



The Welbeck Federation

Data Protection Policy

Executive Head Teacher Signature:	<i>L Jordan</i>
Date Adopted:	Sept 2026
Review Date:	Sept 2027

1. Aims

The Welbeck Federation is committed to protecting the rights and privacy of all individuals whose personal data we collect, store and process.

This policy sets out how the federation complies with the requirements of UK data protection legislation and ensures that personal information is:

-  Processed lawfully, fairly and transparently.
-  Collected for specified and legitimate purposes.
-  Accurate and up to date.
-  Stored securely.
-  Retained only for as long as necessary.
-  Protected from unauthorised access, loss, misuse or disclosure.

This policy applies to all personal data held by the federation, whether in electronic or paper format.

2. Legislation and Guidance

This policy is based on:

-  UK General Data Protection Regulation (UK GDPR)
-  Data Protection Act 2018
-  Freedom of Information Act 2000
-  Education Act 2011
-  Keeping Children Safe in Education (KCSIE)
-  Information Commissioner's Office (ICO) guidance

This policy should be read alongside all Federation policies relating to safeguarding, online safety, information security and records management.

3. Definitions

Personal Data: Any information relating to an identified or identifiable living individual.

Examples include:

-  Names
-  Addresses
-  Telephone numbers
-  Email addresses
-  Online identifiers
-  Photographs
-  CCTV images
-  Pupil records
-  Staff employment records

Special Category Data: Information requiring additional protection, including:

-  Health information
-  Ethnic origin
-  Religious beliefs
-  Biometrics
-  Trade union membership
-  Sexual orientation

Processing: Anything done with personal data, including:

-  Collection
-  Recording
-  Storage

-  Retrieval
-  Sharing
-  Updating
-  Deletion

Data Subject: The individual whose personal data is being processed.

Data Breach: Any unauthorised access, disclosure, loss, alteration or destruction of personal data.

4. Data Controller

The Welbeck Federation is the Data Controller and determines the purposes and means by which personal data is processed.

The Federation collects and processes information relating to:

-  Pupils
-  Parents and carers
-  Staff
-  Governors
-  Volunteers
-  Visitors
-  Contractors

The Federation is registered with the Information Commissioner's Office (ICO) and complies with all relevant data protection requirements.

5. Roles and Responsibilities

Governing Body  Ensuring compliance with data protection legislation.  Monitoring the effectiveness of this policy.  Receiving reports relating to significant data protection issues.  Ensuring sufficient resources are available to support compliance.	Executive Headteacher Lisa Jordan is responsible for:  Ensuring day-to-day compliance.  Promoting a culture of data protection.  Managing risks relating to personal information.  Ensuring staff understand their responsibilities.
Data Protection Officer (DPO) Sam Case is the federation's Data Protection Officer.  Monitoring compliance with data protection legislation.  Providing advice and guidance.  Supporting data protection impact assessments.  Investigating breaches.  Acting as the contact point for the ICO.  Advising on subject access requests and information rights.	School Office Teams  Maintaining accurate records.  Processing information securely.  Supporting information requests.  Following retention and disposal procedures.
All Staff  Follow this policy.  Protect personal information.  Access information only when required.  Complete required data protection training.  Report concerns or breaches immediately.  Maintain confidentiality at all times.	

6. Data Protection Principles

The Federation will ensure personal data is:

-  **Lawful, Fair and Transparent**
Information will only be processed where there is a lawful basis to do so.
-  **Purpose Limited**
Information will only be collected for clear and legitimate purposes.
-  **Data Minimisation**
Only information necessary for educational, safeguarding or operational purposes will be collected.
-  **Accuracy**
Records will be kept accurate and updated where necessary.
-  **Storage Limitation**
Information will be retained only for as long as necessary.
-  **Security**
Appropriate technical and organisational measures will protect personal data.
-  **Accountability**
The federation will be able to demonstrate compliance with data protection legislation.

7. Collecting Personal Data

The Federation collects personal data to:

-  Educate pupils.
-  Safeguard children.
-  Employ and support staff.
-  Meet legal obligations.
-  Communicate with families.
-  Operate the federation effectively.

Information may be obtained from:

-  Parents and carers.
-  Pupils.
-  Staff.
-  Previous schools.
-  Local authorities.
-  Government agencies.
-  Professional services.

8. Sharing Personal Data

The Federation will not share personal information unless:

-  Consent has been provided; or
-  There is a legal obligation; or
-  There is a safeguarding concern; or
-  Sharing is necessary for educational purposes; or
-  Sharing is required for public task responsibilities.

Information may be shared with:

-  The Department for Education
-  Local Authorities
-  Social Care
-  Health Services
-  Police
-  Professional advisers
-  Approved educational software providers

All sharing arrangements will comply with UK GDPR and Data Protection Act 2018 requirements.

9. Subject Access Requests

Individuals have the right to request access to personal information held about them.

Requests may be submitted in writing, by email or verbally.

The Federation will:

-  Verify identity where required.
-  Respond within one calendar month.
-  Provide information free of charge unless requests are manifestly unfounded or excessive.
-  Explain any exemptions applied.

10. Rights of Individuals

Individuals have the right to:

-  Be informed.
-  Access their information.
-  Correct inaccurate data.
-  Request erasure where appropriate.
-  Restrict processing.
-  Object to processing.
-  Data portability (where applicable).
-  Challenge automated decision-making.

Requests should be directed to the Data Protection Officer.

11. Educational Records

Parents may request access to information relating to their child.

Requests will be considered in line with:

-  Data protection legislation.
-  Child protection requirements.
-  The rights of the child.
-  Relevant educational record requirements.

12. Artificial Intelligence (AI) and Data Protection

The Welbeck Federation recognises the growing use of Artificial Intelligence (AI) technologies within education.

Staff must:

-  Use only approved AI systems.
-  Never enter personal, safeguarding, medical, behavioural or confidential information into public AI platforms.
-  Ensure AI-generated content is checked for accuracy and appropriateness.
-  Remain professionally accountable for all decisions.

Pupils will be taught:

-  Safe use of AI technologies.
-  Ethical and responsible use.
-  Critical evaluation of AI-generated content.

The use of AI must always comply with:

-  UK GDPR
-  Data Protection Act 2018
-  Safeguarding requirements
-  Federation Online Safety Policy

13. Photographs and Videos

The Federation may use photographs and videos:

-  On displays.
-  In newsletters.
-  On websites.
-  On social media.
-  For promotional materials.

Parental consent will be obtained through federation consent procedures.

Photographs will not be accompanied by unnecessary personal information.

Parents and carers may withdraw consent at any time.

14. Data Protection by Design and Default

The Federation will consider privacy and information security when:

-  Introducing new systems.
-  Procuring software.
-  Sharing information.
-  Changing working practices.

Where appropriate, Data Protection Impact Assessments (DPIAs) will be completed before new processing activities begin.

15. Data Security

The Federation is committed to protecting personal information through appropriate technical and organisational measures.

These include:

-  Secure passwords.
-  Multi-factor authentication where appropriate.
-  Device encryption.
-  Secure cloud storage.
-  Access controls.
-  Filtering and monitoring systems.
-  Antivirus protection.
-  Security updates.
-  Regular backups.

Personal data must not be stored:

-  In personal email accounts.
-  On unauthorised applications.
-  On unencrypted devices.
-  Within public AI systems.

Where remote working takes place, staff must ensure that information cannot be viewed or accessed by unauthorised individuals.

16. Cyber Security

The Federation recognises cyber security as a fundamental safeguarding and operational priority.

The Federation works with Atom IT to maintain secure systems and networks.

Measures include:

-  Filtering and monitoring systems.
-  Cyber security controls.
-  Email protection.
-  Malware protection.
-  Device management.

- 🔍 Security audits.
- 🔍 Staff awareness training.

All staff must immediately report:

- 🔍 Suspicious emails.
- 🔍 Phishing attempts.
- 🔍 Lost or stolen devices.
- 🔍 Unauthorised access.
- 🔍 Suspected cyber attacks.

Cyber security incidents will be investigated promptly and escalated where necessary.

17. Records Retention and Disposal

The Federation maintains retention schedules to ensure information is kept only for appropriate periods.

When records are no longer required they will be securely destroyed.

Disposal methods include:

- 🔍 Confidential shredding.
- 🔍 Secure deletion of electronic files.
- 🔍 Approved disposal services.

Records of disposal will be maintained where required.

18. Personal Data Breaches

A personal data breach may include:

- 🔍 Loss of personal information.
- 🔍 Sending information to the wrong person.
- 🔍 Unauthorised access.
- 🔍 Cyber attacks.
- 🔍 Accidental disclosure.

All staff must:

- 🔍 Report the breach immediately.
- 🔍 Notify the Executive Headteacher or DPO.
- 🔍 Preserve any evidence.
- 🔍 Follow instructions provided by senior leaders.

The DPO will:

- 🔍 Investigate the breach.
- 🔍 Assess risks.
- 🔍 Determine whether notification to the ICO is required.
- 🔍 Ensure appropriate action is taken.

Where required by law, breaches will be reported to the ICO within 72 hours.

19. Training

All staff, governors and regular volunteers will receive data protection training:

- 🔍 During induction.
- 🔍 Through annual updates.
- 🔍 When legislation or procedures change.

Additional training will be provided where specific roles require it.

20. Monitoring and Review

The Executive Headteacher and Data Protection Officer will monitor implementation of this policy.

This policy will be reviewed:

- 🔍 Annually.

-  Following significant legislative changes.
-  Following significant data breaches.
-  Following recommendations from audits or inspections.

21. Linked Policies

This policy should be read alongside:

-  Online Safety Policy
-  Acceptable Use Policy
-  Child Protection Policy
-  Behaviour Policy
-  Staff Code of Conduct
-  Complaints Policy