

GATEWAY ACADEMY



School Data Protection Policy

Approved by:	Lisa Breslin and Claire Cleary
Last reviewed on:	September 2026
Next review due by:	September 2027

AIMS

Gateway Academy is committed to protecting the privacy and security of personal data. The Academy will ensure that personal data relating to pupils, parents/carers, staff, governors, volunteers, visitors, contractors, consultants and other individuals is collected, stored, processed, shared and securely destroyed in accordance with applicable data protection legislation. This policy applies to all personal data processed by the Academy, whether held electronically or in paper form and whether processing is automated or manual.

The Academy will comply with the **UK General Data Protection Regulation (UK GDPR)**, **Data Protection Act 2018 (DPA 2018)**, **Data (Use and Access) Act 2025 (DUAA 2025)** and, where applicable, the **Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)**. The Academy will also follow relevant guidance issued by the Information Commissioner's Office (ICO) and Department for Education (DfE).

LEGISLATION AND GUIDANCE

This policy has regard to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications Regulations 2003
- Protection of Freedoms Act 2012, where applicable to biometric data
- relevant ICO codes, guidance and statutory requirements
- relevant DfE data protection guidance
- Keeping Children Safe in Education (KCSIE), where relevant to safeguarding and online safety
- applicable requirements relating to CCTV, photographs, videos and educational technology.

The Academy will review this policy and associated procedures regularly to ensure that they remain current.

DEFINITIONS

Data controller

The natural or legal person, public authority, agency or other body which determines the purposes and means of processing personal data.

For personal data for which Gateway Academy determines the purposes and means of processing, the Academy is the data controller.

Data processor

A person or organisation that processes personal data on behalf of the data controller and in accordance with the controller's instructions.

Data subject

An identified or identifiable individual whose personal data is processed.

Personal data

Information relating to an identified or identifiable living individual, including information such as a name, identification number, location data, online identifier or information relating to their physical, physiological, genetic, mental, economic, cultural or social identity.

Special Category Data

Personal data requiring additional protection because it is particularly sensitive, including information relating to:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetics
- biometrics where used for identification purposes
- physical or mental health
- sex life or sexual orientation.

Information about criminal convictions and offences is subject to separate additional safeguards under data protection law.

Processing

Any operation performed on personal data, including collection, recording, storage, alteration, retrieval, consultation, use, disclosure, restriction, erasure or destruction.

Personal data breach

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

The Data Controller

The Academy collects and determines the processing of personal data relating to pupils, parents/carers, staff, governors, volunteers, visitors and other individuals.

The Academy may also process personal data on behalf of others where appropriate.

The Academy is registered with the Information Commissioner's Office (ICO) as required by law.

ROLES AND RESPONSIBILITIES

Governing Board

The Governing Board has overall responsibility for ensuring that the Academy complies with its data protection obligations.

Governors will receive appropriate information and training to enable them to understand their responsibilities.

Data Protection Officer

The Academy has appointed Grow Education Partners Ltd as its Data Protection Officer (DPO).

DPO: Claire Mehegan

Email: DPO@groweducationpartners.com

Telephone: 020 7554 2806

The DPO is responsible for:

- advising the Academy and its staff on data protection obligations;
- monitoring compliance with data protection legislation and this policy;
- advising on Data Protection Impact Assessments (DPIAs);
- supporting the development and review of privacy notices;
- providing advice on data protection risks and data sharing;
- acting as a point of contact for data subjects and the ICO;
- supporting the Academy in responding to data protection complaints and information rights requests.

The DPO will have appropriate independence, resources and access to information to carry out their role effectively.

The DPO may provide an annual report or other compliance report to the Governing Board.

Academy Data Protection Lead

Lisa Breslin, CoHeadteacher, acts as the Academy's day-to-day representative for data protection matters.

All staff

All staff are responsible for protecting personal data and must:

- collect, store and process personal data in accordance with this policy
- only access personal data necessary for their role
- keep personal information secure
- report actual or suspected data breaches immediately
- immediately pass information rights requests to the designated member of staff
- seek advice before introducing new processing activities or systems
- seek advice before sharing personal data with third parties
- seek advice before transferring personal data outside the UK
- report concerns about compliance with this policy to the Data Protection Lead or DPO

Failure to comply with this policy may result in disciplinary action.

DATA PROTECTION PRINCIPLES

The Academy will comply with the data protection principles. Personal data must be:

1. processed lawfully, fairly and transparently;
2. collected for specified, explicit and legitimate purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and kept up to date where necessary;
5. kept for no longer than necessary;
6. processed securely.

The Academy must also demonstrate accountability by taking responsibility for compliance and maintaining appropriate records and evidence.

PROCESSING PERSONAL DATA

Lawfulness, fairness and transparency

The Academy will only process personal data where there is an appropriate lawful basis under data protection legislation.

Depending on the circumstances, this may include:

- consent
- contract
- legal obligation
- vital interests
- public task
- legitimate interests, where applicable
- recognised legitimate interests introduced by the Data (Use and Access) Act 2025, where applicable

The lawful basis must be considered for each processing activity rather than simply for a category of information.

Where special category data is processed, the Academy will also identify an appropriate condition under data protection legislation.

Where criminal offence data is processed, the Academy will comply with the additional requirements that apply.

The Academy will not rely on consent where another lawful basis is more appropriate.

Where consent is relied upon, it will be freely given, specific, informed and unambiguous and individuals will be able to withdraw consent.

Privacy notices

The Academy will provide clear and accessible privacy information explaining:

- what personal data is collected
- why it is processed
- the lawful basis for processing
- who information may be shared with
- how long information is retained
- individuals' data protection rights
- how to contact the Academy and DPO
- how to complain about the Academy's processing of personal data
- relevant filtering and monitoring arrangements

Privacy notices will be reviewed at least annually and whenever there is a significant change to how personal data is processed.

Current privacy notices will be available on the Academy website and through other appropriate means.

Limitation, minimisation and accuracy

The Academy will only collect personal data that is necessary for a specified and legitimate purpose.

Staff must only access and process personal data where it is necessary for their role.

Personal data will be kept accurate and up to date where necessary.

Where the Academy intends to use personal data for a new purpose, it will consider whether this is compatible with the original purpose and whether individuals need to be informed.

Record of Processing Activities

The Academy maintains a Record of Processing Activities (RoPA) in accordance with Article 30 of the UK GDPR.

The RoPA records, where applicable:

- categories of personal data
- purposes of processing
- lawful bases
- categories of data subjects
- recipients and data sharing
- retention periods
- security measures
- international transfers

The RoPA will be reviewed regularly and made available to the ICO where required.

BIOMETRIC RECOGNITION SYSTEMS

Where the Academy uses pupils' biometric data as part of an automated biometric recognition system, it will comply with the relevant requirements of the Protection of Freedoms Act 2012 and data protection legislation.

Parents/carers will be notified before a biometric system is introduced or before their child first participates.

Written consent from at least one parent/carers will be obtained before biometric information is processed where required by law.

Pupils will not be required to participate if they refuse or withdraw from the processing of their biometric information.

An appropriate alternative method of accessing the relevant service will be provided.

Relevant biometric information will be securely deleted when it is no longer required or when consent is withdrawn, subject to any legal requirement to retain it.

SHARING PERSONAL DATA

The Academy may share personal data where this is lawful, necessary and proportionate.

This may include sharing information with:

- parents/carers and pupils where appropriate
- local authorities
- health and social care services
- safeguarding agencies
- the police and other law enforcement agencies
- government departments
- examination and assessment bodies
- professional advisers
- contractors and service providers
- IT and educational technology providers
- emergency services

The Academy will not routinely seek consent where another lawful basis applies.

Where personal data is shared with a processor, the Academy will ensure that appropriate contractual arrangements are in place and that the processor provides sufficient guarantees regarding security and compliance.

Only information necessary for the purpose will be shared.

Data sharing will take account of safeguarding responsibilities and will not be delayed unnecessarily where sharing is necessary to protect a child or another person.

ARTIFICIAL INTELLIGENCE (AI)

The Academy recognises that AI tools can support teaching, learning and administration but may create risks to personal data and privacy.

Staff, pupils and other users must not enter personal, confidential or sensitive Academy information into unauthorised AI tools.

Unauthorised disclosure of personal data through an AI tool will be treated as a potential data breach and reported immediately.

Before introducing an AI system that processes personal data, the Academy will:

- consult the DPO
- consider data protection risks
- complete a DPIA where required
- assess the supplier's data-processing arrangements
- consider where data is stored and whether it is transferred internationally
- establish how data is used, including whether it is used to train an AI model
- ensure appropriate security, transparency and access controls are in place

AI systems will be reviewed when significant changes are made to their functionality or data processing.

FILTERING AND MONITORING

The Academy uses filtering and monitoring systems as part of its safeguarding and online safety arrangements.

Filtering and monitoring may generate personal data, including information about users' online activity, searches, alerts and reports.

The Academy will ensure that:

- filtering and monitoring are lawful, proportionate and transparent
- only authorised staff can access monitoring information
- staff with access receive appropriate training
- information is retained only for as long as necessary
- safeguarding procedures are in place for responding to alerts
- third-party providers are appropriately assessed
- DPIAs are completed before introducing a new filtering or monitoring system or making significant changes to an existing system, where required
- privacy notices explain what is monitored, why it is monitored, who can access information and relevant retention arrangements

Filtering and monitoring arrangements will support the Academy's safeguarding responsibilities and will not be used in a way that is disproportionate to the purpose for which the information is processed.

INTERNATIONAL TRANSFERS

The Academy may use suppliers or systems that process personal data outside the UK.

Before transferring personal data internationally, the Academy will establish:

- where the data will be processed
- the purpose of the transfer
- whether an adequacy decision or other lawful transfer mechanism applies
- what contractual and technical safeguards are required
- whether any additional risks need to be addressed
-

Transfers outside the UK will only take place where permitted under the applicable requirements of UK data protection legislation.

Where required, the Academy may use appropriate safeguards such as the UK International Data Transfer Agreement (IDTA) **or** UK Addendum to EU Standard Contractual Clauses.

The Academy will not assume that processing within the EEA automatically provides the necessary safeguards.

INDIVIDUALS' DATA PROTECTION RIGHTS

Individuals have rights under data protection legislation, depending on the circumstances.

These may include the right to:

- access personal data
- have inaccurate personal data corrected
- have personal data erased in certain circumstances
- restrict processing in certain circumstances
- object to certain processing
- withdraw consent where consent is the lawful basis
- request data portability where applicable
- object to certain automated decision-making and profiling
- receive information about international transfers where applicable

The Academy will consider each request according to the relevant legal requirements.

Requests may be made verbally or in writing.

Staff who receive an information rights request must immediately refer it to the Academy's designated contact.

The Academy may need to verify the identity of the requester before responding.

The Academy will normally respond to a valid subject access request within one month. This may be extended by up to two further months where permitted because of the complexity or number of requests.

The Academy may refuse or charge a reasonable fee for a request where permitted by law, including where a request is manifestly unfounded or excessive.

Requests will not automatically be considered excessive simply because they are repeated. Each request will be considered on its circumstances and in accordance with current data protection law.

CHILDREN AND DATA PROTECTION RIGHTS

Children have their own data protection rights.

The Academy recognises that children may exercise their rights themselves where they have sufficient understanding to do so.

When considering a request made by a parent/carers on behalf of a child, the Academy will consider:

- the child's age
- the child's maturity and understanding
- the nature of the information requested
- the child's best interests
- any relevant safeguarding considerations
- whether the parent/carers has appropriate authority to make the request

There is no fixed age at which a child automatically has sufficient understanding to exercise their data protection rights.

The Academy will therefore consider requests on a case-by-case basis.

Where appropriate, the Academy will provide children with age-appropriate information about their privacy and data protection rights.

REQUESTS FOR EDUCATIONAL INFORMATION

Gateway Academy is an Academy and is therefore not subject to the Education (Pupil Information) (England) Regulations 2005 in the same way as maintained schools.

Parents/carers do not have the same statutory right to access an educational record under those Regulations as they would in a maintained school.

Requests for personal information about a pupil will normally be considered under data protection legislation, including the right of access.

The Academy may provide information to parents/carers where appropriate, taking account of the child's age, maturity, understanding, best interests and any safeguarding considerations.

Requests should be directed to the Academy's designated contact for information rights requests.

CCTV

The Academy uses CCTV at its premises for purposes including safeguarding, security and the prevention and detection of crime.

CCTV will be operated in accordance with data protection law and the Academy's CCTV Policy.

Appropriate signage will be displayed to inform individuals that CCTV is in operation and provide information about how further information can be obtained.

Access to CCTV footage will be restricted to authorised individuals.

CCTV footage will only be retained for as long as necessary and in accordance with the Academy's retention arrangements.

See the Academy's CCTV Policy for further information.

PHOTOGRAPHS AND VIDEOS

The Academy may take photographs and videos as part of its educational, communication, safeguarding and promotional activities.

The Academy will identify an appropriate lawful basis for each use.

Where consent is relied upon, consent will be freely given and individuals will be informed about how images will be used.

For pupils, the Academy will explain the use of images in an age-appropriate way to the pupil and parent/carer where appropriate.

Consent can be withdrawn where consent is the lawful basis.

The Academy will not assume that consent for one use automatically applies to another use.

Images and videos will be stored securely and retained in accordance with the Academy's retention arrangements.

Further information is provided in the Safeguarding and Child Protection Policy and relevant privacy notices.

DATA PROTECTION BY DESIGN AND DEFAULT

The Academy will build data protection into new systems, processes and activities from the outset.

This includes:

- minimising the personal data collected
- restricting access to those who need it
- considering privacy and security risks
- consulting the DPO
- completing DPIAs where required
- maintaining appropriate records
- reviewing suppliers and processors
- reviewing privacy notices
- considering retention and deletion arrangements

A DPIA will be completed where processing is likely to result in a high risk to individuals' rights and freedoms.

This will include consideration of new technologies, large-scale processing of sensitive information, biometric systems, filtering and monitoring systems and other high-risk processing.

EDUCATIONAL TECHNOLOGY (EDTECH)

Before procuring or introducing educational technology that processes personal data, the Academy will consider:

- what personal data the system processes
- why the data is required
- the lawful basis
- security arrangements
- retention and deletion
- who can access the information
- whether information is shared with third parties
- whether data is transferred internationally
- whether AI is used

- whether the supplier uses data to train AI models
- safeguarding and filtering/monitoring arrangements
- whether a DPIA is required

The DPO will be consulted at an early stage when new EdTech is being considered.

The Academy will monitor significant changes to suppliers and systems and will update privacy information where required.

DATA SECURITY AND STORAGE

The Academy will take appropriate technical and organisational measures to protect personal data against:

- unauthorised or unlawful processing
- unauthorised access
- accidental loss
- destruction
- alteration
- disclosure or damage

Measures include, where appropriate:

- secure storage of paper records
- clear desk arrangements
- appropriate access controls
- secure passwords and authentication
- encryption
- secure devices
- secure systems and networks
- appropriate permissions
- secure sharing arrangements
- staff training
- regular review of access rights

Personal data must not be stored on personal devices unless specifically authorised and appropriately secured in accordance with Academy policies.

Staff must not use personal email accounts to store or routinely process Academy personal data.

Technical security requirements will be maintained through the Academy's relevant IT, cyber security and acceptable use arrangements and will be reviewed as technology changes.

DISPOSAL AND RETENTION

Personal data will not be kept for longer than necessary.

The Academy's Data Retention Schedule sets out appropriate retention periods.

When information reaches the end of its retention period, it will be securely destroyed, deleted or anonymised as appropriate.

Paper records will be securely shredded or disposed of through an approved confidential waste service.

Electronic information will be securely deleted or otherwise disposed of in accordance with the relevant system and security requirements.

Where an external organisation disposes of personal data on the Academy's behalf, the Academy will ensure that appropriate contractual and security arrangements are in place.

Where required, records of destruction will be maintained.

PERSONAL DATA BREACHES

All actual or suspected personal data breaches must be reported immediately to the Academy's Data Protection Lead.

Examples include:

- sending personal information to the wrong person
- leaving confidential information unattended
- losing a device containing personal data
- unauthorised access to personal information
- accidentally publishing personal information
- inappropriate disclosure of safeguarding information
- entering personal or sensitive information into an unauthorised AI system

All breaches will be logged and investigated.

The Academy will assess the potential risk to individuals and take appropriate remedial action.

The DPO will be consulted as appropriate.

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

Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals will be informed without undue delay where required by law.

The Academy will not automatically notify affected individuals simply because a breach has occurred; notification will depend on the legal risk assessment.

Full procedures are set out in the Academy's Breach Management Policy.

DATA PROTECTION COMPLAINTS

The Academy takes concerns about the collection and use of personal information seriously.

Anyone who has concerns about how the Academy is processing their personal data may make a data protection complaint to the Academy or its Data Protection Officer.

Complaints may be made by contacting:

Data Protection Officer: Claire Mehegan

Grow Education Partners Ltd

Email: DPO@groweducationpartners.com

Telephone: 020 7554 2806

The Academy will:

- provide a clear and accessible way to make a complaint
- acknowledge the complaint within **30 days**
- investigate the complaint appropriately and without undue delay
- keep the complainant informed of progress where appropriate
- communicate the outcome of the complaint without undue delay

Data protection complaints will be handled separately from the Academy's general complaints procedure where appropriate.

If an individual remains dissatisfied, they may raise their concern with the Information Commissioner's Office (ICO).

TRAINING

All staff and governors will receive appropriate data protection training as part of induction.

Refresher training will be provided periodically and when required because of:

- changes in legislation
- changes in ICO or DfE guidance
- significant changes to Academy systems or processes
- identified training needs
- data protection incidents

Records of training will be maintained.

Staff who have particular responsibilities for handling personal data will receive additional training where appropriate.

MONITORING AND REVIEW

The DPO will monitor compliance with this policy and provide advice and recommendations to the Academy.

The Academy will undertake appropriate monitoring, auditing and review of its data protection arrangements.

The policy will be reviewed at least annually and sooner where there are significant changes to:

- legislation
- ICO or DfE guidance
- Academy systems
- data processing activities
- identified risks

The Governing Board will approve significant changes to the policy.

The policy will be published on the Academy website.

RELATED POLICIES AND DOCUMENTS

This policy should be read alongside:

- Privacy Notices
- Data Retention Policy/Retention Schedule
- Data Breach Management Policy
- CCTV Policy
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Acceptable Use Policy
- Acceptable Use of AI Policy
- ICT/IT Security Policy
- Email Use Policy
- Records Management arrangements
- Freedom of Information Publication Scheme
- Disaster Recovery/Business Continuity Plan
- Risk Register
- relevant Data Sharing and Processor Agreements
- relevant DPIAs
- Record of Processing Activities (RoPA).