

Gateway Academy



Confidentiality Policy



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

AIMS

This policy sets out how the Academy manages confidential information to protect the privacy, welfare and safety of pupils, staff and families. It explains how confidential information is handled, shared, stored and disposed of in accordance with safeguarding requirements and data protection law.

LEGAL AND REGULATORY FRAMEWORK

This policy is informed by:

- Keeping Children Safe in Education 2026 (DfE)
- Working Together to Safeguard Children 2026
- Information Sharing: Advice for Practitioners Providing Safeguarding Services
- Children Act 1989 and Children Act 2004
- Education Act 2002
- Data Protection Act 2018 and UK GDPR
- Academy Trust Handbook 2026
- Information and Records Management Society (IRMS) Schools Retention Schedule

The policy should be read alongside the Academy's Child Protection and Safeguarding Policy, Data Protection Policy, Whistleblowing Policy, Online Safety Policy and Records Management arrangements.

SCOPE

This policy applies to all staff, governors, volunteers, supply staff, students on placement and external professionals working with or on behalf of the Academy.

It applies to confidential information shared verbally, in writing, electronically or through digital systems.

PRINCIPLES

The Academy will:

- Respect confidentiality and only share information where there is a legitimate and lawful reason to do so.
- Share information on a need-to-know basis and only the information necessary for the purpose.
- Recognise that confidentiality must not prevent information being shared where this is necessary to safeguard a child or protect others.
- Handle personal information in accordance with data protection law and the Academy's Data Protection Policy.
- Take appropriate technical, organisational and physical measures to protect confidential information from unauthorised access, loss, damage or disclosure.

CONFIDENTIALITY AND SAFEGUARDING

Staff must never promise a pupil absolute confidentiality.

If a pupil or other person discloses information that may indicate a safeguarding concern, the information must be shared promptly with the Designated Safeguarding Lead (DSL) or, where appropriate, another member of the safeguarding team.

Information must be shared where necessary to protect a child or prevent harm. Staff should not delay sharing information because consent has not been obtained where there is a lawful safeguarding basis for sharing.

The Academy will follow current statutory information-sharing guidance. The statutory Information Sharing Duty under section 16LA of the Children Act 2004 comes into force on 30 September 2026. Where there is an immediate risk of harm, staff should take appropriate action without delay in accordance with the Academy's safeguarding procedures.

STAFF RESPONSIBILITIES

Staff must:

- Keep confidential information secure and only access information necessary for their role.
- Avoid discussing confidential matters where they may be overheard by unauthorised people.
- Not share passwords or access confidential systems using another person's account.
- Take care when sending emails, documents or other information to ensure that information is shared with the correct recipient.
- Report any actual or suspected loss, unauthorised disclosure or data breach in accordance with the Academy's Data Protection Policy.
- Follow the Academy's clear desk and clear screen arrangements.

Confidential information must not be discussed with parents, colleagues, pupils or other third parties unless there is a legitimate reason and the individual is authorised to receive it.

GOVERNORS AND MEETINGS

Governors must maintain the confidentiality of information obtained through their role.

Confidential matters concerning individual pupils, staff or other sensitive issues must be treated appropriately and excluded from published minutes where permitted or required. Confidential papers and records must be stored securely and only shared with authorised individuals.

The Academy Trust Handbook permits confidential matters, including those relating to named pupils, staff or matters which trustees consider should remain confidential, to be excluded from published meeting information.

WHISTLEBLOWING

Confidentiality must not prevent staff from raising concerns about safeguarding, malpractice, fraud, wrongdoing or other matters covered by the Academy's Whistleblowing Policy.

Staff will not be prevented from making a protected disclosure where they have a legal right to do so.

SECURE STORAGE AND RECORDS

Confidential information must be stored securely using appropriate physical and technical controls. Paper records must be kept securely and not left unattended. Digital information must be protected through appropriate access controls, passwords and other security measures appropriate to the sensitivity of the information.

Records must be retained and securely disposed of in accordance with the Academy's records retention arrangements and the applicable retention schedule.

DATA PROTECTION

The Academy processes personal information in accordance with the Data Protection Act 2018, UK GDPR and the Academy's Data Protection Policy.

Individuals have data protection rights, including rights of access and, where applicable, rectification, erasure and restriction of processing. These rights are subject to legal conditions and exemptions.

Requests concerning personal information will be managed in accordance with the Academy's Data Protection Policy and advice from the Data Protection Officer (DPO).

ROLES AND RESPONSIBILITIES

Designated Safeguarding Lead (DSL)

Leads on safeguarding concerns and ensures relevant information is shared appropriately to protect children.

All Staff

Are responsible for maintaining confidentiality, handling information securely and reporting safeguarding concerns or data breaches promptly.

Governors

Are responsible for ensuring appropriate arrangements are in place for confidentiality, information governance and safeguarding.

Data Protection Officer (DPO)

Provides advice on data protection, information rights, data sharing and data breaches and supports compliance with data protection legislation.

Monitoring and Review

The policy will be reviewed annually, or sooner where legislation, statutory guidance or Academy arrangements change.

The Academy will ensure that staff and governors are aware of their responsibilities under this policy.