Abbey Multi Academy Trust

Policies & Procedures

Data Protection Complaints Policy

Our approach to resolving concerns about personal information

Approved on	18 March 2026
Approved by	Abbey MAT Board of Trustees
Next review due	31 March 2027

In Partnership to
Educate, Nurture and Empower

Data Protection Complaints Policy

Contents

1. Introduction 3
2. Scope and purpose 3
3. Accessibility and making a complaint 3
4. Key principles 3
5. Acknowledgement and statutory timescales 4
6. Investigation process 4
7. Complaints involving children 4
8. Outcome and response 5
9. Escalation and ICO rights 5
10. Record keeping and accountability 5
11. Roles and responsibilities 5
12. Relationship with other Trust procedures 5
13. Review 6
Appendix 1: Data protection complaint process map 7
Appendix 2: Roles and responsibilities matrix 8
Appendix 3: Decision-making principles for complaints involving children's personal information 11

Data Protection Complaints Policy

1. Introduction

Abbey Multi Academy Trust is committed to handling personal information lawfully, fairly and transparently. This policy explains how the Trust manages complaints relating to the use of personal data and sets out the procedure followed when concerns are raised about data protection matters.

This procedure is established under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the statutory framework governing data protection complaints. It provides a dedicated route for data protection concerns and operates separately from the Trust's general school complaints procedure.

2. Scope and purpose

A data protection complaint is any concern about how personal data has been collected, used, stored, shared, retained or otherwise handled by the Trust or one of its academies. This may include concerns about access to information, accuracy of records, data sharing, data security or the exercise of individual data rights.

This procedure applies whenever a complaint relates to personal information held or processed by the Trust. Where a complaint includes both data protection issues and wider educational or service concerns, the Trust may separate these elements so that data protection matters are handled under this policy while other issues follow the relevant school procedure.

3. Accessibility and making a complaint

The Trust aims to make the process for raising data protection concerns clear and accessible. Complaints may be made using the Trust's online form, by email, in writing or verbally. Where a complaint is made verbally, staff will assist in recording the concern so that it can be processed appropriately.

All data protection complaints are overseen by the Trust's Data Protection Officer, who acts as the lead adviser on compliance and investigation.

4. Key principles

When handling data protection complaints, the Trust will act in accordance with the principles of fairness, transparency, proportionality and accountability. Complaints will be acknowledged, considered carefully and investigated without undue delay. The Trust will ensure that complainants are informed about the progress and outcome of their complaint and will maintain clear records of decisions taken and actions carried out.

This process is designed to resolve concerns wherever possible at Trust level, while recognising the right of individuals to approach the Information Commissioner's Office (ICO) if they remain dissatisfied.

5. Acknowledgement and statutory timescales

In accordance with statutory requirements, the Trust will normally acknowledge receipt of a data protection complaint within 30 days. This acknowledgement confirms that the complaint has been received and is being reviewed under the Trust's data protection complaints procedure.

The statutory requirement applies to acknowledgement rather than completion of the investigation. The Trust will progress investigations without undue delay, recognising that timescales may vary depending on complexity and the nature of the information involved.

6. Investigation process

Upon receipt of a complaint, the Data Protection Officer will undertake an initial review to understand the issues raised, identify any immediate risks, and determine what further enquiries are required. The investigation will be proportionate to the nature of the concern and may include reviewing records, speaking with relevant staff, considering applicable policies, and examining the lawful basis for processing personal data.

Where further information is needed, the complainant may be contacted for clarification. The Trust will keep the complainant informed if investigations take longer than expected and will ensure that communication remains clear and professional throughout.

Where concerns overlap with safeguarding or child protection matters, the Trust will work alongside safeguarding leads to ensure that decisions appropriately protect individuals while remaining compliant with data protection law.

7. Complaints involving children

The Trust recognises that children may have the ability to exercise their own data protection rights where they have sufficient understanding and maturity. When complaints relate to a child's personal data, consideration will be given to the child's capacity to make decisions about their information.

Children aged 13 and over are generally more likely to have such capacity, although decisions will always be made on a case-by-case basis. Parental responsibility does not automatically override the wishes of a child who is assessed as capable of making their own decisions. The Trust will balance legal rights, the best interests of the child, and safeguarding considerations when determining how to proceed.

8. Outcome and response

At the conclusion of an investigation, the Trust will provide a clear written response explaining the outcome of the complaint. This will include an explanation of what was considered, any actions taken, and the reasons for decisions made. Where appropriate, the Trust may apologise, correct information, adjust processes or take steps to prevent similar issues from arising.

The Trust aims to resolve complaints fairly and constructively, recognising that the purpose of the process is to address concerns and improve practice rather than assign blame.

9. Escalation and ICO rights

If a complainant remains dissatisfied with the Trust's response, they have the right to raise their concern with the Information Commissioner's Office (ICO), which is the UK's independent regulator for data protection.

The Trust encourages individuals to contact the Data Protection Officer first if any aspect of the response is unclear or if further discussion may help resolve the issue.

10. Record keeping and accountability

The Trust will maintain records of data protection complaints, including dates received, acknowledgement, investigation steps, decisions reached and actions taken. These records form part of the Trust's accountability obligations under data protection law and will be retained in line with the Trust's data retention schedule.

Information gathered during a complaint investigation may be used to identify patterns, training needs and opportunities for organisational improvement.

11. Roles and responsibilities

The Data Protection Officer is responsible for overseeing the complaints process, ensuring legal compliance and advising on complex or high-risk matters. Senior Trust leaders retain overall accountability for ensuring that appropriate systems and resources are in place to support effective handling of complaints.

All staff are responsible for recognising potential data protection complaints and referring them promptly to the Data Protection Officer. Staff should not make independent decisions regarding legal rights or disclosures without appropriate guidance.

12. Relationship with other Trust procedures

This policy operates independently from the Trust's general complaints procedure. Data protection complaints are not progressed through school complaint

escalation routes or governor panels, as they are handled under statutory data protection processes.

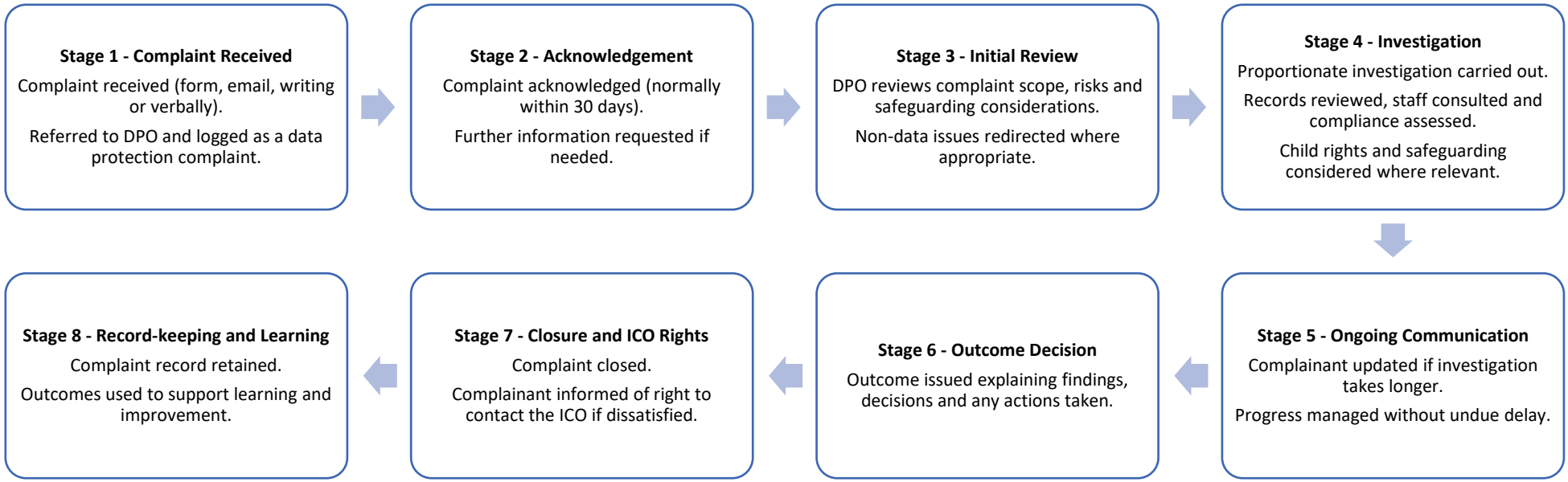
This policy should be read alongside the Trust's Data Protection Policy, Privacy Notices, Record Retention Policy and Safeguarding Policies.

13. Review

This policy will be reviewed annually or sooner where legislation, ICO guidance or Trust practice requires amendment.

Appendix 1: Data protection complaint process map

Statutory process for handling data protection complaints, separate from the school complaints procedure



Appendix 2: Roles and responsibilities matrix

This matrix clarifies roles and decision-making responsibilities when handling data protection complaints:

ROLE	RESPONSIBILITIES
Data Protection Officer (DPO)	Leads the handling of data protection complaints, oversees investigations, and ensures compliance with data protection law.
Headteacher / Academy Leader	Supports investigations by providing information and ensuring school cooperation.
Designated Safeguarding Lead (DSL)	Advises where safeguarding issues may affect decisions or information sharing.
Senior Information Risk Owner (SIRO) / Accounting Officer	Provides strategic oversight of information risk and supports decision-making in high-risk cases.
CEO / Executive Leadership	Maintains overall organisational accountability and ensures appropriate governance arrangements are in place.
Staff	Recognise potential data protection complaints and refer them promptly to the DPO.
Trustees / Governors	Provide strategic oversight of compliance but do not hear individual data protection complaints.

Process oversight summary:

The Trust's governance approach to data protection complaints ensures that:

- legal compliance is led by the DPO
- operational knowledge comes from academies
- safeguarding expertise is included where required
- leadership oversight exists for risk and accountability
- statutory independence of the data protection complaints process is maintained

Roles and responsibilities in more detail:

Data Protection Officer (DPO)

The Data Protection Officer leads the handling of data protection complaints across the Trust. The DPO is responsible for ensuring the process complies with data protection law and statutory requirements. This includes logging complaints,

overseeing investigations, advising on lawful processing, considering child data rights and determining appropriate outcomes.

The DPO may request information from academies or Trust departments and will coordinate responses where complaints involve more than one area. The DPO is responsible for ensuring complainants receive a clear outcome and are informed of their right to approach the Information Commissioner's Office (ICO).

Headteacher / Academy Leader

The Headteacher or Academy Leader supports the investigation by providing information, context and access to relevant staff or records. They are responsible for ensuring that school-level cooperation is timely and accurate.

Headteachers do not make legal decisions about data protection rights or determine outcomes independently. Where issues arise that may affect school operations or reputation, the Headteacher works collaboratively with the DPO.

Designated Safeguarding Lead (DSL)

The DSL provides advice where a complaint overlaps with safeguarding or child protection matters. Safeguarding considerations may influence what information can be disclosed or how a complaint is progressed.

The DSL does not decide data protection matters but ensures that safeguarding risks are appropriately considered within the investigation.

Trust Senior Leadership (Co-CEOs / Executive Team)

Senior leaders maintain overall organisational accountability for compliance and ensure sufficient resources and governance arrangements are in place. They are consulted where complaints present significant organisational risk or reputational impact.

Senior leaders are not normally involved in individual complaint decision-making unless escalation is required for governance or risk management reasons.

Senior Information Risk Owner (SIRO)

Where appointed, the Senior Information Risk Owner (SIRO) provides strategic oversight of information risk and will be consulted in high-risk cases, including serious data breaches or matters likely to involve regulatory scrutiny.

The SIRO supports organisational learning and risk management rather than day-to-day complaint handling.

Where the Trust has not appointed a SIRO, the Accounting Officer will fulfil this role and assume responsibility for strategic oversight of information risk.

School and Trust Staff

All staff have responsibility for recognising when a concern relates to personal data and ensuring that it is referred promptly to the Data Protection Officer. Staff must cooperate with investigations and provide accurate information when requested.

Staff should not make independent decisions about disclosure, refusal of rights, or legal interpretations of data protection law.

Governors / Trustees

Governors and Trustees provide strategic oversight of compliance but do not act as a complaint appeal panel for data protection complaints. Data protection complaints are handled under statutory processes and overseen by the Data Protection Officer.

Governance oversight is maintained through policy review, reporting and assurance rather than individual case decisions.

Appendix 3: Decision-making principles for complaints involving children's personal information

Purpose

This appendix sets out the principles the Trust applies when handling data protection complaints that involve children. It supports consistent and lawful decision-making where issues arise about consent, parental involvement, or access to a child's personal data.

These principles are applied by the Data Protection Officer (DPO) in consultation with relevant safeguarding and school leaders where appropriate.

1. General principle

Children have data protection rights in their own right. The Trust recognises that, depending on their understanding and maturity, children may be able to make decisions about how their personal information is used.

Decisions are based on the individual circumstances of each case rather than age alone.

2. Capacity and understanding

When a complaint involves a child's personal data, the Trust considers whether the child has sufficient understanding to exercise their own rights. This assessment takes account of factors such as age, maturity, ability to understand the issue, and the complexity or sensitivity of the information involved.

Children aged 13 and over are generally more likely to have the capacity to make their own decisions about personal data; however, this is not automatic and each case is assessed individually.

Where a child is assessed as capable of making their own decision, their views will normally carry significant weight.

3. Role of parents and carers

Parents and those with parental responsibility play an important role in supporting children and may raise complaints on a child's behalf, particularly where younger children are involved.

However, parental responsibility does not automatically give a right to override the wishes of a child who is considered capable of exercising their own data protection rights. The Trust will balance parental involvement with the child's rights and best interests.

Where there is uncertainty about authority to act, the Trust may request further information before proceeding.

4. Disagreement between parent and child

Where a parent and child disagree about how personal data should be used or disclosed, the Trust will carefully consider:

- whether the child has sufficient understanding to decide
- the potential impact on the child
- safeguarding considerations
- the nature of the information requested or disputed

The DPO will document the reasoning behind decisions and may seek advice from safeguarding or senior leaders where necessary.

5. Safeguarding considerations

Safeguarding and child welfare always remain central to decision-making. In some circumstances, sharing or withholding information may be necessary to protect a child or another individual.

Where safeguarding concerns exist, the Designated Safeguarding Lead (DSL) will be consulted. Decisions may limit disclosure or alter how a complaint is progressed where this is necessary for safety or welfare.

Safeguarding considerations may override usual expectations of disclosure where required by law or professional duty.

6. Communication with children

Where appropriate, the Trust will communicate directly with children in language suitable for their age and understanding. The Trust aims to ensure that children understand what decisions are being made about their personal data and why.

7. Recording decisions

Where a complaint involves a child, the Trust will record:

- how capacity was considered
- whether parental authority was relevant
- any safeguarding advice obtained
- the reasoning behind the final decision

This supports accountability and transparency and demonstrates compliance with data protection obligations.

8. Principle of proportionality

Decisions relating to children's data will be proportionate to the nature of the complaint and the potential impact on the child. The Trust aims to balance legal rights, safeguarding duties and practical realities in a fair and reasonable manner.

9. Summary of approach

In practice, the Trust applies the following principles:

- children may have their own data rights
- capacity depends on understanding, not age alone
- parental responsibility is important but not absolute
- safeguarding considerations may influence decisions
- clear reasoning must be recorded