DDAT

Derby Diocesan Academy Trust

Data Protection Policy

May 2026

Approved by Trust Board on: 23rd October 2026

Review date: May 2027

Contents

1. Introducing our DP Policy 4
2. Scope and Responsibilities 4
3. DP Legislation & Regulator 4
4. Our DP Objectives 5
5. Our DP Rules 5
6. Rights: 7
7. Data sharing 8
8. Non-UK data transfers 8
9. Data protection breaches and incidents 9
10. Artificial Intelligence (AI) 9

Annexe.1 Legal Conditions for Processing 10
- A1.1 Introduction 10
- A1.2 Our role and basis for processing 10
- A1.3 Data Subjects' Rights 11

Annexe.2 Data Protection - Personal Data Breach Procedure (including Cyber Incidents) 12
- A2.1 Introduction 12
- A2.2 Scope and Responsibilities 12
- A2.3 What is a Personal Data Breach? 12
- A2.4 Breach / Incident Response Plan 12

Annexe.3 Data Protection Impact Assessment Guidance 16
- A3.1 Introduction 16
- A3.2 What is a Data Protection Impact Assessment (DPIA)? 17
- A3.3 When will a DPIA be appropriate? 17
- A3.4 The Benefits of a DPIA 17
- A3.5 Steps to be followed when considering a new project 18
- A3.6 Monitoring 18

Annexe.4 Subject Access Request (SAR) Procedure 18
- A4.1 Introduction 18
- A4.2 Scope and Responsibilities 19
- A4.3 Receiving a valid SAR 19
- A4.4 Responding to a SAR 20
- A4.5 Exemptions 20
- A4.6 SAR Request Form 21

Annexe.5 Requests under the Freedom of Information Act 2000 / Environmental Information Regulations 2004 24
- A5.1 Introduction: what a publication scheme is and why it has been developed 24
- A5.2 Values 25
- A5.3 Categories of information published 26

A5.4 Classes of Information Currently Published 26
A5.5 How to request information 27
A5.6 Advice & Assistance 28
A5.7 Paying for information 30
A5.8 Feedback and Complaints 30
Annexe.6 Data Protection Complaints Policy 31
A6.1 Purpose 31
A6.2 Scope 31
A6.3 How to Make a Complaint 31
A6.4 Acknowledgement and Response Timeline 31
A6.5 Investigation Process 31
A6.6 Contestability and Redress 32
A6.7 Record Keeping 32
A6.8 Escalation 32
A6.9 Staff Training 32

All Education Data Hub policies, procedures and guidance notes should be read in conjunction with the relevant HR advice and guidance.

1. Introducing our DP Policy

1.1 Our Data Protection (DP) Policy lays out our approach to data protection. We recognise the importance of protecting the personal data we are entrusted with, and this policy sets out how we comply with relevant legislation.

1.2. If you have any queries about this Policy, please contact our Data Lead Kieren Done whose details can be found in our Privacy Notices.

2. Scope and Responsibilities

2.1. This Policy applies to all staff, including temporary staff, consultants, LTC members/trustees, volunteers, and contractors, and anyone else working on our behalf.

2.2. All staff are responsible for reading and understanding this policy before carrying out tasks that involve handling personal data, and for following this policy, including reporting any suspected breaches of it to our Data Protection Officer.

2.3. All leaders are responsible for ensuring their team read and understand this policy before carrying out tasks that involve handling personal data, and that they follow this policy, including reporting any suspected breaches of it.

2.4. Our Data Protection Officer is responsible for advising us about our data protection obligations, dealing with breaches of this policy, including suspected breaches, incidents, identified risks, and monitoring compliance with this policy. Our Data Protection Officer is impartial and any other duties they perform must:

- be compatible with their duties as a data protection officer.
- not lead to a conflict of interest.

3. DP Legislation & Regulator

3.1. Relevant legislation includes, but is not limited to:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018 (DPA 2018), which enacts the GDPR in the UK and includes exemptions and further detail, as well as offences that individuals can be prosecuted for;
- Privacy and Electronic Communications Regulations (PECR), which cover electronic direct marketing (“marketing” includes fundraising and promoting an organisation’s aims, not just selling.)
- Freedom of Information Act 2000, which provides key definitions referred to in the other legislation.
- Environmental Information Regulations 2004
- Human Rights Act 1998
- Computer Misuse Act 1990, which covers unauthorised access to, and use of, computers and computer materials.
- Education (Pupil Information) Regulations 2005 which gives parents the right to access their child’s education record.
- The School Attendance (Pupil Registration) (England) Regulations 2024
- Protection of Freedoms Act 2012 – for further details see our Protection of Biometric Information document.
- The Data (Use and Access) Act 2025
- Children's Wellbeing and Schools Bill (anticipated to be passed in 2025)

3.2. In the UK, the Information Commissioner's Office (ICO) is the data protection regulator.

3.3. Breaches of data protection legislation can result in significant monetary penalties and damage to reputation, as well as the risk of real harm to people whose data is handled in an unfair or unlawful way.

3.4. Individual members of staff may be prosecuted for committing offences under Sections 170 – 173 of the DPA 2018.

3.5. The Data (Use and Access) Act inserts Section 164A into the DPA 2018 which means organisations must:

- give people a way of making data protection complaints;
- acknowledge receipt of complaints within 30 days of receipt;
- without undue delay, take appropriate steps to respond to complaints, including making appropriate enquiries, and complainants informed; and
- without undue delay, tell complainants the outcome of their complaints.

4. Our DP Objectives

We are committed to making sure that:

4.1 Personal data is only processed in keeping with legal data protection principles. The principles include: data being processed lawfully, fairly and in a transparent manner; data being processed only for specific, explicit and valid purposes; data being adequate, relevant and accurate; data not being kept longer than is necessary; and data being kept secure;

4.2 We adopt a "Privacy by Design" and "Privacy by Default" approach;

4.3 We can demonstrate our accountability and compliance;

4.4 The people whose data we hold (Data Subjects) understand the ways and reasons why we process their data, and can easily and fairly exercise their rights around their data;

4.5 We only share personal data when it is fair and lawful to do so, and when we share data we do it in a safe and secure way;

4.6 Data is not transferred outside of the UK except where the country has an 'adequacy decision' or the transfer is covered by 'appropriate safeguards', as defined in UK GDPR Article 46, or there is a specific situation that allows the transfer as defined by UK GDPR Article 49;

4.7 All data breaches, including near misses, are managed properly and reported appropriately, so we can minimise any risks and improve practices in the future. This includes any breaches of the Data Protection Act (DPA 2018) where the individual responsible may be liable.

5. Our DP Rules

5.1 We follow the legal Data Protection Principles:

i. **Fair, lawful and transparent processing**: The reason for processing personal data must meet one of the legal conditions listed in Article 6 of the UK GDPR. In addition, when "special categories" of personal data are being processed, the purpose must also meet one of the legal conditions listed in Article 9 of the UK GDPR. "Special categories" are information about a person's race or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life or sexual orientation, or genetic and biometric data.

Legal conditions: See Annexe 1 for an explanation of the Legal Conditions for Processing.

Other legislation: All processing must also comply with the other DP Principles and any other relevant legislation, including the DPA 2018 and the Privacy and Electronic Communications Regulations (PECR) as appropriate. Any individual who obtains, discloses or retains data when they do not have permission to do so may be committing an offence under the DPA 2018 Section 170. All electronic "direct marketing" is subject to the PECR, which require us to obtain consent before sending direct marketing messages electronically by email or SMS ("marketing" includes fundraising and similar types of messages, not just selling.)

Transparency: To be fair and transparent, our data processing, including how and why we process data, is explained in our Privacy Notices. We also explain how and why data will be processed at the point where we collect that data, as much as is reasonably possible, and especially if the processing is likely to be unexpected.

ii. **Purpose limitations**: We only use the data we collect for the reasons we explained in our privacy notice. If we need to use it for another reason, we must inform our data subjects of the new reason for processing before we do it.

iii. **Data limitations**: We minimise the amount of data that we collect and process, keeping it to only what is necessary for the reasons we are collecting it. We must not collect or retain any personal data "just in case".

iv. **Data accuracy**: We must take reasonable steps to ensure that the personal data we collect and hold is accurate and, where necessary, kept up to date.

v. **Data retention**: We only keep personal data for as long as is necessary for the reasons for which we are processing it, and we must be transparent with our data retention schedules which can be found here https://ddat.org.uk/gdpr/ . Any individual who purposefully retains data that they do not have authority for may be committing an offence under the DPA 2018 Section 170.

vi. **Data security & integrity**: We use both technical and organisational security measures to protect data from unauthorised or unlawful processing, or from accidental loss, destruction or damage. Security measures must be appropriate to the level of risk involved in the data and the processing. Our measures include, but are not limited to: technical measures such as ICT systems security, ICT access controls, pseudonymisation, and encryption; and organisational measures such as business continuity plans, physical security of our premises and data, policies, procedures, training, audits and reviews.

Security is considered at all times. This includes when data is being stored, used, transferred, or disposed of, whether the data is electronic or hard copy, and regardless of how and where the data is being accessed and stored, especially when data is sent or taken off site, or to another organisation.

Any individual who purposefully re-identifies pseudonymised information without permission may be committing an offence under the DPA 2018 Section 171.

Organisational measures include extensive staff training. All staff are trained. This training is delivered live and covers all aspects of Data Protection awareness. Key themes are explained, including lawful basis, consent, and breach and subject access request awareness. The training is based on 'lessons learned' from other schools, action taken by the ICO and incidents reported in the press. There is discussion, questions and debate. It includes an assessment which must be passed (75% is the pass score), the school holds a register of attendance and scores.

This training is delivered in full every two years with refresher updates shared in between. A refresher 'inset' day pre-recorded presentation from the DPO is provided every September.

In addition, there is role-based training for Senior staff, Designated Safeguarding Leads, LTC members/Trustees, midday supervisors and other casual staff.

Specific areas of compliance are addressed in a Bitesize suite of short courses, accessed regularly by relevant staff.

5.2 Privacy by Design & Default

When we are planning projects or new ways of working that involve processing of personal data, we must consider the data protection implications, and how to make sure we meet legal and good practice requirements, from the planning stages, and keep a record of the outcomes.

For particularly high-risk processing, whether from a new or adapted way of working with personal data, we must do this using formal Data Protection Impact Assessments (DPIAs), to document the risks, decision-making process and decisions made, including recommendations and actions.

High risk processing includes processing the data of children, especially if processing special categories of data about children.

A DPIA is always required before setting up CCTV or biometric systems, or similar tracking technologies.

A DPIA may be carried out retroactively to decide if changes or new controls are needed for existing ways of working.

5.3 To demonstrate and support our compliance with data protection legislation, we keep records of the processing we carry out, we have appropriate policies and procedures in place, we train our staff in data protection, we have a Data Protection Officer in post, we carry out regular audits and reviews of our activities, and we record and investigate data security breaches.

Our records of processing include our contact details and information about why we are processing personal data, what types data we process, the categories of people we process data about, information about how long we hold the data for, and general information about our security measures, as well as the types of external organisations the data is shared with, including any transfers outside of the UK, and the safeguards in place if data is transferred outside the UK.

6. Rights:

We process personal data in line with the legal rights of data subjects', including their right to:

- Be informed about their data being processed, which links to the first DP Principle of fair, lawful and transparent processing;
- Request access to their data that we hold (sometimes requests are known as [Data] Subject Access Requests, or DSARs or SARs);
- Ask for inaccurate data to be rectified;
- Ask for data to be erased (sometimes known as the "right to be forgotten"), in limited circumstances;
- Restrict processing of their data, in limited circumstances;
- Object to the processing, in some circumstances, including stopping their data being used for direct marketing;
- Data portability, which means to receive copies of some of their data in a format that can be easily used by another organisation or person;
- Not be subject to automated decision making or profiling, if it has legal effects or similarly significant effects on the data subjects;
- Withdraw consent when we are relying on consent to process their data;

- Make a complaint to the ICO or seek to enforce their data-related rights through the courts.

We must respond to, and fulfil, all valid requests within one calendar month, unless it is necessary to extend the timescale, by up to two months in certain circumstances. Not all the rights are absolute rights, and we cannot always carry out the requested action in full, or at all. For example, the right to erasure may be limited in some circumstances because we are required to keep some records, and a number of exemptions in the DPA 2018 apply to SARs, meaning we can withhold some information in some situations.

In responding to requests, we also explain to data subjects they have the right to make a complaint to the ICO or seek to enforce their rights through the courts.

Any individual who purposefully alters, defaces, blocks, erases, destroys or conceals information to prevent it being provided in a SAR to a data subject who has requested it, and has a right to receive it, may be committing an offence under the DPA 2018 Section 173.

7. Data sharing

7.1 Data Processors:

We rely on the services of a number of external organisations to support our work (both management and curriculum). These include people, companies, systems and software that process personal data as part of the work they do on our behalf. These are our "data processors". When working with data processors, we carry out appropriate due diligence checks to make sure that they can provide sufficient guarantees that they will comply with data protection legislation, including keeping data secure and cooperating with us to uphold data subjects' rights. We must require contractors and their staff to comply with this DP Policy.

In accordance with UK GDPR Article 28, we must appoint data processors only on the basis of a legally binding, written contract, that requires them to, amongst other things: only process personal data based on our instructions; keep the data secure; assist us to comply with our legal obligations and uphold data subjects' rights; delete or return the data at the end of the contract; and allow inspections and audits of their processing activities. Data Processor contracts, and compliance, must continue to be monitored throughout the contract period. These are sometimes referred to as Data Processing Agreements (DPA).

7.2 Third Parties:

We must only share personal data with any other external organisation, including other data controllers such as agencies and other schools, when the sharing meets one or more appropriate legal condition, and is carried out in keeping with the data protection principles and while upholding the rights of data subjects. Where necessary we should enter into Data Sharing Agreements (DSA), or similar agreements, to help facilitate the sharing of personal data. A DSA does not make the sharing lawful, it only provides a framework to work within, to help share data in an effective and safe way that respects people's data protection rights, when an appropriate and lawful reason to share the data has been identified.

8. Non-UK data transfers

Personal data must not be transferred outside the UK unless it is allowed by the conditions in Chapter V of the UK GDPR, including having appropriate safeguards in place or the transfer being necessary for a specific situation that allows it. A "non-UK transfer" includes storing data on cloud-based software and systems where the servers that are located outside the UK, or where data remains in the UK, but is under the control of a non-UK service provider.

9. Data protection breaches and incidents

a. All breaches, suspected breaches and incidents should be reported immediately to the Data Protection Officer, and must be investigated appropriately, corrective and preventive action taken and recorded. This includes, but is not limited to, any personal data we handle being lost, or being shared, destroyed, changed or put beyond use when it should not be. This also includes Cyber Incidents/Attacks.
b. Specifically, breaches and incidents that are likely to result in a risk to any rights and freedoms of the data subjects affected, must be reported to the ICO within 72 hours of the school becoming aware of them.
c. If a breach or incident is likely to result in a high risk to the rights and freedoms of affected data subjects, we must also tell the data subjects, as soon as possible and without undue delay, to allow them to take any actions that might help to protect them and their data. We will also consider informing data subjects about a breach or incident, even if we are not legally obliged to, if it is appropriate for other reasons, such as preserving open communication.
d. We must log all breaches and incidents, including those that are not reportable to the ICO.

More information relating to data protection breaches and incidents can be found in Annexe.2 Data Protection - Personal Data Breach Procedure (including Cyber Incidents)

10. Artificial Intelligence (AI)

We recognise that technology is rapidly evolving and are committed to remaining at the forefront of developments, adapting our ways of working as necessary.

AI is an integral part of the modern world and offers numerous opportunities for enhancing teaching, learning, and administrative processes, as well as potential risks, including to data protection principles.

We have an Artificial Intelligence Policy as we aim to foster a responsible and inclusive environment for the use of AI in education, upholding privacy, fairness, and transparency for the benefit of all involved.

Annexe.1 Legal Conditions for Processing

A1.1 Introduction

"Personal data" means any information where a living person is either identified or identifiable, from the information alone, or with other information. Personal data can include written information, pupil work, photographs, CCTV and film footage or voice recordings, in electronic format (which can include in Social Media, apps, databases or other electronic formats) or hard copy (including copies printed from electronic sources, and handwritten data when it is part of a filing system, or intended to be filed).

"Special category data" is personal data that needs more protection because it is sensitive, and there are tighter controls around this type of data:

• personal data revealing racial or ethnic origin;

• personal data revealing political opinions;

• personal data revealing religious or philosophical beliefs;

• personal data revealing trade union membership;

• genetic data;

• biometric data (where used for identification purposes);

• data concerning physical and mental health;

• data concerning a person's sex life; and

• data concerning a person's sexual orientation.

In addition, the DfE advises that Pupil Premium/FSM status is treated as Sensitive Data.

"Data Subjects" include our pupils, staff, contractors, parents, local authority contacts, and anyone else we might come into contact with.

"Data Controller" means the school, which alone or jointly with other Data Controllers, decides on why and how personal data is processed.

"Processing" means collecting, storing, using, sharing and disposing of data.

"Processors" are the external bodies who processes personal data on behalf of the controller.

A1.2 Our role and basis for processing

The role of any school is to educate and safeguard children. These are statutory obligations and come from various Acts and statutory instruments.

This means the overwhelming volume of our collection and processing data is based on the legal condition listed in Article 6 (1) c of the UK GDPR that "processing is necessary for compliance with a legal obligation to which the controller is subject". The relevant legal obligations depend on the specific data processing, but they include:

Equality Act 2010

Education (Governors' Annual Reports) (England)(Amendment) Regulations 2002.

Special Educational Needs and Disability Act 2001

Health & Safety of Pupils on Educational Visits 1998

Safeguarding Vulnerable Groups Act 2006

Disability Discrimination Act(s)

The Education Act 1944, 1996, 2002, 2011

The Education & Adoption Act 2016

The Education (Information About Individual Pupils) (England) Regulations 2013

The Education and Skills Act 2008

The School Attendance (Pupil Registration) (England) Regulations 2024

Statutory Guidance for Local Authorities in England to Identify Children Not Receiving Education – February 2007)

The Education and Inspections Act 2006

The Children Act 1989, 2004

The Childcare Act 2006

The Children & Families Act 2014

Local Safeguarding Children Boards Regulations 2006 (SI 2006/90)

The Localism Act 2011 Contract (traded services)

The Education (Pupil Information) (England) Regulations 2005

Keeping Children Safe in Education (Statutory Guidance)

Processing personal data as part of some of our functions related to safeguarding children that don't directly link to a statutory function above is based on Article 6 (1) e of the UK GDPR, that "processing is necessary for the performance of a task carried out in the public interest."

We have a separate Special Category Data Policy document which sets out in detail what lawful basis we rely on for processing Special Category Data.

When we wish to process data for any other reason, we must ask for consent as per Article 6 (1) a of the UK GDPR. Typically, this will be for areas of our work that includes the public celebration of our school and pupils' work. Data Subjects, or their parent/guardian, retain the right to change their consent preferences at any time by notifying the school office.

A1.3 Data Subjects' Rights

All of our data subjects have a number of rights – these are detailed in section of the policy 1.6 above.

To exercise these rights or for further help and information about processing and our commitment to keeping data safe, please contact our Data Lead Kieren Done or Data Protection Officer:

Data Lead/Data Protection Officer	Kieren Done COO/Data Lead or DPO Education Data Hub, Derbyshire County Council
Data Lead/DPO Email:	operations@ddat.org.uk or dpforschools@derbyshire.gov.uk
Data Lead/DPO Phone:	Kieren Done DDAT COO/Data Lead 0333 3554353 or Education Data Hub 01629 532888

Data Lead/DPO Address:	DDAT, Top Floor Endcliffe Mount, Deepdale Business Park, Ashford Road, Bakewell DE45 1GT or Education Data Hub, County Hall, Smedley Street, Matlock, Derbyshire, DE4 3AG

Annexe.2 Data Protection - Personal Data Breach Procedure (including Cyber Incidents)

A2.1 Introduction

A2.1.1 We recognise that a breach of personal data could happen, despite our policies, procedures and measures in place to protect personal data, and we must respond to any breach as quickly as possible in order to minimise any risks or potential harm to the school or to individuals.

A2.1.2 This procedure supports our Data Protection Policy. It includes our guidelines for reacting to and handling any actual or suspected breach of personal data, as soon as we become aware of the incident, in line with the UK GDPR, the DPA 2018 and best practice.

A2.2 Scope and Responsibilities

This policy applies to all instances when it is known or suspected that personal data that the school handles has been subject to a breach or incident (see below for breach definition.)

All staff are responsible for reading, understanding and complying with this policy.

Our Data Protection Officer provides assistance and further guidance on data breaches and incidents. The Head Teacher/Data Lead is responsible for taking the lead on the steps in this procedure once a breach, or suspected breach, has been reported internally, including reporting to the Data Protection Officer.

Any staff member becoming aware of a breach or incident is responsible for immediately reporting it internally, to ensure it can be handled appropriately.

A2.3 What is a Personal Data Breach?

A2.3.1 If personal data we handle is lost, destroyed, altered, disclosed, accessed or put beyond use when it shouldn't be, this is a Personal Data Breach.

A2.3.2 Where we *suspect* personal data has been subject to a breach, we should follow this procedure until we are sure that the personal data has or hasn't been breached.

A2.3.3. A personal data breach can occur accidentally or intentionally, and can be caused by staff, by an external threat (including cyber incidents), or anyone else.

A2.4 Breach / Incident Response Plan

All members of staff are responsible for taking all reasonable steps and cooperating with key staff in following this procedure when a breach is found or suspected (including Cyber incidents/attacks).

The breach response plan has 8 steps, which are covered in detail below:

1. Report the breach or incident internally;
2. Record the breach or incident (using the GDPRiS software where applicable)

3. Assess the risk;
4. Contain and recover;
5. Notify the ICO of the breach (if applicable);
6. Notify the affected Data Subjects of the breach (if applicable);
7. Review;
8. Implement any necessary changes to prevent reoccurrence.

Use the Data Breach Checklist (at the end of this procedure) and Data Breach Log for all personal data breaches.

A2.4.1 Report the breach internally (staff)

As soon as you become aware of a breach, or possible breach, report it to the Head Teacher/Data Lead or another senior staff member in their absence, who will lead on the breach response, including informing the Data Protection Officer of the breach and keeping them updated on the investigation and actions.

The report must be made as soon as possible even if the breach is discovered outside of normal working hours.

A2.4.2 Record the breach (school staff)

Log the breach or incident (using the GDPRiS software where applicable). Include as many details as possible and attach documents or evidence if appropriate.

If full details aren't available immediately, log what information *is* available, and add more detail as it becomes available.

A2.4.3 Assess the risk (DPO)

Consider what harm could come from the breach, including who could be harmed, how they could be harmed, and how severe the harm could be, as well as how likely it is the harm will happen. This risk assessment, based on severity and likelihood, will depend on the types of information involved (how sensitive is it, what could be done with it?), how much information is involved, and how exposed the data is, as well as the individual circumstances of the data subjects (that the data is about).

Examples:

> If a laptop has been lost, if it is encrypted there is a very small chance of any data being accessed. But if hard copy documents have been lost or left unattended, they are much more likely to be accessed and read.
>
> If personal data is included in an email by accident, the data may be at more risk of being misused if the email has gone to a member of the public, rather than to another school.
>
> Accidentally disclosing an address might not pose a risk to most data subjects, but it could be very high risk for someone who is escaping domestic violence, or for the adoptive family of a child.

A2.4.4 Contain and recover (with DPO support)

Take reasonable actions to contain the risks, and/or recover the data, if possible.

Containment and recovery actions could include, as appropriate:

- Attempting to find lost devices or paperwork;
- If devices have been stolen, report this to appropriate law enforcement agencies e.g. police.
- If a breach or incident is still occurring, for example, due to an ongoing IT issue, then IT must take appropriate steps to minimise the breach, such as closing down an IT system or server. In the event of a Cyber attack, immediately report to the Action Fraud line on 0300 1232040.
- Warning staff and third parties such as the County Council, to be aware of any "phishing" attempts that might be linked to personal data that has been accessed by criminals/unauthorised people;
- If data has been sent to, or shared with, someone it shouldn't have been, consider if you can contact them to recover the data. Bear in mind that "recall" doesn't usually work on externally sent emails;
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use;
- If the data breach or incident includes any entry codes or IT system passwords, change these immediately and inform the relevant agencies and members of staff;
- Contacting the Trust / Local Authority Communications Division if part of the crisis service, so that they can be prepared to handle any press enquiries.

A2.4.5 Notify the ICO of the breach (DPO);

Breaches or incidents that could result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office (the ICO – the UK's data protection regulator) and, in some cases, to the data subject(s) involved too.

Not all breaches will need to be reported. For example, if data is deleted in error it is technically a breach, but if the data is backed up and can be promptly reinstated, it does not represent a risk to data subjects.

If the DPO decides not to report a breach to the ICO and/or the data subjects involved, the decision and reasons must be recorded.

If it is likely the breach will result in a risk to people's rights and freedoms, it must be reported to the ICO.

Reports to the ICO must be made within 72 hours of us becoming aware of the breach. Information can be provided to the ICO in stages, giving them the details as and when we find out more, but the first contact must be within 72 hours.

The information to be provided to the ICO:

- A description of the personal data breach or incident that has occurred including, where possible:
    - the types and approximate number of people whose data is involved;
    - the types and approximate number of personal data records involved;
- The likely consequences of the breach or incident;
- The measures taken, or proposed to be taken, in response to the breach, including actions to mitigate any possible harm to data subjects;
- The name and contact detail of the Data Protection Officer, or any other contact details of people who can provide more information.

Guidance on how to report to the ICO is on their website: https://ico.org.uk/for-organisations/report-a-breach/

A2.4.6 Notify the affected Data Subjects of the breach (DPO);

If the risk to data subjects is assessed as high, the breach must also be reported to everyone whose data is involved, to allow them to take any appropriate steps to protect themselves and so they are aware of anything that may happen. For example, if financial information has been lost or stolen, they can alert their bank for fraudulent activity, or if passwords have been lost or stolen they can change them on their accounts and any other accounts that they used the same password on.

We can choose to report to data subjects even if the risk is not high, if it would be better for us to tell them about the breach for other reasons, such as supporting transparent relations and trust. In many circumstances it will be preferable for data subjects to hear about a breach or incident from us rather than from any other source.

A2.4.7 Review

Once the immediate controls have been put in place, review how the breach happened, going right down to the root causes of the breach. Consider all possible impacts on the situation that may have caused, or contributed to, the breach. Identify what changes will help prevent any similar breaches in future.

The review stage also includes reviewing and evaluating the response to the breach. Consider how effective the response was, and if improvements could be made when handling any future breaches.

As examples, did the person who first became aware of the breach know to report it internally? Did attempts to recover the data work? How could the breach have been handled better or quicker?

The breach, and outcomes of the review, should be reported to the next available Senior Management Team and Full LTC members/Trustees meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance.

A2.4.8 Implement any necessary changes to prevent reoccurrence.

Depending on what the review indicates about how the breach occurred, actions must be taken to reduce the risk of something similar happening, including amongst other things, improved IT security, new or improved written procedures, refresher training, improved supervision, changes to processes, communications to remind colleagues about risks, etc.

A2.5 Data Breach/Incident Checklist

Action	Give dates, initials and links to docs where appropriate
Date and time of discovery	
Date and time of occurrence	
What happened	

Immediate steps taken to contain the breach, e.g. changing passwords, shutting computers down, halting network traffic, restore data from backups	
Acknowledge breach by thanking informant for information – log it here	
Inform DPO 01629 532888	
Assess Risk:	[Consider how many people are affected, what type of data is involved, how could people be harmed, and how likely are they to be harmed?]
Necessary to inform ICO? 0303 1231113	
Date and time reported to ICO	
Necessary to inform data subjects?	
Data subjects informed?	
Law enforcement agencies e.g. police informed?	
Any other third parties informed?	[Consider banks, suppliers, anyone else who needs to know about the breach.]
Review:	[Consider what was in place that should have prevented the breach, and why it failed, how could further breaches be prevented, how have we helped the people effected? Should we improve security, procedures, training, etc?]
Steps taken to avoid reoccurrence	
Concluding letter	
SLT/LTC members/Trustees de brief	
Report completed by	

Annexe.3 Data Protection Impact Assessment Guidance

A3.1 Introduction

A Data Protection Impact Assessment (DPIA) is a tool to help us identify how to comply with our data protection obligations and protect individuals' rights.

An effective DPIA, carried out in the earliest planning stages of a project or change to policy, will allow us to identify and fix problems early on, reducing the associated costs, risks, and damage to reputation which might otherwise occur.

This guidance explains the principles which form the basis for a DPIA, sets out the basic steps to carry out during the assessment process and includes a template which can be adapted as needed to fit the project.

DPIAs will be drawn up with the assistance of the DPO, who will have the expertise needed to fully consider the issues, but the responsibility for ensuring a DPIA is undertaken lies with the staff member responsible for the project or policy.

A3.2 What is a Data Protection Impact Assessment (DPIA)?
A DPIA is a process which helps an organisation to identify and reduce the privacy risks of any project which involves personal data. To be effective a DPIA must be used throughout the development and implementation of the school's/trust's project.

A DPIA will enable the school to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved, as well as provide evidence of investigation into the suitability of any third parties who will be given access to data in the project.

A3.3 When will a DPIA be appropriate?
DPIAs should be considered for all new projects, at the earliest stages, to allow greater scope for influencing how the project will be implemented. A DPIA can also be useful when planning changes to an existing system.

The school must carry out a DPIA for processing that is likely to result in a "high risk to individuals" (Article 35(1) UK GDPR). When considering if the processing is likely to result in high risk, the school and the DPO should consider the relevant ICO Guidance:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

These list types of data processing that are likely to result in high risk. The most relevant to schools relate to processing of vulnerable data subjects (children), the processing of sensitive data or data of a highly personal nature, and monitoring of people's online or offline behaviour. Because so many activities in schools include the processing of children's data including sensitive data, it is likely that most projects in schools will require a DPIA to be carried out.

Prior to implementation, use of AI tools should be assessed to consider if a DPIA is required to determine whether their use is proportionate and fair by assessing the benefits against the risks to the rights and freedoms to individuals and/or whether it is possible to put safeguards in place.

Conducting a DPIA does not have to be complex or time consuming but there should be a level of rigour in proportion to the potential privacy risks.

A3.4 The Benefits of a DPIA
Consistent use of DPIAs should increase the awareness of privacy and data protection issues within the school and ensure that all relevant staff involved in designing projects think about privacy at its earliest stages.

Examples of where a DPIA would be appropriate

- Purchasing/implementing a new IT system for storing and accessing personal data.
- A proposal to identify people in a particular group or demographic and take action in relation to the group.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of the school.

- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Purchasing/implementing cloud hosted applications.
- The collection of new data on an existing system.
- Setting up a CCTV system.
- Authorising the use of a Generative AI platform.

A3.5 Steps to be followed when considering a new project

A DPIA should be undertaken before a project is underway, in the same way that schools/trust consider the cost impact of a project before making a commitment to spend any money. Consult with the DPO and consider consulting with affected data subjects as a first step. The DPIA process should then be a collaborative task between the Headteacher, Business Officer and staff who will be using the system/managing the project.

A3.6 Monitoring

Where a DPIA is required, the DPO will provide advice and support as needed. However, the responsibility for reviewing and completing the DPIA rests with the school's designated data lead. The completed DPIA should then be submitted to the DPO for approval. Any DPIAs considered high risk approved by the DPO will be shared with the Trust Board approval. The LTC should monitor implementation of actions identified in DPIAs.

Where risks highlighted in the DPIA meet the school's/trust's threshold, these must be added to the risk register.

Annexe.4 Subject Access Request (SAR) Procedure

A4.1 Introduction

A4.1.1 We process personal data in line with all of the legal rights of data subjects', including their right to:

- Be informed about their data being processed, which links to the first DP Principle of fair, lawful and transparent processing;
- Request access to their data that we hold;
- Ask for inaccurate data to be rectified;
- Ask for data to be erased (sometimes known as the "right to be forgotten");
- Restrict processing of their data, in limited circumstances;
- Object to the processing, in some circumstances, including stopping their data being used for direct marketing;
- Data portability, which means to receive copies of some of their data in a format that can be easily used by another organisation or person;
- Not be subject to automated decision making or profiling, if it has legal effects or similarly significant effects on the data subjects;
- Withdraw consent when we are relying on consent to process their data;
- Make a complaint to the ICO or seek to enforce their rights through the courts.

A4.1.2 This procedure supports our Data Protection Policy, and explains how we respond to requests from, or on behalf of, individuals for access to the data we hold that is about the individual. This is known as the right to access, and is a legal right under the UK GDPR and the DPA 2018. Requests are known as [Data] Subject Access Requests, or DSARs or SARs.

A4.1.3 For any queries about how to exercise any of the rights above, contact our Data Protection Officer.

A4.2 Scope and Responsibilities

The right to access applies to all pupils, parents, staff and anyone else that we hold personal data about. In some circumstances, for example with pupils, a parent or other person with authority may make the Subject Access Request on their behalf.

All leaders are responsible for ensuring their team read and understand this procedure as they may receive a SAR on behalf of the school.

Our Data Protection Officer (DPO) provides assistance and further guidance on responding to SARs.

Any individual who purposefully alters, defaces, blocks, erases, destroys or conceals information to prevent it being provided to a data subject who has requested it, and has a right to receive it, may be committing an offence.

A4.3 Receiving a valid SAR

Format: A SAR does not need to be in writing, it can be in any format, including a letter, email, text message, over social media, over the telephone, or face to face, and can be made to any member of staff at the school.

However, in order to process the request as efficiently as possible, and to help us comply with statutory timeframes, we ask that the form contained in Annexe 1 below is completed.

Content: A SAR does not need to refer to data protection legislation or be described as a subject access request to be a valid SAR. Any request for access to personal information from, or on behalf of, a data subject, must be treated as a SAR.

Identity & Authority: We must verify the identity of the person making the SAR, and if the SAR is being made on behalf of someone else, we must confirm they have authority to act on their behalf in exercising their rights. Checking identity must not be used as a delaying tactic, and how to verify identity will depend on who is making the SAR, and how well they are known to the person handling the request. For example, a staff member will not usually be required to confirm their identity, but a request from a former staff member, or on behalf of someone else, would need to be verified using proof of identity, signature and address.

A parent / person with parental responsibility does not automatically have the right to make a SAR on behalf of their child.

A child may exercise these rights on their own behalf if we believe they are competent to do so. Assessing competence is based on the age, maturity and level of understanding of the child. Each situation should be decided in collaboration with the professionals working with the child, but 12 years is regarded as a starting point. A child will not be considered competent if it is evident that he or she is acting against their own best interests or under pressure from a parent or other person with authority.

Where a SAR is received from a parent of a competent child, consent to process the request and release all/part of the information must be sought from the child.

No charge: In most cases, a SAR will be responded to free of charge. In limited circumstances, where a request is manifestly unfounded or excessive an appropriate charge can be made. Requests made under EPIR 2005 may be charged for. A proposed charge will be agreed with the DPO.

Refusing to fulfil a SAR: In limited circumstances, the request or elements of it may be refused under the exemptions in the DPA 2018, for example:

- if the requestor cannot confirm their identity or authority to make the request on behalf of another person, the request must be refused until confirmation is provided;
- where a request is manifestly unfounded or manifestly excessive;
- information relating to education data, social work data or health data if might cause serious harm to the physical or mental health of the data subject or another individual (this applies even when a competent child has consented to their parent receiving their data);

Elements of data held that may be withheld or redacted, include:

- information that would reveal that a child is at risk of abuse, where disclosure of that information would not be in the child's best interests (this applies even when a competent child has consented to their parent receiving their data);
- information contained in adoption and parental order records;
- certain information given to a court in proceedings concerning a child.

A4.4 Responding to a SAR

Timescales: SARs must be responded to as soon as possible, and within one month at the latest. In the case of complex or multiple requests an extension of up to an extra two months can be applied, but the requestor must be informed of the extension within the first month. The calculation of time must commence once the SAR is determined as valid. An acknowledgement should be sent to the requestor as soon as possible to inform them that the SAR has been received, the start date, and that it is being processed.

For SARs, school holidays, bank holidays and weekends are all included within the month. For example, a valid SAR received on 20th July must be fulfilled by 20th August despite the school closure.

Format: The DPO should decide with the requestor, the most appropriate and preferred method of providing information.

Content: The 'right to access' allows the requestor to receive information held about them, as a Data Subject. The requestor will not necessarily receive every version of information, if it is held in different ways or duplicated. Access is to the data, not the particular documents.

Third party data: Where the person's data is combined with another person's data, which does or could identify that other person (third party), that data may be redacted, or withheld if redaction would not fully prevent the other person being identified. Data can be disclosed that identifies the third party if that person has given their consent to disclose it, or it is judged to be reasonable to disclose the information without that person's consent. Deciding if it is reasonable should take into account things such as the type of information, any duty of confidentiality owed, the role of the other person, whether the person is capable of giving consent, and whether they have expressly refused consent.

A4.5 Exemptions

Exemptions under the DPA 2018 allow us to withhold data from a SAR in some further circumstances, including amongst others: where legal professional privilege applies, where management forecasts or negotiations could be prejudiced by disclosing the data, confidential references, and where exam results are requested but they are not yet due to be published.

The application of exemptions will be approved by the DPO, but **if in doubt do not disclose information**, as it can always be disclosed at a later date.

Response: When sending the relevant data to the requestor, the information must be clear, so any codes or jargon used will be explained in the SAR response. In responding to requests we also explain to data subjects they have the right to make a complaint to the ICO or seek to enforce their rights through the courts.

Data subjects also have a right to receive, in response to their SAR, the following information, which is contained within our Privacy Notice (a link to which will accompany the release):

- the purposes of our processing;
- the categories of personal data concerned;
- the recipients or categories of recipient we disclose the personal data to;
- retention periods for storing the personal data or, where this is not possible, our criteria for determining how long it will be stored for;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of any automated decision-making (including profiling); and
- the safeguards we provide if we transfer their personal data to a third country or international organisation.

Monitoring: The receipt of SARs must be logged and coordinated centrally, using GDPRiS where appropriate, to ensure timescales are being met and SARs are being handled appropriately.

A4.6 SAR Request Form
Section 1

About yourself or person you are making this request on behalf of (Please use block capitals and black ink) – this information will help us to identify the personal data that we may hold about you.

Title (Mr /Mrs /Miss /Ms /Dr /Rev etc)	

Surname/Family Name	
First Name(s)	
Maiden/Former Name(s) (if applicable)	

Date of Birth (dd/mm/yyyy)	

Home Address (Include Postcode)	

This is the address to which all replies will be sent, unless you specify otherwise.

Name of person making request on behalf of data subject (if applicable)	
Surname/Family Name	
First Name(s)	
Relationship to data subject	
Preferred alternative address for correspondence (if applicable)	

Contact telephone number	
Contact e mail address	

Section 2- About your request

What records that you believe we hold would you like access to:

Have you made a request for this information before? (Yes/No)	
If yes, could you please provide date of request? (dd/mm/yyyy)	

Where do you want to view your information? For example, in person, or be sent a paper copy to your home or alternative address or be sent a copy in a specific electronic format to an email address (if this is your preferred option we would encrypt the file to keep it secure)

Do you need any other help with this request? (Please specify below)

Section 3 - Proof of identity

Establishing Proof of Identity

If we have a verified current address for you on our systems we must contact you at that address and ask you to confirm that the request has come from yourself.

If this is not possible, we must ask for documentary evidence to verify you are who you say you are.

To help establish your identity we may ask you to provide at least two different documents which, between them, provide sufficient information to prove your name, date of birth, current address and signature. For example, a combination of driving licence, medical card, birth/adoption certificate, passport and any other official documents e.g. utility bills, which show those details.

If you are making this request on behalf of someone else you must provide evidence you have the right to do so, e.g. letter of consent, birth certificate evidencing you have parental responsibility for a child or any other relevant legal documentation, unless you have supplied this information to us already for other purposes.

On receipt of completed form we must contact you to arrange verification of these documents.

Please note that it may be necessary to seek further information or proof of identity (of data subject or requestor) before the request can be processed. If this is the case, then the statutory one month day limit must start from the date all necessary information and proof is received. Every effort should be made to provide you with your information as soon as possible after receipt of your application, however in some cases we may need longer than a month to respond to your request if any complex issues are involved.

Section 4 – Declaration

(To be signed by the Requestor)

The information, which I have supplied in this application, is correct, and I am the person to whom it relates/I have the right to make this request on their behalf (delete as appropriate).

Signature

Date

Warning – A person who impersonates another or attempts to impersonate another may be guilty of an offence. It is similarly an offence to coerce consent from a Data Subject or interested third party.

Should any advice or guidance be required in completing this application, please contact our Data Protection Officer.

General advice on the UK GDPR and Data Protection Act 2018 can be obtained from The Information Commissioners' Office, contact details are below.

The information on this form must only be used to support you in exercising your rights under the Data Protection Act 2018 and must be destroyed, in line with our retention policy, after a decision on your request has been made. For further information on how the school may use your personal information visit: https://ddat.org.uk/gdpr/

Please return this form once completed to:

FAO DDAT Data Lead Kieren Done

Mark your envelope "Subject Access Request - Confidential".

Data Lead	Kieren Done
Data Lead Email:	operations@ddat.org.uk
Data Lead Phone:	0333 3554353
Data Lead Address:	DDAT, Top Floor, Endcliffe Mount, Deepdale Business Park, Ashford Road, Bakewell DE45 1GT

If however, you are dissatisfied with our response, you can of course contact the ICO quoting our ICO registration number ZA102461 and stating that the Data Controller is Derby Diocesan Academy Trust (DDAT).

Information Commissioners' Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number

Fax: 01625 524 510. Website: https://ico.org.uk/concerns/

Annexe.5 Requests under the Freedom of Information Act 2000 / Environmental Information Regulations 2004

Requests for Environmental Information, for example, information about land development, pollution levels, energy production, and waste management must be dealt with under the Environmental Information Regulations 2004, all other requests must be dealt with under the Freedom of Information Act 2000

A5.1 Introduction: what a publication scheme is and why it has been developed

One of the aims of the Freedom of Information Act 2000 (FOIA) is that public authorities, should be clear and proactive about the information they will make public. Therefore, all schools/trusts are required to produce a Publication Scheme that specifies the classes of information which the school publishes or intends to publish.

The scheme must set out the school's/trust's commitment to make certain classes of information routinely available, such as policies and procedures, minutes of meetings, annual reports and financial information.

Derby Diocesan Academy Trust (DDAT) must make the publication scheme available on the website under 'freedom of information', 'guide to information' or 'publication scheme'. If required, information should also be available in hard copy. If the school are asked for any of the information listed on the publication scheme, it must be made available quickly and easily.

In order to comply with the above, Derby Diocesan Academy Trust must produce a publication scheme, setting out:

- The classes of information which we publish or intend to publish;
- The manner in which the information will be published; and
- Whether the information is available free of charge or on payment.

The scheme (in 5.4 below) covers information already published and information which is to be published in the future.

Some information which we hold may not be made public, for example personal information.

This publication scheme conforms to the model scheme for schools approved by the Information Commissioner, which sets out Derby Diocesan Academy Trust's (DDAT) high-level commitment to proactively publish information.

A5.2 Values

Derby Diocesan Academy Trust (DDAT) Mission Statement and Vision

For every child and young person to embrace "life in all its fullness" (John 10:10).

Our Vision for Derby Diocesan Academy Trust is to nurture and empower everyone to reach their fullest potential, supporting each other on this journey. Inspired by the teachings of Jesus Christ, we cultivate a vibrant learning community where children and young people flourish academically, emotionally, and spiritually. Our mission and vision flow from the Church of England's vision for education, which emphasises the development of wisdom, knowledge, and skills; hope and aspiration; community and living well together; and dignity and respect. Together, as a community rooted in Christian faith and education, we embrace the abundant possibilities of "Life in all its fullness".

Derby Diocesan Academy Trust (DDAT) Values

Inclusivity:
Jesus showed that no one was excluded from the love of God. In John's gospel he said: "I give you a new commandment, that you love one another. Just as I have loved you, you also should love one another." (John 13:34-35) We offer life-giving love to every child and family, reflecting our belief in social justice and the importance of community. We focus on relationships and participation, fostering qualities that enable people to flourish together. Our actions embody our commitment to recognising the value and uniqueness of individuals, celebrating difference.

Integrity:
Truth is not simply about knowledge and facts. Jesus said that when we follow his teachings, "you will know the truth, and the truth will set you free." John 8:32 We are honest and trustworthy which we see as essential for personal growth and trust in our community. We behave ethically to support decision making and to ensure a sustainable future for all, remaining grounded in the Christian understanding of truth and righteousness.

Community:
Jesus encouraged his followers to work together, with all our differences. "Two are better than one, because they have good reward for their toil. For if they fall, one will lift up the other; but woe to one who is alone and falls and does not have another to help." Ecclesiastes 4:9-10 We build community, working together for the common good. Collaboration and mutual support are key to achieving our shared goals and enhancing our collective well-being. Our teamwork emphasises the qualities of character necessary for living well together.

Excellence:
"Whatever your task, put yourselves into it, as done for the Lord and not for your masters." Colossians 3:23 Whatever our strengths and weaknesses, we reach for the highest standards in all our endeavours. Jesus teaches his followers to be who God intends them to be and gives us hope that we can carry on when it is hard. We encourage all children and adults to pursue their best. Inspired by the Christian pursuit of excellence in all things, we delight in seeking wisdom and knowledge, developing confidence and talents in all areas of life. We champion the faithful commitment to do little things well.

Courage:

“Be strong and courageous. Do not be afraid; do not be discouraged, for the Lord your God will be with you wherever you go.” Joshua 1:19 Jesus travelled to Jerusalem, knowing that he would lay down his life for his friends. We are courageous and tenacious, grounded in the example of Jesus’ life to have faith and hope in the face of adversity. This determination includes enabling healing, repair, and renewal, and coping wisely when things go wrong.

In addition to our obligations under the FOIA and EIR, we seek to be as transparent as possible with our community and stakeholders. Annex 5 outlines how we should respond to requests.

A5.3 Categories of information published
This publication scheme guides you to information which we currently publish or which we should publish in the future. This is split into categories of information known as ‘classes’. These are contained in section 5.4 below.

A5.4 Classes of Information Currently Published

A5.4.1 Information to be published on the Derby Diocesan Academy Trust (DDAT) website

See separate FOI publication scheme: https://ddat.org.uk/gdpr/

A5.4.2 Governing Body Documents

Information published in governing body documents includes:

- The name of the school
- The category of the school
- The name of the governing body
- The manner in which the governing body is constituted
- The term of office of each category of LTC member/trustee if less than 4 years
- The name of anybody entitled to appoint any category of LTC member/trustee
- Details of any trust
- If the school has a religious character, a description of the ethos
- The date the instrument takes effect
- A ‘public’ version of governing body and its committees minutes that have been approved by the governing body [current and last full academic school year].

A5.4.3 Derby Diocesan Academy Trust (DDAT) Policies & Information [including pupils & curriculum]

Policies that can be found on the school website.

- 16-19 Bursary Policy & Procedures - School
- Attendance Policy - Trust
- Acceptable Use of IT, the Internet and Electronic Communication - Trust
- CCTV Policy - School
- Charging and Remissions Policy - Trust
- Child Protection and Safeguarding Policy - Trust
- Code of Conduct [Local Trust Committee members/Trustees [school to delete as appropriate] - Trust
- Complaints Procedure for External Complaints against Staff - Trust
- Confidential Reporting Code (Whistleblowing) - Trust

- Curriculum Information - School
- Data Protection Policy - Trust
- Disability Equality Duty - School
- Exam Policy - School
- Exam Access Arrangements Policy - School
- Homework Policy - School
- Lettings Policy - School
- Marking Policy - School
- Mission Statement - School
- Privacy Notices - School
- Publication Scheme - School
- SEN and Disability Policy - Trust
- SEN Local Offer Information - School

A5.4.4 Other information related to the school

- Published reports of Ofsted referring expressly to the school
- Published report of the last inspection of the school and the summary of the report and where appropriate inspection reports of religious education in those schools/trusts designated as having a religious character
- Post-Ofsted inspection action plan - A plan setting out the actions required following the last Ofsted inspection and where appropriate an action plan following inspection of religious education where the school is designated as having a religious character
- School session times and term dates
- School Calendar
- Details of school events and Inset days throughout the academic year

A5.5 How to request information
Where information is not published on our website, you may make a request by contacting the school in writing.

To help us process your request quickly, please clearly mark any correspondence "**FREEDOM OF INFORMATION REQUEST or ENVIRONMENTAL INFORMATION REQUEST".**

We must respond to requests no later than 20 working days from receipt of the request.

Except where:

- We reasonable require further information to meet a request, have informed the requestor of this requirement, but have not been supplied with that further information.
- The information is no longer readily available as it is contained in files that have been placed in archive storage or is difficult to access for similar reasons.
- An exemption applies under part 2 of the Freedom of Information Act 2000 or part 3 of the Environmental Information Regulations 2004.
- The cost of providing the information exceeds the appropriate limit under Freedom of Information Act 2000, part 1, section 12.
- The request is vexatious or manifestly unreasonable.
- The request is a repeated request from the same person made within 60 consecutive working days of the initial one.
- A fee notice was not honoured.

Where information has been exempted from disclosure, we must, within 20 working days, give notice to the requestor which:

- States the fact, and
- Specifies the exemption in question.

A5.5.1 Format

The information provided must be in the format requested, where possible. Where it is not possible to provide the information in the requested format, we must assist the requestor by discussing alternative formats in which it can be provided.

The information provided must also be in the language in which it is held, or another language that is legally required. Translations and alternative formats required under relevant disability and discrimination regulations must be provided where necessary.

A5.5.2 The appropriate limit

The school will not comply with any freedom of information request that exceeds the statutorily imposed appropriate limit of £450.

In determining whether the cost of complying with a freedom of information request is within the appropriate limit, we must take account only of the costs we reasonably expect to incur in relation to:

- Determining whether we hold the information.
- Locating the information, or a document which may contain the information.
- Retrieving the information, or a document which may contain the information.
- Extracting the information from a document containing it.
- Costs related to the time are to be estimated at a rate of £25 per person per hour.

Where multiple requests for information are made to the school within 60 consecutive working days of each other, either by a single person or by different persons who appear to be acting in concert, the estimated cost of complying with any of the requests is to be taken to be the total costs to the school of complying with all of them.

A5.6 Advice & Assistance

The school has a duty to provide advice and assistance and must do so in the following circumstances.

- If an individual requests to know what types of information the school holds and the format in which it is available, as well as information on the fees regulations and charging procedures.
- If a request has been made, but the school is unable to regard it as a valid request due to insufficient information, leading to an inability to identify and locate the information.
- If a request has been refused, e.g. due to an excessive cost, and it is necessary for the school to assist the individual who has submitted the request.

The school must provide assistance for each individual on a case-by-case basis.

In order to provide assistance as outlined above, the school should engage in the following good practice procedures:

- Make early contact and keep the requestor informed of the process of their request.
- Accurately record and document all correspondence concerning the clarification and handling of any request.
- Give consideration to the most appropriate means of contacting the requestor, taking into account their individual circumstances.
- Remain prepared to assist a requestor who has had their request denied due to an exemption.

The school must give particular consideration to what level of assistance is required for a requestor who has difficulty submitting a written request.

In circumstances where a requestor has difficulty submitting a written request, the school must:

- Make a note of the application over the telephone and then send the note to the requestor to confirm and return – the statutory time limit for a reply would begin here.
- Direct the individual to a different agency that may be able to assist with framing their request.

This list is not exhaustive and the school may decide to take additional assistance measures that are appropriate to the case.

Where a requestor's request has been refused either because the information is accessible by other means, or the information is intended for future publication or research, the school, as a matter of good practice, should provide advice and assistance.

The school should advise the requestor how and where information can be obtained, if it is accessible by other means.

Where there is an intention to publish the information in the future, the school should advise the requestor of when this publication is expected.

If the request is not clear, the school should ask for more detail from the requestor in order to identify and locate the relevant information, before providing further advice and assistance.

If the school is able to clearly identify the elements of a request, it must respond following usual procedures and must provide advice and assistance for the remainder of the request.

If any additional clarification is needed for the remainder of a request, the school must ensure there is no delay in asking for further information.

If a requestor decides not to follow the school's/trust's advice and assistance and fails to provide clarification, the school is under no obligation to contact the requestor again.

If the school is under any doubt that the requestor did not receive the advice and assistance, the school must re-issue it.

The school is not required to provide assistance where a requestor's request is vexatious or repeated, as defined under section 14 of the Freedom of Information Act 2000 or manifestly unreasonable under regulation 12(4)(b) of the Environmental Information Regulations 2004.

The school is also not required to provide information where the cost of complying with a request exceeds the limit outlined in the Freedom of Information Act 2000. In such cases, the school should consider whether any information can be provided free of charge if the requestor refuses to pay the fee.

A record must be kept by the school of all the advice and assistance provided.

A5.7 Paying for information

Information published on our website is free, although you may incur costs from your Internet service provider. If you don't have Internet access, you can access our website using a local library or an Internet café.

Single copies of information covered by this publication are provided free unless stated otherwise in section 6. If however your request means that we have to do a lot of photocopying or printing, the following charges will apply:

- 5p per single side of A4,
- 10p per single side of A3.
- plus any postal charge at the current rate applied by Royal Mail.

For a priced item such as some printed publications or videos we must let you know the cost before fulfilling your request. Where there is a charge this must be indicated on application on an individual basis.

A5.8 Feedback and Complaints

Data Lead/Protection Officer	Kieren Done DDAT COO/Data Lead or DPO Education Data Hub, Derbyshire County Council
Data Lead/DPO Email:	Operations@ddat.org.uk or dpforschools@derbyshire.gov.uk
Data Lead/DPO Phone:	0333 3554353 (DDAT) or 01629 532888
Data Lead/ DPO Address:	DDAT Top Floor Endcliffe Mount, Deepdale Business Park, Ashford Road, Bakewell DE45 1GT Or County Hall, Smedley Street, Matlock, Derbyshire, DE4 3AG

If however, you are dissatisfied with our response to your concerns you can of course contact the ICO quoting our ICO registration number ZA102461.

Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number

Fax: 01625 524 510

Website: https://ico.org.uk/concerns/

Annexe.6 Data Protection Complaints Policy

A6.1 Purpose
This policy outlines how our school handles complaints related to data protection, in accordance with the Data (Use and Access) Act 2025, the UK GDPR, and the Data Protection Act 2018. It ensures that individuals can raise concerns about the handling of their personal data and receive a timely, fair, and transparent response.

A6.2 Scope
This policy applies to:

- Pupils and their parents/carers
- Staff and volunteers
- LTC members and trustees
- Third-party service users and partners

A6.3 How to Make a Complaint
Individuals may submit a data protection complaint via:

- Online form (available on the school website)
- Email to the school's/trust's Data Lead and/or DPO
- Written letter addressed to the Headteacher or DPO
- Telephone or in-person at the school office

All complaints must include:

- The nature of the concern
- The data subject affected
- Any relevant dates or supporting evidence

A6.4 Acknowledgement and Response Timeline
- Complaints must be acknowledged within 30 calendar days of receipt.
- The school must take appropriate steps without undue delay to investigate the complaint.
- Complainants must be kept informed of progress.
- A formal outcome must be provided once the investigation concludes.

A6.5 Investigation Process
- The DPO should lead the investigation, supported by relevant staff.
- The investigation may include reviewing records, speaking to staff, and consulting external advisors.
- If the complaint is upheld, corrective actions must be taken promptly.

A6.6 Contestability and Redress

- Individuals have the right to challenge decisions made by automated systems or AI tools.
- Staff are empowered to override AI-generated suggestions where appropriate.
- If a complaint results in adverse consequences or unfair treatment, the school must offer appropriate redress, which may include:
    - Correction or deletion of data
    - Apology and explanation
    - Review of procedures or training

A6.7 Record Keeping

- All complaints and outcomes must be logged securely.
- Records must be retained in accordance with the school's/trust's Data Retention Schedule.
- Complaint volumes may be reported to the Information Commissioners Office (ICO) as required.

A6.8 Escalation

If a complainant is dissatisfied with the outcome, they may escalate the matter to the ICO once the school's/trust's internal process is complete.

A6.9 Staff Training

All staff must receive training on:

- Recognising and escalating data protection complaints
- Understanding their responsibilities under this policy
- Using the complaints platform and reporting procedures