcome. Individuals also have the right to complain to the Information Commissioner's Office.

17. Training and awareness

- All staff and governors will receive appropriate data protection awareness training at induction and refresher training at appropriate intervals.
- Staff will be trained to recognise SARs and suspected personal data breaches and to know who to report them to.
- Training will reflect the risks associated with the Federation's use of pupil, safeguarding, SEND, health, workforce and other sensitive information.
- The Federation will keep appropriate records of training and use incidents, requests and audits to identify further training needs.

To conform with the requirements of GDPR (General Data Protection Regulation) all data is handled according to the terms of our Privacy Notice. A copy of this is available on our school website.

18. Monitoring, compliance and review

The DPO and Federation leaders will monitor compliance through appropriate checks, incident reviews, SAR records, breach records, DPIAs, training records and other assurance activity. This policy will be reviewed biennially and sooner where there is a significant change in legislation, ICO guidance, Federation processing activities or identified risk.

Appendix 1 – Quick reference: SARs

If you receive…	Do…	Do not…
A verbal or written request for someone's personal data	Send it promptly to the School Office/DPO and record when it was received.	Wait for the requester to use the words 'SAR'.
A request from a parent for a child's information	Pass it to the DPO/appropriate lead so authority, the child's rights and any education-record issues can be considered.	Automatically assume parental responsibility means all information must be disclosed.
A request labelled 'FOI' that is clearly for the requester's own personal data	Treat it as a SAR and record it accordingly.	Process the request solely under FOIA.

Appendix 2 – Quick reference: data breach

Immediate action	What to remember
Report immediately	Tell the Executive Headteacher, School Office and/or DPO. Do not wait to establish the seriousness.
Contain	Recover, delete, restrict access, change passwords or isolate systems where appropriate.
Record	All breaches must be logged, even if they are not reported to the ICO.
Assess risk	Consider likelihood and severity of harm to individuals.
ICO notification	If the breach is likely to result in a risk to individuals' rights and freedoms, notify the ICO without undue delay and, where feasible, within 72 hours.
Tell affected people	If the breach is likely to result in a high risk, inform affected individuals without undue delay unless a lawful exception applies.
Learn	Record the decision, investigate the cause and implement improvements.

To conform with the requirements of GDPR (General Data Protection Regulation) all data is handled according to the terms of our Privacy Notice. A copy of this is available on our school website.