



Pathway Primary Federation

Data Protection Policy

UK GDPR • Data Protection Act 2018 • Data (Use and Access) Act 2025

'Love of God and others as oneself.'

POLICY CONTROL	
Policy owner	Executive Headteacher
Data Protection Officer	Classroom365 Limited – info@classroom365.co.uk – 020 7952 5308
Approved by	Pathway Primary Federation Governing Board
Approval date	Autumn 2026
Next review	Autumn 2027

Scope: Classroom365 Limited is appointed as the external DPO for both Federation schools. This policy applies across both schools and to all personal data processed in paper or electronic form.

Contents

- 1. Purpose and aims
- 2. Legislation and guidance
- 3. Scope
- 4. Definitions
- 5. Data-protection principles
- 6. Roles and responsibilities
- 7. Collecting personal data and privacy notices
- 8. Lawful bases and special-category data
- 9. Data security and acceptable handling
- 10. Sharing and disclosing personal data
- 11. International transfers
- 12. Retention and secure disposal
- 13. Individual rights and subject access requests
- 14. Data-protection complaints
- 15. Personal-data breaches
- 16. Data protection by design and DPIAs
- 17. Biometric data, CCTV and photographs
- 18. Automated decision-making and artificial intelligence
- 19. Training, monitoring and review
- 20. Linked policies and documentation
- Appendix 1: Subject access request form
- Appendix 2: Data-protection complaint form
- Appendix 3: Immediate action following a suspected breach

1. Purpose and aims

Pathway Primary Federation is committed to protecting the rights and privacy of pupils, parents and carers, staff, governors, volunteers, visitors and others whose personal data it processes. This policy explains how the Federation will collect, use, store, share and dispose of personal data lawfully, fairly, transparently and securely.

The aims of this policy are to:

- ensure compliance with current data-protection law and regulatory guidance
- define clear responsibilities for governors, leaders, staff and others who process personal data
- embed data protection by design and by default in Federation systems and decision-making
- ensure that individuals can exercise their information rights effectively
- provide clear routes for reporting breaches, concerns and complaints

2. Legislation and guidance

This policy is based on and should be read in accordance with:

- the UK General Data Protection Regulation (UK GDPR)
- the Data Protection Act 2018
- the Data (Use and Access) Act 2025 and relevant commencement provisions
- the Privacy and Electronic Communications Regulations 2003, as amended
- the Protection of Freedoms Act 2012 where biometric data is processed
- the Education (Pupil Information) (England) Regulations 2005
- current guidance issued by the Information Commissioner's Office (ICO) and Department for Education

Where legislation or authoritative guidance changes, the Federation will follow the current legal requirement and update this policy as soon as reasonably practicable.

3. Scope

This policy applies to Whittington CE (VA) Primary School and Morda CE (VC) Primary School, including their nursery and specialist or resourced provision where applicable. It applies to all governors, employees, agency staff, contractors, volunteers and others processing personal data on behalf of either school.

It applies to personal data held electronically or in structured paper records and to any processing carried out on school premises, remotely, on educational visits or using Federation equipment, systems or accounts.

4. Definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living individual.
Special-category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric identifiers, health information, sex life or sexual orientation.
Criminal-offence data	Personal data relating to criminal convictions, offences or related security measures.
Processing	Any operation involving personal data, including collecting, recording, organising, storing, consulting, sharing, altering, restricting, erasing or destroying it.
Data subject	The individual to whom personal data relates.
Controller	The body that determines why and how personal data is processed. The Federation governing board acts for the schools in determining their processing arrangements.
Processor	A person or organisation that processes personal data on behalf of a controller.
Personal-data breach	A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
DPO	The independent Data Protection Officer appointed to advise, monitor compliance and act as a contact with the ICO.

5. Data-protection principles

The Federation will ensure that personal data is:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept in identifiable form for no longer than necessary
- processed securely using appropriate technical and organisational measures

The Federation is responsible for, and must be able to demonstrate, compliance with these principles. This is the accountability principle.

6. Roles and responsibilities

6.1 Governing board

The governing board has overall responsibility for ensuring that the Federation complies with data-protection law. It will maintain appropriate policies, oversight, resources and assurance arrangements and will appoint an independent DPO with sufficient expertise and access to senior leadership.

6.2 Data Protection Officer

The DPO will:

- inform and advise the Federation about its legal obligations
- monitor compliance, including policies, audits, staff awareness and training
- advise on data-protection impact assessments
- provide advice on personal-data breaches, information-rights requests and complaints
- act as a contact point for data subjects and the ICO
- report independently to the highest management level and avoid conflicts of interest

The Federation's external DPO is Classroom365 Limited, Crampton Primary School, Iliffe Street, London SE17 3LE. Email: info@classroom365.co.uk. Telephone: 020 7952 5308. Its appointment covers both Federation schools.

6.3 Executive Headteacher and senior leaders

The Executive Headteacher is responsible for implementing this policy across the Federation. Heads of School and other designated leaders will ensure that local procedures are followed, risks and breaches are escalated promptly, privacy information is provided and staff receive suitable training.

6.4 All staff, governors and volunteers

Everyone who handles personal data must:

- complete required training and follow this policy and related procedures
- use personal data only for authorised school purposes
- access only the information needed for their role
- keep information accurate, secure and confidential
- report any suspected breach, loss, inappropriate disclosure or cyber incident immediately
- consult a senior leader or the DPO when uncertain
- not use personal accounts, unauthorised applications or unapproved devices to process school personal data

6.5 Contractors and processors

Third parties processing personal data for the Federation must be subject to appropriate due diligence and a written contract meeting data-protection requirements. Their security, location, subcontracting and deletion arrangements will be assessed and reviewed.

7. Collecting personal data and privacy notices

Personal data will be collected only where it is necessary for legitimate educational, safeguarding, employment, governance or operational purposes. Collection forms and systems will request the minimum information required.

The Federation will provide clear, accessible privacy notices explaining what information is collected, the purposes and lawful bases, recipients, retention, international transfers, individual rights, DPO details and the right to complain. Privacy notices will be reviewed at least annually and whenever processing changes significantly.

Separate notices will be maintained as appropriate for pupils and parents/carers, workforce, governors and volunteers, job applicants, visitors, contractors and other groups whose data is processed.

8. Lawful bases and special-category data

Before processing personal data, the Federation will identify and document an appropriate lawful basis under Article 6 UK GDPR. Schools commonly rely on legal obligation, public task, vital interests, contract or, in limited circumstances, consent or legitimate interests.

Consent will be freely given, specific, informed, unambiguous and capable of withdrawal. It will not be used where the school can rely more appropriately on a statutory or public-task basis.

Where special-category data is processed, the Federation will also identify a condition under Article 9 UK GDPR and, where required, a condition and safeguards under the Data Protection Act 2018. Criminal-offence data will be processed only where authorised by law and subject to appropriate safeguards.

9. Data security and acceptable handling

The Federation will use proportionate technical and organisational measures to protect confidentiality, integrity and availability. These will include, as appropriate:

- role-based access and prompt removal or amendment of access when roles change
- strong passwords, multi-factor authentication and secure account management
- encryption and secure transfer methods
- supported devices, security updates, malware protection, filtering and monitoring
- secure storage of paper records and clear-desk practices
- backups, recovery arrangements and continuity planning
- physical security and appropriate disposal of equipment and records
- regular review of permissions, suppliers, systems and risks

Personal data must not be sent to personal email accounts, stored in personal cloud services or copied to removable media unless specifically authorised and protected. Screens and documents must not be left visible to unauthorised people. Confidential conversations must take place appropriately.

10. Sharing and disclosing personal data

The Federation will share personal data only where there is a lawful basis, the disclosure is necessary and proportionate, the recipient is authorised and the information is transferred securely. The minimum necessary information will be shared.

Information may be shared without consent where the law permits or requires this, including for safeguarding, child protection, legal obligations, public tasks, vital interests, prevention or detection of crime, or responding to emergencies. Safeguarding information will never be withheld solely because consent has not been obtained.

Regular or systematic sharing will be supported by an appropriate agreement, protocol or processor contract. Disclosures outside routine arrangements will be recorded where appropriate, including what was shared, with whom, why, when and under which lawful basis.

11. International transfers

Before making personal data accessible to a separate organisation outside the UK, including through cloud hosting or remote support, the Federation will determine whether this is a restricted transfer. It will proceed only where the transfer is covered by UK adequacy regulations, appropriate safeguards such as an approved international data transfer agreement or addendum, or a lawful exception. A transfer-risk assessment will be completed where required, with advice from the DPO.

12. Retention and secure disposal

Personal data will not be kept for longer than needed. The Federation will maintain and follow an information-retention schedule that reflects legal, safeguarding, educational, employment, financial and operational requirements. Records subject to legal hold, complaint, investigation or litigation will not be destroyed until authorised.

Electronic and paper information will be securely deleted or destroyed at the end of its retention period. Disposal through contractors will be subject to appropriate security and evidence of destruction where necessary.

13. Individual rights and subject access requests

Depending on the circumstances, individuals have rights to be informed, access their data, rectify inaccurate information, erase data, restrict processing, receive portable data, object to processing and receive safeguards relating to solely automated decisions.

Requests may be made verbally or in writing to any member of staff and must be forwarded immediately to the Executive Headteacher and DPO. The Federation will verify identity proportionately and may seek clarification where needed to identify the information requested.

Timescale: The Federation will respond without undue delay and normally within one calendar month. The period may be extended by up to two further months for a complex request or multiple requests, with the requester informed within the initial month. Any lawful “stop the clock” provision will be applied only in accordance with current legislation and ICO guidance.

The Federation will conduct searches that are reasonable and proportionate. Requests will normally be free of charge. A reasonable fee may be charged, or a request refused, only where the law permits, such as where a request is manifestly unfounded or excessive. Any refusal will explain the reasons and rights of complaint.

Requests for a pupil’s educational record under education legislation are distinct from subject access requests and will be handled under the applicable procedure and timescale.

14. Data-protection complaints

Anyone may complain about the Federation’s handling of their personal data. Complaints should be sent to the Executive Headteacher or DPO using the contact details in this policy. The Federation will provide an accessible method of making a complaint, acknowledge receipt within 30 days, take appropriate steps to investigate without undue delay and keep the complainant informed of progress and outcome.

If the complainant remains dissatisfied after the Federation has considered the matter, they may complain to the Information Commissioner’s Office at ico.org.uk or by telephone on 0303 123 1113. The Federation’s response will explain this right.

15. Personal-data breaches

Any actual or suspected personal-data breach must be reported immediately to the Executive Headteacher, Head of School or other designated senior leader. It must not be investigated informally or concealed. The DPO will be informed promptly, normally within 24 hours of the Federation becoming aware of the incident.

The Federation will contain the incident, preserve evidence, assess risks to individuals, document decisions and take remedial action. Where a breach is likely to risk individuals’ rights and freedoms, the controller will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware. Where a high risk is likely, affected individuals will also be informed without undue delay unless a lawful exception applies.

16. Data protection by design and DPIAs

Data protection will be considered from the outset of any new system, service, initiative, data-sharing arrangement or significant change in processing. Default settings will collect, use and retain only the data necessary for the stated purpose.

A data-protection impact assessment (DPIA) will be completed before processing that is likely to result in high risk, including where new technologies, systematic monitoring, large-scale sensitive data, biometric identification or significant profiling may be involved. The DPO will advise on the DPIA. High residual risks will be escalated and, where required, the ICO consulted before processing begins.

17. Biometric data, CCTV and photographs

Biometric data used for identification will be processed only where lawful and in accordance with the Protection of Freedoms Act 2012, including required notification, consent and alternative arrangements for pupils. The Federation will maintain a separate biometric policy where such systems are used.

CCTV or other surveillance will be used only for specified, necessary and proportionate purposes, with appropriate signage, access controls, retention and privacy information. A DPIA will be completed where required.

Photographs and recordings may constitute personal data. The Federation will identify an appropriate lawful basis, distinguish operational school use from optional promotional use, manage permissions where consent is relied upon and avoid publishing information that creates an unreasonable safeguarding or privacy risk.

18. Automated decision-making and artificial intelligence

The Federation will assess data-protection, safeguarding, accuracy, bias, intellectual-property and security risks before using artificial-intelligence or automated systems involving personal data. Staff must use only approved tools and must not enter confidential or identifiable school information into public or unapproved AI services.

Where a decision producing legal or similarly significant effects is made solely by automated means, the Federation will ensure there is a lawful basis and appropriate safeguards, including meaningful information, the ability to contest the decision and access to human review, as required by current law.

19. Training, monitoring and review

All staff and governors will receive appropriate data-protection training at induction and refresher training at least annually. Additional role-specific training will be provided for staff handling sensitive information, information-rights requests, breaches, contracts, records management or information security.

Compliance will be monitored through audits, incident and request logs, training records, supplier reviews, policy checks and DPO reporting. The governing board will review this policy annually, and earlier following significant legal, regulatory or operational change or a serious incident.

20. Linked policies and documentation

- Privacy notices
- Information Security Policy
- Records Management and Retention Policy/Schedule
- Personal Data Breach Procedure
- Subject Access Request Procedure
- Freedom of Information Policy and Publication Scheme
- Online Safety and Acceptable Use Policies
- Safeguarding and Child Protection Policy
- CCTV and Biometric Data Policies, where applicable
- Staff Code of Conduct
- Complaints Policy
- Business Continuity and Disaster Recovery arrangements
- Processor contracts, data-sharing agreements, records of processing and DPIA register

Appendix 1: Subject access request form

A request does not have to be made on this form. It is provided to help the Federation identify and respond to the information sought.

Information required	Response
Name of data subject	
Date of birth, if relevant	
Current address	
Telephone and email	
Name of requester, if different	
Relationship/authority to act	
Description of information requested	
Relevant date range, people, systems or documents	
Preferred secure response method	

The Federation may request proportionate evidence of identity or authority. Do not send original identity documents unless asked. Return to the Executive Headteacher or DPO using the contact details in this policy.

Appendix 2: Data-protection complaint form

Complaints may also be made verbally or in another accessible format.

Information required	Response
Your name	
Contact details	
Data subject, if different	
School concerned	☐ Whittington CE (VA) Primary School ☐ Morda CE (VC) Primary School
Date or period concerned	
What happened?	
What personal data was involved?	
Who have you already contacted?	
What outcome are you seeking?	
Any supporting documents	

Send the complaint to the Executive Headteacher or DPO. The Federation will acknowledge it within 30 days and investigate without undue delay.

Appendix 3: Immediate action following a suspected breach

1. Report it immediately to the Executive Headteacher, Head of School or designated senior leader. Do not wait until the end of the day.
2. Contain the incident where safe to do so: recall an email, disconnect a lost or compromised device, recover papers, change access or seek IT support. Do not delete evidence.
3. Record the facts: what happened, when, whose data, what types and quantities of data, who may have received or accessed it, and action already taken.
4. The senior leader informs the DPO promptly and opens the breach log. The time at which the Federation became aware must be recorded.
5. Assess likelihood and severity of harm to individuals, including safeguarding, discrimination, identity fraud, financial loss, distress, confidentiality and reputational harm.
6. Decide, with DPO advice, whether ICO notification is required within 72 hours and whether affected individuals must be informed without undue delay.
7. Complete remedial action, document the decision and lessons learned, and update systems, training, contracts or procedures as necessary.

Never: conceal a breach, contact affected families before senior/DPO advice, blame individuals publicly, alter records, or assume that a near miss does not need to be reported.

Data Protection Policy

Introduction

The Data Protection Act 1998 (the 'DPA') aims to promote high standards in the handling of personal information protecting individuals rights to privacy. The DPA applies to anyone holding information about

living individuals in electronic format and in some cases on paper. As the school is a holder of personal records they must also follow this act.

What are main principals of good information handling?

Personal information must be:

- Fairly and lawfully processed;
- Processed for specified purposes;
- Adequate relevant and not excessive;
- Accurate, and where necessary, kept up to date;
- Not kept for longer than is necessary;
- Processed in line with the rights of the individual;
- Kept Secure;
- Not transferred to countries outside the European Economic Area unless there is adequate protection for the information.

Who is covered?

The DPA covers staff, pupils, parents and any other individuals for which the school holds personal details.

Who is responsible for ensuring that the school complies with the DPA?

The Headteacher has ultimate responsibility in ensuring that the school complies with this act however everyone within the school has a responsibility to ensure that they abide by the principles listed above in handling personal data. If you are unsure about the action you are taking with regard to personal data you must check with the Headteacher to ensure you are complying with the DPA.

Some of the questions you can ask yourself to ensure that the action you are taking will comply with the DPA are:

- Do I really need this information about an individual? Do I know what I'm going to use it for?
- Do the people whose information I hold know that I've got it and are they likely to understand what it will be used for? Would any of them be surprised at what I'm doing with their personal information?
- If I'm asked to pass personal information on am I sure it's okay to do so under the DPA? (check with your Headteacher if unsure)
- Am I satisfied that the personal information I hold is secure be it on the computer or paper based?
- Is the personal data held accurate and up to date?
- Do I delete/destroy personal information (securely) as soon as I have no need for it?
- Is access to personal information limited only to those with a strict need to know? Who will have access to this information if I place it on computer file or hold on a paper record?

Ensure that any personal data that you hold is only shared with other members of school staff or authorities who are entitled to have access to this data. If you have any queries or concerns you must raise them with the Headteacher immediately.

As an individual you also have a responsibility to ensure that the details held about you are accurate and kept up to date for example ensuring that the school is notified if you move house.

Individual Rights

All individuals (including staff) have a right under the DPA to ask for a copy of the information held about them on computer and in some manual filing systems.

Requests for access to personal data should be referred to the Executive Headteacher who will deal with it promptly and within a maximum of 40 days from receiving the request. A small charge to cover photocopying, secure postage etc can be made at the discretion of the Headteacher,

The School will only monitor individual staff when there are concerns about the individual's use of e-mail, internet, telephone or other data that the member of staff may be using inappropriately. If monitoring is used for training purposes the individual will be made aware of this at the time.

Miscellaneous

The School will also ensure that any service providers used that will handle personal data for example HR, Payroll comply with the DPA.

Any member of staff found to mishandle data or share personal data with unauthorised individuals will be subject to investigation under the School's Disciplinary Policy. Deliberate, malicious or reckless breaking of the DPA will be counted as gross misconduct and could result in dismissal. Under this Act you can also be criminally liable if you knowingly or recklessly disclose personal information in breach of the policy.

If there are any queries concerning this policy or you require further assistance or training please contact the Executive Headteacher.