Clarendon Federation

Data Protection Policy

This policy provides a framework for protecting personal information held by Clarendon Federation, including information about pupils, parents and carers, staff, governors, volunteers, visitors and other individuals who work with the Federation.
It is written for a school federation in England and reflects the importance of safeguarding, confidentiality, secure information management and compliance with UK data protection legislation.

The policy should be approved by the Federation's governing body and reviewed regularly. Before adoption, the Federation should confirm its Data Protection Officer (DPO) arrangements, retention schedules, data breach procedures and links to existing safeguarding, information security and records management policies.

Policy Document Control

Document information	**Details**
Policy title	Data Protection Policy
Organisation	Clarendon Federation
Policy owner	Executive Headteacher / Headteachers
Responsible officer	Data Protection Officer (DPO)
Approved by	Governing Body
Date approved	November 2026
Date of implementation	November 2026
Review frequency	Annually, or sooner if legislation or circumstances change
Next review date	November 2027

Related policies	Safeguarding and Child Protection, Confidentiality, Information Security, Records Management and Retention, Freedom of Information, Acceptable Use of ICT, CCTV, Social Media and Privacy Notices

Clarendon Federation is committed to protecting the privacy, rights and freedoms of all individuals whose personal information it collects, holds, uses or shares.
The Federation recognises that the safe and appropriate handling of personal information is essential to maintaining the trust of pupils, parents and carers, staff, governors and the wider community.

As a Federation of schools, Clarendon Federation processes personal information to support education, teaching and learning, safeguarding, inclusion, staff management, financial administration and the effective operation of its schools.

The Federation will ensure that personal information is:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date where necessary.
- Retained only for as long as required.
- Protected against unauthorised or unlawful processing, accidental loss, destruction or damage.
- Handled in a way that respects the rights and freedoms of individuals.

The Federation will take appropriate technical and organisational measures to protect personal information and will ensure that all staff understand their responsibilities.

This policy applies to all schools within Clarendon Federation and to everyone who handles personal information on its behalf.

Legislative Framework

This policy is informed by the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Data (Use and Access) Act 2025.
- Freedom of Information Act 2000.
- Human Rights Act 1998.
- Children Act 1989 and Children Act 2004.
- Education Act 1996.
- Safeguarding legislation and statutory guidance, including *Keeping Children Safe in Education*.
- Relevant guidance published by the Information Commissioner's Office (ICO).
- Department for Education guidance on data protection in schools.

The Federation will review this policy and its associated procedures to ensure that they reflect current legislation and guidance.

The UK GDPR, the Data Protection Act 2018 and the changes introduced by the Data (Use and Access) Act 2025 provide the principal legal framework for the Federation's handling of personal information. The Department for Education has published updated school guidance reflecting the 2025 Act. (GOV.UK)

Scope of the Policy
This policy applies to all personal information processed by Clarendon Federation, regardless of whether it is held electronically, in paper records, through digital platforms or in another format.

It applies to information relating to:

- Pupils and former pupils.
- Parents, carers and family members.
- Employees, former employees and job applicants.
- Governors and other individuals involved in governance.
- Volunteers, students on placement and visitors.
- Contractors, suppliers and service providers.
- Other individuals who interact with the Federation.

The policy applies to all employees, including teaching staff, support staff, temporary staff and agency workers, as well as governors, volunteers, contractors and other individuals who have access to personal information.

Everyone covered by this policy must comply with its requirements and any associated procedures.

Definitions
Personal data
Information relating to an identified or identifiable living individual. This may include a name, address, date of birth, contact details, pupil records, employment records, photographs, digital identifiers or other information that identifies an individual.

Special category data
Personal data requiring additional protection because it is particularly sensitive. Examples include information about health, disability, racial or ethnic origin, religious beliefs and certain biometric information.

Processing
Any activity involving personal data, including collecting, recording, storing, accessing, using, sharing, amending or deleting information.

Data subject
The individual to whom the personal data relates.

Data controller
The organisation that determines the purposes for which, and the means by which, personal data is processed. Clarendon Federation must establish and document the appropriate controller arrangements for the Federation and its individual schools.

Data processor
An organisation or individual that processes personal data on behalf of a data controller.

Data breach
A security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data Protection Officer (DPO)
The person appointed to advise and monitor compliance with data protection legislation, provide guidance and act as a point of contact for data protection matters.

Roles and Responsibilities
Governing Body
The Governing Body is responsible for ensuring that appropriate arrangements are in place to protect personal information across Clarendon Federation.
It will:

- Approve this policy and review it regularly.
- Ensure that suitable data protection procedures are established and maintained.
- Provide appropriate oversight of data protection compliance.
- Ensure that appropriate resources are available to support secure information management.
- Receive assurance about significant data protection risks, incidents and areas requiring improvement.
- Ensure that data protection responsibilities are understood by leaders and staff.

Executive Head and Associate Executive Headteacher
The Executive Headteacher and Headteachers are responsible for implementing this policy within their areas of responsibility.
They will:

- Promote a culture of confidentiality and responsible information handling.
- Ensure that staff understand their data protection responsibilities.
- Ensure that appropriate procedures are followed when personal information is collected, stored, shared and disposed of.
- Ensure that staff complete appropriate training.
- Ensure that suspected data breaches are reported promptly.
- Support investigations into data protection incidents.
- Ensure that data protection is considered when introducing new systems, technologies or working practices.
- Work with the DPO to address risks and improve compliance.

Data Protection Officer
The Federation will maintain appropriate DPO arrangements in accordance with the law.
The DPO will:

- Advise the Federation on its obligations under data protection legislation.
- Monitor compliance with legislation, this policy and associated procedures.
- Advise on data protection impact assessments where required.
- Provide advice about data protection risks and appropriate safeguards.
- Support staff with data protection queries.
- Act as a contact point for the ICO and individuals where appropriate.
- Advise on personal data breaches and the need for regulatory notification.
- Support the handling of subject access requests and other information rights requests.
- Provide or arrange guidance and training.
- Report significant concerns and recommendations to the appropriate senior leaders and governors.

The DPO must be able to perform their duties independently and without conflicts of interest.

The Federation will ensure that the DPO's contact details are accessible to staff and members of the public.

Federation Staff
All staff are responsible for protecting the personal information they access or handle. Staff must:

- Read and follow this policy and associated procedures.
- Complete required data protection training.
- Access personal information only where there is a legitimate work-related reason.
- Keep personal information secure and confidential.
- Share information only with authorised individuals and organisations.
- Use approved systems and communication methods.
- Check recipients carefully before sending emails, messages or documents.
- Report suspected data breaches immediately.
- Avoid discussing confidential information where unauthorised people may overhear.
- Ensure that paper records are stored securely.
- Follow the Federation's records retention and disposal arrangements.
- Seek advice if they are unsure whether information can be accessed, shared or disclosed.

Failure to comply with this policy may result in disciplinary action and, where appropriate, further legal or regulatory consequences.

Pupils, Parents and Visitors
The Federation will provide accessible information about how personal data is used and protected.

Pupils will be supported to understand privacy, online safety and the importance of respecting other people's personal information in an age-appropriate way.

Parents and carers will be informed about the information the Federation collects, how it is used and the circumstances in which it may be shared.

Data Protection Principles
Clarendon Federation will apply the following principles to all personal data processing.
Lawfulness, Fairness and Transparency

Personal data will be processed lawfully, fairly and transparently.

The Federation will explain, through appropriate privacy notices and other communications:

- What personal information is collected.
- Why it is collected.
- The lawful basis for processing it.
- How the information will be used.
- Who it may be shared with.
- How long it will be retained.
- What rights individuals have.
- How individuals can contact the Federation about their information.

Privacy information will be written in clear and accessible language, taking account of the needs of children and other individuals who may require additional support.

Purpose Limitation
Personal information will only be collected for specified and legitimate purposes. The Federation will not use information for an incompatible purpose without first establishing that the further processing is lawful.

Staff must not use personal information obtained through their professional role for personal reasons or unrelated activities.

Data Minimisation
The Federation will collect and use only the personal information necessary for the purpose concerned.

Staff must not collect additional information simply because it may be useful in the future.

When sharing information, staff must ensure that only the relevant and necessary information is disclosed.

Accuracy
The Federation will take reasonable steps to ensure that personal information is accurate and, where necessary, kept up to date.

Staff must update records when changes are reported or identified.

Where information is disputed, the Federation will consider the circumstances and take appropriate steps to correct the information or record the disagreement.

Storage Limitation
Personal information will not be retained for longer than necessary.

The Federation will maintain a records retention schedule setting out the appropriate retention periods for different categories of information.

Records will be securely deleted, destroyed or anonymised when they are no longer required, unless there is a lawful reason to retain them.

Integrity and Confidentiality
Personal information will be protected using appropriate technical and organisational security measures.

These may include:

- Password protection and access controls.
- Secure electronic record systems.
- Multi-factor authentication where appropriate.
- Encryption of information where required.
- Secure storage of paper records.
- Appropriate staff training.
- Secure transfer and disposal arrangements.
- Monitoring and reviewing access to sensitive information.

Accountability
The Federation must be able to demonstrate that it complies with data protection legislation.

It will maintain appropriate records and evidence, including:

- Records of processing activities, where required.
- Privacy notices.
- Records retention schedules.
- Data protection impact assessments, where required.
- Data sharing agreements, where appropriate.
- Staff training records.
- Data breach and incident records.
- Information rights request records.
- Records of relevant decisions and risk assessments.

The Federation will regularly review its arrangements to identify and address areas for improvement. These measures reflect the Department for Education's guidance on documenting and demonstrating compliance. (GOV.UK)

Types of Information Processed
Clarendon Federation may process personal information relating to pupils, families, staff and other individuals.

Pupil Information
Pupil information may include:

- Names, addresses and dates of birth.
- Contact details for parents and carers.
- Attendance and punctuality records.
- Academic attainment and progress information.
- Assessment and examination results.
- Behaviour and exclusion records.
- Special educational needs and disability information.
- Education, Health and Care Plans and related documentation.
- Medical information and details of relevant health needs.
- Safeguarding and child protection records.
- Photographs, videos and recordings.
- Information about pupil participation in school activities.
- Information needed to support educational provision and transitions between schools.

Parent and Carer Information
This may include:

- Names and contact details.
- Relationships to pupils and parental responsibility information.
- Emergency contact information.
- Relevant family circumstances.
- Information needed to support safeguarding and welfare.
- Communications with the school.
- Information required to administer payments, trips or school activities.

The Federation will collect and use family information only where there is a legitimate and lawful purpose.

Staff Information
Staff information may include:

- Recruitment and application records.
- Employment contracts and personnel files.
- Payroll and pension information.
- Qualifications and training records.
- Performance management and professional development records.
- Absence and attendance information.
- Occupational health and relevant medical information.
- Safeguarding and safer recruitment information.
- Disciplinary and grievance records.
- Emergency contact details.

Access to staff records will be restricted to authorised individuals with a legitimate need to use them.

Special Category and Sensitive Information
The Federation recognises that information relating to health, disability, safeguarding and other sensitive matters requires particular care.

Such information will only be processed where the relevant legal requirements are met and appropriate safeguards are in place.

Staff must not disclose sensitive information to colleagues, parents or external organisations unless the disclosure is authorised and lawful.

Lawful Basis for Processing
The Federation will identify and document an appropriate lawful basis for each purpose for which it processes personal data.

Depending on the circumstances, lawful bases may include:

- **Legal obligation:** processing necessary to comply with a legal requirement.
- **Public task:** processing necessary to perform a task in the public interest or exercise official authority.
- **Contract:** processing necessary to enter into or perform a contract with an individual.
- **Vital interests:** processing necessary to protect someone's life in circumstances where this basis applies.
- **Consent:** processing based on freely given, specific, informed and unambiguous consent.
- **Legitimate interests:** processing necessary for legitimate interests, where this basis is available and its requirements are met.

The Federation will determine the appropriate basis for each processing activity rather than relying on one basis for all its activities.

For special category data, the Federation will also identify and document an applicable condition under data protection legislation.

Where criminal offence data is processed, the Federation will identify the relevant legal authority and safeguards.

Consent
Consent will only be used where it is an appropriate lawful basis.

Where consent is relied upon, it must be freely given, specific, informed and unambiguous. It must also be possible to demonstrate that consent was obtained.

Individuals will be informed of their right to withdraw consent.

The Federation recognises that consent is not always the appropriate basis for processing pupil or staff information. For example, statutory educational or safeguarding duties may provide a more appropriate lawful basis.

Where consent is used for photographs, videos, publicity or optional activities, the Federation will ensure that its arrangements are appropriate to the intended use.

Privacy Notices
The Federation will provide privacy notices to explain how personal information is collected and used.

Separate privacy notices may be maintained for:
- Pupils and parents or carers.
- Employees and job applicants.
- Governors and volunteers.
- Website users.
- Visitors and CCTV.
- Other groups where necessary.

Privacy notices will be reviewed regularly and updated when the purposes or arrangements for processing personal information change.

The Federation will ensure that individuals can find the relevant privacy notice easily.

Sharing Personal Information
Clarendon Federation may need to share personal information with other organisations to meet its legal responsibilities and support pupils, families and staff.

Information may be shared, where lawful and necessary, with:
- The local authority.
- The Department for Education.
- Other schools and educational settings.
- Health professionals and NHS services.
- Social care services.
- Police and other relevant safeguarding agencies.
- Examination boards and assessment providers.
- Relevant government departments.
- Payroll, pension and employment service providers.
- Approved educational software and technology providers.
- Other organisations providing services to the Federation.

Information will only be shared where there is an appropriate legal basis and the disclosure is necessary and proportionate.

Before sharing personal information, staff must consider:

1. Is there a legitimate and lawful reason to share the information?
2. Is the information necessary for the purpose?
3. Is the recipient authorised to receive it?
4. Is the information accurate and relevant?
5. Is a secure method of transfer being used?
6. Is a record of the decision or disclosure required?

Where appropriate, the Federation will establish data sharing agreements or contracts setting out the responsibilities of the organisations involved.

Personal information will not be shared with third parties simply because they request it.

Safeguarding Information Sharing

The Federation recognises that protecting children from harm may require information to be shared promptly with appropriate agencies.

Data protection legislation does not prevent necessary and proportionate information sharing for safeguarding purposes.

Where a safeguarding concern arises, staff must follow the Federation's safeguarding and child protection procedures and consult the Designated Safeguarding Lead (DSL) or deputy where appropriate.

Staff must not delay necessary safeguarding action because of uncertainty about data protection.

The Federation will ensure that safeguarding information is shared securely and only with appropriate individuals or organisations.

Where necessary, information may be shared without consent where there is a lawful basis to do so.

Confidentiality and Professional Conduct

All staff are expected to maintain professional confidentiality.

Staff must:

- Discuss pupils and families only with colleagues who need the information for their work.
- Avoid discussing confidential matters in corridors, reception areas, public spaces or other places where conversations may be overheard.
- Keep confidential documents out of sight when not in use.
- Avoid leaving pupil information on printers, photocopiers or shared desks.
- Ensure that confidential information is not included in communications with the wrong recipient.
- Never use personal information to gossip, make inappropriate comments or support personal interests.
- Avoid sharing confidential information through personal social media accounts or unauthorised messaging services.

Confidentiality obligations continue after an individual's employment or involvement with the Federation has ended.

However, confidentiality must not prevent staff from reporting safeguarding concerns, suspected wrongdoing or information that must lawfully be disclosed.

Information Security
The Federation will maintain appropriate measures to protect electronic and paper records.

Electronic Information
Staff must:

- Use Federation-approved devices, accounts and systems for work-related information.
- Use strong passwords and follow the Federation's password and authentication requirements.
- Lock screens when leaving devices unattended.
- Never share passwords or authentication credentials.
- Avoid downloading personal information onto unapproved devices.
- Store information only in authorised locations.
- Use secure methods when transferring sensitive information.
- Report lost or stolen devices immediately.
- Follow the Federation's ICT acceptable use and cyber-security procedures.

Personal information must not be entered into unapproved applications, websites or artificial intelligence tools.

Paper Records
Paper records containing personal information must be stored securely when not in use.

Staff must ensure that:

- Confidential files are kept in locked storage where appropriate.
- Paperwork is not left unattended in public areas.
- Documents are transported securely.
- Records are not removed from school premises without authorisation.
- Confidential waste is disposed of using approved secure disposal arrangements.

Remote Working
Staff working away from school must maintain the same standards of confidentiality and security as they would on school premises.

Personal information must not be accessed or discussed where unauthorised people can see or hear it.

Staff must follow Federation procedures for remote access and must not store confidential information on personal devices unless expressly authorised and appropriately secured.

Email and Electronic Communication
Staff must take particular care when sending information electronically.

Before sending an email or attachment containing personal information, staff must:

- Check the recipient's address carefully.
- Confirm that the recipient is authorised to receive the information.
- Check attachments before sending.
- Use secure transfer methods where appropriate.

- Consider whether the amount of information being shared is necessary.
- Use appropriate recipient protections when communicating with multiple parents or carers.

Sensitive information must not be sent through personal email accounts or unapproved messaging services.

If an email is sent to the wrong recipient or information is otherwise disclosed in error, the incident must be reported immediately in accordance with the data breach procedure.

Photographs, Videos and Recordings
The Federation recognises that photographs, videos and recordings may contain personal data.

Images and recordings will be collected and used only for appropriate and lawful purposes.

These may include:
- Recording learning and school activities.
- Sharing pupils' achievements.
- Producing educational resources.
- School websites and newsletters.
- Federation publications and approved publicity.
- Safeguarding, security or operational purposes.

The Federation will explain how images and recordings are used through appropriate privacy information and consent arrangements where applicable.

Staff must:
- Use approved devices and systems.
- Follow Federation procedures for taking and storing images.
- Avoid identifying pupils unnecessarily in published material.
- Respect applicable restrictions on the use of images.
- Ensure that images are shared only with authorised recipients.
- Avoid storing school images on personal devices unless expressly authorised.

The Federation will consider pupils' privacy, dignity and safeguarding needs when deciding whether an image or recording should be taken, stored or published.

Where a parent or carer requests that a pupil's image not be used for a particular purpose, the Federation will consider the request and apply its published arrangements, taking account of any legal obligations or safeguarding requirements.

CCTV and Monitoring
Where CCTV is used, the Federation will ensure that its use is lawful, necessary and proportionate.

Appropriate measures will be taken to:
- Explain the purpose of CCTV.
- Display appropriate signage.
- Restrict access to recordings.
- Store recordings securely.

- Retain recordings only for an appropriate period.
- Respond lawfully to requests for access to footage.
- Ensure that any disclosure is authorised and necessary.

CCTV will not be used for purposes that are incompatible with its stated purpose without an appropriate legal basis and assessment.

Any staff monitoring arrangements must be proportionate, transparent and compliant with relevant legislation.

Data Protection and Digital Technology
The Federation recognises that digital systems and educational technology can support teaching, learning and school administration but may introduce data protection risks.

Before introducing a new digital system or service, the Federation will consider:
- What personal information will be collected.
- Why the information is needed.
- Whether the proposed processing is lawful.
- Whether the provider has appropriate security measures.
- Who can access the information.
- Whether information will be shared with third parties.
- Where the information will be stored.
- How long the information will be retained.
- How information will be deleted when no longer required.
- Whether a data protection impact assessment is necessary.

The Federation will ensure that appropriate contracts and data processing arrangements are in place where required.

Artificial Intelligence
Staff must not upload identifiable pupil, parent, staff or other confidential information to public or unapproved artificial intelligence tools.

Any use of AI involving personal information must be authorised and assessed in accordance with the Federation's procedures.

Staff must not rely on AI-generated information without appropriate professional review, particularly where it could affect safeguarding, inclusion, assessment, pupil support or employment decisions.

The Federation will ensure that new technologies are used responsibly and in ways that protect the rights and interests of individuals.

Records Management and Retention
The Federation will maintain a records management system that supports the secure storage, retrieval, retention and disposal of personal information.

A retention schedule will specify how long different categories of records should be retained and how they should be disposed of.

Retention periods will reflect applicable legal requirements, statutory guidance, safeguarding considerations, operational needs and relevant records management guidance.

The Federation will review its records periodically to identify information that is no longer required.

Records will not be destroyed where they are subject to a legal hold, investigation, complaint, safeguarding process or other legitimate requirement for continued retention.

When records are no longer required, they will be securely destroyed or permanently deleted.

The Federation will ensure that electronic deletion and paper disposal arrangements are appropriate to the sensitivity of the information.

The Department for Education recommends that schools document retention periods and review whether personal information remains necessary, disposing of information securely when it is no longer needed. (GOV.UK)

Data Breaches and Information Security Incidents
A personal data breach may include:

- Sending personal information to the wrong recipient.
- Losing a laptop, tablet, mobile phone or USB device containing personal information.
- Losing paper records.
- Unauthorised access to pupil or staff records.
- Accidentally publishing confidential information online.
- Sharing sensitive information with someone who is not authorised to receive it.
- A cyberattack or ransomware incident.
- Altering or deleting personal information without authorisation.
- Leaving confidential information accessible to unauthorised individuals.

Reporting a Breach
All staff must report a suspected or actual data breach immediately to the Headteacher, designated senior leader or DPO, following the Federation's incident reporting procedure.

Staff must not wait until they have established the full extent of the breach before reporting it.

The initial report should include, where known:

- What happened.
- When it happened.
- What information may have been affected.
- Which individuals may be affected.
- Who may have accessed the information.
- What immediate action has already been taken.

Managing a Breach
The Federation will:

1. Take immediate steps to contain the incident.
2. Prevent further unauthorised access or disclosure where possible.

3. Notify the appropriate senior leader and DPO.
4. Assess the nature and seriousness of the breach.
5. Identify the individuals and information affected.
6. Assess the likely risks to individuals.
7. Determine whether notification to the ICO is legally required.
8. Determine whether affected individuals must be informed.
9. Record the incident and the action taken.
10. Identify lessons learned and implement improvements.

The Federation will ensure that incidents are recorded even where they do not meet the threshold for reporting to the ICO.

Reporting to the ICO
Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, the Federation will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Where notification is required but cannot be made within that period, the reasons for the delay will be documented.

Where a breach is likely to result in a high risk to individuals' rights and freedoms, the Federation will inform affected individuals without undue delay unless a legal exception applies.

The DPO will advise on the appropriate response and reporting requirements.

The Federation will follow current ICO guidance and its internal breach response procedure. (GOV.UK)

Data Protection Impact Assessments
A Data Protection Impact Assessment (DPIA) will be completed where processing is likely to result in a high risk to individuals' rights and freedoms.

A DPIA may be required when introducing:
- New systems that process significant amounts of personal information.
- Technologies involving systematic monitoring.
- Systems processing sensitive pupil or staff information.
- New arrangements for sharing personal information.
- Processing involving vulnerable individuals where the risks justify an assessment.
- Other activities likely to create significant privacy risks.

A DPIA should identify:
- The purpose of the processing.
- The types of personal information involved.
- The lawful basis for processing.
- The necessity and proportionality of the proposed activity.
- Potential risks to individuals.
- Measures to reduce or manage those risks.
- Any outstanding risks requiring further action.

The DPO will advise on DPIAs and whether additional safeguards or consultation are necessary.

Processing must not proceed where unresolved risks mean that legal requirements are not met.

Individual Rights
Clarendon Federation recognises the rights individuals have under data protection legislation.

Depending on the circumstances, these rights include:

- The right to be informed about how personal data is used.
- The right of access to personal data.
- The right to have inaccurate personal data corrected.
- The right to request erasure of personal data in certain circumstances.
- The right to restrict processing in certain circumstances.
- The right to data portability where applicable.
- The right to object to certain processing.
- Rights relating to automated decision-making and profiling where applicable.
- The right to raise concerns about how personal information is handled.

These rights are subject to legal conditions and exemptions. For example, the Federation may need to retain information to meet statutory duties or protect a child.

Requests will be considered individually and handled in accordance with current legislation.

Subject Access Requests
A subject access request (SAR) is a request by an individual to access their personal data.

Requests may be made verbally or in writing and do not need to use the phrase *subject access request*.

Staff must forward any request for personal information to the DPO or designated senior leader as soon as possible.

The Federation will:

- Record the date the request is received.
- Establish the identity and authority of the requester where necessary.
- Clarify the scope of an unclear request where appropriate.
- Identify and retrieve relevant personal information.
- Consider whether any legal exemptions or third-party privacy rights apply.
- Review information before disclosure.
- Provide the response securely.
- Keep a record of the request and the action taken.

The normal statutory response period is one calendar month, subject to the applicable rules, including provisions for clarification, identity verification and extensions in qualifying circumstances.

Where a request is complex and the law permits an extension, the Federation will inform the requester within the required timeframe.

The Federation will not normally charge a fee for responding to a subject access request, except where legislation permits.

Staff must not independently decide to withhold requested information or disclose records without following the Federation's procedure.

The Federation will follow the Department for Education's current guidance on subject access requests, including its advice on response times and searching relevant records. (GOV.UK)

Other Information Rights Requests
Individuals may request that their personal information be corrected, erased or restricted, or object to particular processing.

All such requests must be referred promptly to the DPO or designated senior leader.

The Federation will assess each request in accordance with the relevant legal requirements and respond within the applicable statutory timeframe.

Where the Federation cannot comply with a request, it will explain the reasons where required and inform the individual of any relevant rights to complain or seek further review.

The Federation will maintain records of information rights requests and the decisions made.

Data Protection Complaints
Clarendon Federation is committed to addressing concerns about the handling of personal information fairly, promptly and transparently.

Individuals who are concerned about the use of their personal data may raise their concerns with the Federation's DPO or designated data protection contact.

Complaints may relate to:

- The collection or use of personal information.
- Inaccurate records.
- Unauthorised disclosure.
- Requests for access or correction.
- Concerns about retention or deletion.
- Other matters relating to data protection.

The Federation will:

1. Acknowledge and record the complaint.
2. Review the concern and gather relevant information.
3. Consider the complaint fairly and impartially.
4. Take appropriate action to resolve the issue.
5. Communicate the outcome to the complainant.
6. Explain any further steps available to the individual.
7. Record the outcome and any improvements required.

Complaints will be handled within the applicable legal requirements and the Federation's complaints procedure.

Where a complaint relates to the DPO or an individual who would ordinarily investigate the concern, the Federation will ensure that an appropriate independent person considers it.

Individuals may also complain to the ICO if they remain concerned about how their personal information is being handled.

The Federation will review its complaints procedure to ensure that it reflects the data protection complaint requirements introduced by the Data (Use and Access) Act 2025.

Children and Young People's Personal Information
Clarendon Federation recognises that children require particular protection when their personal information is collected and used.

The Federation will:

- Process children's information fairly and lawfully.
- Provide age-appropriate privacy information where appropriate.
- Protect sensitive information relating to pupils.
- Consider the child's rights and interests when responding to requests for information.
- Ensure that access to pupil records is managed lawfully.
- Take account of safeguarding considerations when sharing information.
- Support pupils to develop an understanding of privacy and responsible information sharing.

The Federation recognises that parents and carers do not automatically have unrestricted access to every record relating to a child.

Requests for pupil information will be considered in accordance with data protection law, education legislation, the child's circumstances and any relevant safeguarding concerns.

Where a child is capable of exercising their own information rights, the Federation will take account of their understanding and the applicable legal requirements.

Staff Training and Awareness
The Federation will ensure that staff receive appropriate data protection information and training.

Training will cover:

- The principles of data protection.
- Confidentiality and professional conduct.
- Secure handling of personal information.
- Recognising and reporting data breaches.
- Sharing information appropriately.
- Responding to information rights requests.
- Safeguarding and data protection.
- Secure use of digital systems.
- Relevant changes in legislation and guidance.

New staff will be made aware of their responsibilities as part of induction.

Refresher training will be provided at appropriate intervals and when necessary.

The Federation will maintain records of training and take action where additional support is required.

Third-Party Providers and Contractors
The Federation may use external organisations to provide services, including educational software, payroll, IT support, assessment platforms and other administrative services.

Before engaging a provider that processes personal information, the Federation will consider:

- Whether the provider is suitable for the proposed purpose.
- What personal information the provider will access.
- What security measures are in place.
- Whether appropriate contractual arrangements are required.
- Whether the provider uses other processors.
- Where the information will be stored and processed.
- How information will be returned or deleted when the service ends.
- Whether the proposed arrangements meet legal requirements.

Contracts will include appropriate data protection provisions where required.

The Federation will take reasonable steps to ensure that providers meet their contractual obligations and protect personal information.

International Transfers
The Federation will ensure that personal information is not transferred outside the United Kingdom unless the transfer complies with applicable data protection legislation.

Before using a service that may transfer or make personal information accessible internationally, the Federation will assess the proposed arrangements.

Where required, appropriate safeguards and transfer mechanisms will be established.
The Federation will consider the location of data storage and processing when procuring digital systems and services.

Freedom of Information
The Federation recognises its obligations under the Freedom of Information Act 2000 where applicable.

Requests for recorded information may fall under freedom of information legislation rather than data protection legislation.

Where a request involves personal information, the Federation will consider the interaction between the relevant legal frameworks and apply any appropriate exemptions.

Requests must be referred to the designated member of staff responsible for freedom of information.

Staff must not independently release information where a formal assessment is required.

Monitoring and Compliance
The Federation will monitor its compliance with this policy through appropriate arrangements, which may include:

- Regular reviews of data protection procedures.
- Information security checks.
- Audits of access to records.
- Reviews of records retention and disposal.
- Monitoring of data breaches and near misses.
- Reviews of information rights requests and complaints.
- Staff training records.
- Reviews of third-party data processing arrangements.
- Data protection impact assessments where required.
- Reports and recommendations from the DPO.

Significant risks and recurring issues will be reported to senior leaders and governors.

Where weaknesses are identified, the Federation will establish appropriate actions, responsibilities and timescales to address them.

Breaches of This Policy
Failure to comply with this policy may place pupils, staff, families and the Federation at risk.

Depending on the circumstances, a breach may result in:
- Additional training or supervision.
- Changes to working practices or access permissions.
- A formal investigation.
- Disciplinary action in accordance with the Federation's procedures.
- Notification to the ICO or another relevant authority.
- Other action required by law.

The Federation will consider the circumstances of each incident fairly and proportionately.

Staff must report suspected breaches even where they believe the incident was accidental.

Policy Review
This policy will be reviewed annually and sooner if there are significant changes to legislation, regulatory guidance, the Federation's systems or its information processing arrangements.

The review will consider:
- Changes in data protection legislation.
- Updated ICO and Department for Education guidance.
- Findings from audits and monitoring.
- Data breaches and lessons learned.
- Complaints and information rights requests.
- Changes to digital systems and external providers.
- Feedback from staff and governors.

Any significant changes will be brought to the attention of relevant staff and approved in accordance with the Federation's governance arrangements.

Appendix 1: Data Protection Checklist for Staff

All Clarendon Federation staff should use the following checklist when handling personal information.

Before collecting information

- Is the information necessary for a legitimate purpose?
- Is there a lawful basis for collecting it?
- Have individuals been given appropriate privacy information?
- Is the information being collected through an approved system?

When using information

- Am I authorised to access this information?
- Am I using it for an appropriate purpose?
- Is the information accurate and up to date?
- Am I keeping it confidential?
- Am I sharing only what is necessary?

When sending information

- Have I checked the recipient carefully?
- Have I checked the attachment?
- Is the recipient authorised to receive the information?
- Am I using an approved and secure method?
- Have I considered whether additional protection is needed?

When storing information

- Is the information stored in an approved location?
- Is access restricted appropriately?
- Are paper records secured?
- Am I following the retention schedule?

When something goes wrong

- Have I reported the incident immediately?
- Have I taken appropriate steps to contain the incident?
- Have I followed the advice of the DPO or designated senior leader?

Remember: If you are unsure whether personal information can be accessed, shared, stored or deleted, seek advice before proceeding, unless immediate action is necessary to protect a child or another person from harm.

Appendix 2: Data Breach Reporting Procedure

Step 1: Identify
Recognise that personal information may have been lost, disclosed, altered, accessed or destroyed without authorisation.

Step 2: Report immediately
Contact the Headteacher, designated senior leader or DPO using the Federation's agreed reporting arrangements.

Step 3: Contain
Take appropriate steps to prevent further disclosure or loss, provided this does not compromise safeguarding or other urgent action.

Step 4: Assess
The appropriate senior leader and DPO will assess the nature of the breach, the information involved, the individuals affected and the potential risks.

Step 5: Notify
Determine whether the ICO and affected individuals must be notified, and complete any required notifications within the applicable statutory timescales.

Step 6: Record
Document the incident, the assessment, the decisions made and the action taken.

Step 7: Review
Identify lessons learned and implement measures to reduce the likelihood of a similar incident occurring again.

Appendix 3: Responsibilities at a Glance

Role	Key responsibility
Governing Body	Oversight, approval and assurance of data protection arrangements
Executive Head	Federation-wide leadership and implementation
SLT	Implementation within their schools and prompt reporting of concerns
Data Protection Officer	Advice, monitoring, compliance support and guidance on information rights and breaches
Designated Safeguarding Lead	Safeguarding information sharing in accordance with safeguarding procedures
School Business Manager / Administrative Team	Secure handling of administrative records and support with information requests, where delegated
IT / Systems Provider	Technical safeguards and support in accordance with agreed responsibilities
All Staff	Confidentiality, secure handling of information and immediate reporting of suspected breaches
Governors, Volunteers and Contractors	Compliance with applicable confidentiality and data protection requirements

The allocation of responsibilities must reflect the Federation's actual staffing, contractual arrangements and governance structure.

Appendix 4: Implementation Actions Before Adoption

To ensure that this policy accurately reflects Clarendon Federation's arrangements, the following actions should be completed before formal approval.

Action	Responsible person	Status
Confirm the Federation's legal data controller arrangements	Executive Headteacher / Governing Body	22.10.26
Insert the DPO's name and contact details	Executive Headteacher / DPO	22.10.26
Confirm how data protection concerns and complaints should be submitted	DPO / Federation Leadership Team	22.10.26
Check that pupil, parent, staff and website privacy notices are current	DPO / Relevant Leaders	22.10.26
Review the records retention schedule	DPO / Records Management Lead	22.10.26
Confirm the data breach reporting route and out-of-hours arrangements	DPO / Executive Headteacher	22.10.26
Review subject access request and other information rights procedures	DPO / Administrative Team	22.10.26
Review data sharing agreements and processor contracts	DPO / Relevant Leaders	22.10.26
Confirm staff training and induction arrangements	Federation Leadership Team	22.10.26
Review digital systems, information security and AI use	DPO / IT Lead	22.10.26
Check that the data protection complaints procedure reflects current legislation	DPO / Federation Leadership Team	22.10.26
Present the policy for approval	Executive Headteacher / Governing Body	22.10.26

Official Guidance and Further Information
The Federation should use the following official resources when reviewing its arrangements:

- Department for Education: Data protection in schools
- Department for Education: Data protection policies and procedures
- Department for Education: Record keeping and management
- Department for Education: Subject access requests
- Information Commissioner's Office

Important: This is a comprehensive draft for Clarendon Federation, not a legal compliance certification. Before adoption, the Federation should check it against its existing policies, governance arrangements and current ICO guidance, particularly the requirements introduced by the Data (Use and Access) Act 2025. The Department for Education's school guidance was updated on 14 October 2026, so the latest guidance should be consulted as part of the approval process. (GOV.UK)