

JUNE 2026

# STCAT DATA PROTECTION POLICY

---

Approved By: TRUST BOARD  
Policy Owner: DATA PROTECTION OFFICER  
Next Review Date Due By: JUNE 2028



**St Thomas**  
Catholic Academies Trust

## Contents

1. Aims .....	3
2. Legislation and guidance .....	3
3. Definitions .....	3
4. The data controller .....	5
5. Roles and responsibilities.....	5
6. Data protection principles .....	6
7. Collecting personal data .....	6
8. Sharing personal data .....	7
9. Subject access requests and other rights of individuals.....	8
10. Parental requests to see the educational record .....	10
11. Biometric recognition systems.....	11
12. CCTV .....	11
13. Photographs and videos .....	11
14. Artificial Intelligence (AI) .....	12
15. Digital Verification and Information Gateway .....	12
16. Data protection by design and default.....	13
17 Children’s Personal Data .....	13
18. Automated Decision Making .....	14
19. Data security and storage of records .....	14
20. International Data Transfers .....	15
21. Disposal of records .....	15
22. Personal data breaches.....	15
23. Training.....	16
24. Complaints.....	16
25. Monitoring arrangements .....	16
26. Links with other policies and procedures.....	16
24. Equalities Monitoring .....	17
Appendix 1: Personal Data Breach Procedure .....	18
Appendix 2: Reporting Data breaches and Handling a Request for Data Procedure for Staff.....	21
Appendix 3: Complaint Form - Data Protection.....	22

## 1. Aims

St Thomas Catholic Academies Trust (the "Trust") aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## 2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- Data Use and Access Act 2025 (DUA 2025).

It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#), DUA, [guidance on right of access](#) and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

## 3. Definitions

Term	Definition
<b>Automated Decision Making</b>	Refers to decisions made solely by automated means without human involvement, which may have legal or similarly significant effects on individuals.
<b>Personal data</b>	Any information relating to an identified, or identifiable, individual. This may include the individual's: <ul style="list-style-type: none"> <li>• Name (including initials)</li> <li>• Identification number</li> <li>• Location data</li> <li>• Online identifier, such as a username</li> </ul>

	It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> </ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Data processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
<b>Personal data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

## 4. The data controller

The Trust and the schools within the Trust process personal data relating to parents, pupils, staff, directors, governors, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and has paid its data protection fee to the ICO as legally required. ICO registration number is ZA138068

## 5. Roles and responsibilities

This policy applies to **all staff**, employed by the Trust, to Board Directors and Governors and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

### 5.1 The Board of Directors

The Board of Directors, with the support of each Local Academy Committee, has overall responsibility for ensuring that each school within the Trust complies with all relevant data protection obligations.

### 5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of their activities directly to the board and, where relevant, report to the board their advice and recommendations on Trust/school data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust/school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

The DPO for the Trust is Maxine Gilmartin and is contactable via email or phone (dpo@stcat.co.uk; 01582 361601).

### 5.3 Headteacher

The headteacher of each school acts as the representative of the data controller on a day-to-day basis. The headteacher will ensure that all staff are aware of their data protection obligations.

### 5.4 School Data Protection Lead

The School Data Protection Lead (DPL) is responsible for the day to day data protection processes within school (ie responding to SARs etc).

### 5.5 All staff

All staff are required to comply with this policy and with the Trust's Data Protection Procedures when handling personal data.

## 6. Data protection principles

The UK GDPR is based on data protection principles that require full compliance. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

The Trust is committed to processing personal data lawfully, fairly, and transparently in accordance with UK data protection legislation.

Personal data will only be processed where a valid lawful basis applies under UK GDPR. These may include processing necessary for the performance of a contract, compliance with a legal obligation, the protection of vital interests, the performance of tasks carried out in the public interest or in the exercise of official authority, the pursuit of legitimate interests, or where valid consent has been obtained. Where special category personal data is processed, the Trust will ensure that an appropriate additional condition for processing is satisfied.

The Trust recognises its responsibilities as a public authority and will normally rely on lawful bases other than consent where appropriate. Where consent is relied upon, including in relation to pupils, the Trust will ensure that consent is valid, informed, and capable of being withdrawn.

The Trust is committed to transparency and will provide individuals with clear and appropriate information about how their personal data is used at the point of collection, in line with legal requirements.

### 7.2 Transparency and Reuse of Personal Data

The Trust is committed to transparency in the use of personal data and will ensure that individuals are provided with clear information about the purposes for which their data is processed, in accordance with data protection legislation.

In limited circumstances, the Trust may further process personal data for a compatible purpose without providing additional notification, where permitted by law and where doing so would involve disproportionate effort. Any such further processing will be lawful, proportionate, and subject to appropriate safeguards to protect individuals' rights and freedoms.

Where reliance is placed on an exemption from re-notification, the Trust will ensure that the decision is properly documented and that appropriate information about the

processing is made publicly available where required. Detailed arrangements for assessing compatibility, disproportionate effort, and safeguards are set out in Trust procedures.

### 7.3 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's retention schedule.

### 7.4 Recognised Legitimate Interests

The Trust recognises that, in certain circumstances, it may rely on Legitimate Interests as a lawful basis for processing personal data in accordance with Article 6(1)(f) UK GDPR. Legitimate interests may include the Trust's own operational interests, the interests of individual academies within the Trust, and the broader interests of staff, pupils, parents, visitors, and the community. These recognised interests may cover, for example:

- Ensuring the safety, security, and welfare of pupils, staff, and visitors.
- Preventing and detecting crime or safeguarding concerns.
- Managing Trust sites and resources effectively.
- Investigating incidents, complaints, or misconduct.
- Maintaining network and information security.
- Pursuing the Trust's educational, organisational, and administrative functions.

Where the Trust relies on legitimate interests, it will ensure that the processing is necessary, proportionate, and balanced against the rights and freedoms of the individuals concerned.

## 8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – where required, we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.

## 9. Subject access requests and other rights of individuals

### 9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguarding provided if the data is being transferred internationally

Subject access requests should include:

- Name of individual
- Correspondence address

- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must **immediately** forward it to the School Data Protection Lead.

## 9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

### Primary schools

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

### Secondary schools

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our schools may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

## 9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 calendar month of receipt of the request. The clock starts on the day the request is received, including weekend or public holiday, and ends on the corresponding date in the next month. If that date doesn't exist (eg request on 31 March, deadline is 30 April) or falls on a weekend/bank holiday, the deadline moves to the next working day.
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary
- If we need extra information to verify identity or clarify the request, the timeline starts once we have received that information.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Conflicts with safeguarding obligations

- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- Contains third party information
- Is legally privileged

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

Searches for information will be reasonable and proportionate. This means we do not have to search systems unlikely to contain relevant data, provide data the requestor already has access to or provide email exchanges with the requestor that they already hold.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

#### 9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (ie making decisions or evaluating certain things about an individual based on their personal data with no human involvement, that might negatively affect them)
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

## 10. Parental requests to see the educational record

Parents, or those with parental responsibility, may request access to their child's educational record (which includes most information about a pupil) this will usually be provided within 30 days of receipt of a written request to the Trust's DPO.

## 11. Biometric recognition systems

Note that in the context of the Protection of Freedoms Act 2012, a “child” means a person under the age of 18.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can be given a PIN or card instead of biometrics.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults (including students over the age of 18) use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

## 12. CCTV

The Trust uses CCTV in various locations around the Trust sites to ensure it remains safe. We will adhere to the ICO's guidance for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Trust IT Department.

## 13. Photographs and videos

### 13.1 School activities

As part of the school activities, we may take photographs and record images of individuals within our Trust/school.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

### **13.2 Recordings of meetings**

In all circumstances, meetings, whether online or in person, will only be recorded where there is a legal basis to do so in line with UK GDPR. Where a legal basis is identified, consideration should be given to a less intrusive method of recording the meeting first, ie audio recording or an additional note taker. Where a meeting is recorded, all parties must be in agreement to the recording and the method used.

## **14. Artificial Intelligence (AI)**

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the Trust will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

## **15. Digital Verification and Information Gateway**

Where applicable, the Trust will comply with provisions relating to:

- Digital verification services (Part 2, DUA Act)
- Information disclosure via approved gateways (e.g., HMRC or public authorities)

These provisions are unlikely to routinely affect our operations, but the Trust will monitor forthcoming secondary legislation.

## 16. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge. .
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the Trust/school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our Trust/schools and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

## 17 Children's Personal Data

The Trust recognises that children merit enhanced protection in relation to the processing of their personal data, as they may be less aware of the risks, consequences, and safeguards involved. All processing of children's personal data across the Trust and its academies will be lawful, fair, transparent, and carried out in the best interests of the child.

The Trust is committed to:

- Taking a child-centred approach when designing, implementing, or reviewing processing activities involving children's data.
- Applying heightened technical and organisational security measures where personal data relates to children.
- Ensuring access to children's personal data is restricted to authorised staff with a legitimate need to know.

- Embedding data minimisation, ensuring only personal data that is necessary for the specified purpose is collected and retained.
- Ensuring that age-appropriate privacy notices are provided to pupils, tailored to their age, understanding, and educational stage.
- Verifying and recording parental or guardian consent where consent is the applicable lawful basis, in accordance with data protection legislation and Trust procedures.

Further operational detail is set out in the Trust's Data Protection Procedures.

## 18. Automated Decision Making

The Trust does not make decisions about individuals based solely on automated processing, including profiling, where such decisions would produce legal effects or similarly significant effects on them. Any decisions that affect pupils, parents, staff or other individuals are always subject to appropriate human involvement. Where automated processes are used to support decision-making (for example, within management information systems), they are used in a lawful, fair and transparent manner, and individuals have the right to request human intervention, to express their view, and to challenge any decision made.

## 19. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Highly sensitive information should only be taken off site in exceptional circumstances, with permission from the Headteacher. If necessary, DPO advice should be sought.
- Staff and students should use complex passwords to access school computers, laptops and other electronic devices. The IT team can provide further advice.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupil's, directors or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust and school-owned equipment (if you are unsure please see the Trust DPO).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

## 20. International Data Transfers

The Trust is committed to ensuring that personal data is not transferred outside the United Kingdom unless appropriate safeguards are in place to protect the rights of individuals, in accordance with data protection legislation.

Personal data may be transferred internationally where this is necessary to support the Trust's operational or statutory functions, for example where cloud-based systems or third-party service providers are located outside the UK.

Where personal data is transferred outside the UK, the Trust will ensure that one or more of the following safeguards applies:

- The transfer is to a country or territory that has been recognised as providing an adequate level of protection for personal data
- Appropriate safeguards are in place, such as the use of UK-approved Standard Contractual Clauses or other recognised contractual protections
- The transfer is permitted under a specific exemption provided by data protection legislation

The Trust will take all reasonable steps to ensure that international transfers are lawful, fair and transparent, and that personal data remains adequately protected regardless of where it is processed.

Individuals will be informed where relevant about international transfers through the Trust's Privacy Notices and may request further information by contacting the Trust's Data Protection Officer (DPO).

## 21. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust/school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

## 22. Personal data breaches

The Trust and all schools will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in **Appendix 2**.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium

- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

## 23. Training

All staff, directors and governors are required to complete mandatory data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

## 24. Complaints

Under section 103 of the Data (Use and Access) Act 2025, individuals have a statutory right to lodge a complaint directly with the data controller if they believe their data protection rights have been infringed.

Complaints can be submitted by completing the form at Appendix 3 and sending this to the DPO by email or post ([dpo@stcat.co.uk](mailto:dpo@stcat.co.uk) / Data Protection Officer, St Thomas Catholic Academies Trust, c/o St Martin de Porres Catholic Primary School, Pastures Way, Luton, LU4 0PF).

Complaints will be acknowledged within 30 calendar days of receipt and an investigation of your complaint will be completed and a full response provided without undue delay. If the investigation requires more time, we will keep you informed of progress and provide an expected resolution date.

Following the investigation, we will explain the findings and any actions taken and provide information on rights to escalate the complaint to the Information Commissioner's Office if you are not satisfied with our response.

If you are dissatisfied with our response, you may contact the ICO: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; website: <https://ico.org.uk>; Helpline: 0303 123 1113.

## 25. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary **every 2 years** and approved by the Trust Board.

## 26. Links with other policies and procedures

This data protection policy is linked to our:

- STCAT Code of Conduct for employees
- STCAT Cyber and Information Security Policy
- STCAT Data Protection Procedures

- STCAT Freedom of Information Policy and Publication Scheme
- STCAT ICT Usage Policy (SchoolsHR Policy)
- STCAT Protection of Biometric Data Policy
- STCAT Retention Schedule
- STCAT Safeguarding Children Policy and Child Protection Procedure

## 27. Equalities Monitoring

<p>To what extent does this policy have any implications for people of relevant protected characteristics (RPC) as outlined below?</p> <ul style="list-style-type: none"> <li>• Age</li> <li>• Disability</li> <li>• Gender reassignment</li> <li>• Marriage and civil partnership</li> <li>• Pregnancy and maternity</li> <li>• Race</li> <li>• Religion or belief</li> <li>• Sex</li> <li>• Sexual orientation</li> </ul> <p>(Equality Act, 2010)</p>	<p><b>Assessment:</b> None. Special category data that relates to some of the relevant protected characteristics, is specially dealt with under UK GDPR and the DPA 2018 to ensure it is processed appropriately.</p>
<p>Will this policy advantage or disadvantage any particular group?</p>	<p>No</p>
<p>How will this policy, if relevant, promote equality of opportunity across our Trust?</p>	<p>This policy is intended to support everyone, irrespective of any protected characteristics, in processing of individual personal data and access requirements to it.</p>
<p>Success criteria and monitoring</p>	<p><b>Success criteria:</b> There are no complaints to the Trust relating to issues around personal data.</p> <p><b>Monitoring:</b> Directors will receive an annual update in relation to data protection.</p>

## Appendix 1: Personal Data Breach Procedure

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will alert the headteacher
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored centrally.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored centrally.
- If necessary, the DPO and headteacher of the school will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

### **Actions to minimise the impact of data breaches**

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

#### **Sensitive information being disclosed via email (including safeguarding records)**

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent

in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with directors/governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen

# Appendix 2: Reporting Data breaches and Handling a Request for Data Procedure for Staff

## DATA PROTECTION

All Staff

Tasks for the DPO

Guidance on this procedure

Found or caused a data breach? Been asked to provide data on an individual?  
**Immediately notify our Data Protection Officer (DPO)**

**Our DPO is: Maxine Gilmartin**  
 Telephone: 01582 361601 Email: dpo@stcat.co.uk

### What is a data breach?

It's a breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

#### A breach may involve:

- non-anonymised data being published on the school website showing test results of children eligible for the pupil premium
- safeguarding information about a child being made available to unauthorised people
- the theft of a school laptop containing non-encrypted personal data about pupils

### Why must you escalate a data breach?

1. If someone's personal data falls into the wrong hands it can result in serious harm to that person.
2. We are legally required to investigate data breaches.
3. Learning what went wrong will help us to adapt procedures and prevent future breaches

### What is a Freedom of Information Request?

The Freedom of Information Act 2000 provides public access to information held by public authorities.

#### It does this in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.

The Act **does not** give people access to their own personal data. If a member of the public wants to see information that a public authority holds about them, they should make a **subject access request**.

FoI's should be made in writing, and once received should be immediately passed on to the DPO.

### What is a Subject Access Request?

The right of access (Subject Access Request) gives individuals the right to obtain a copy of their personal data as well as other supplementary information.

SAR's should be made in writing but can be made verbally, and once received should be immediately passed on to the DPO.

## ! REMEMBER !

IF YOU ARE UNSURE IF A BREACH HAS BEEN COMMITTED, OR IF AN INFORMATION REQUEST HAS BEEN MADE, ALWAYS CONTACT YOUR DPO.

Reporting data breaches

Reporting a data request

The DPO will...

Alert the Headteacher and if need be the Chair of Governors

Acknowledge the request, and check the identity of the individual if making a SAR.

Contain and minimise the impact of the breach  
Taking all reasonable efforts, and assisted by relevant staff where necessary

Begin to identify who will assist with the collation of information.

All staff contacted by the DPO are expected to assist the DPO in a timely manner, this may be retrieving relevant information and/or assisting with the redaction process. The DPO has 1 calendar month to collate, and present all information for a subject Access Request.

The DPO has 20 working days to collate and respond with all information requested under the Freedom of information act 2000

Assess the potential consequences  
How serious are they? How likely are they to happen?

Respond to the request

A written response will be sent to the requestor, along with redacted hard copies if a SAR.

Risk to someone's rights and freedoms: is it likely?  
Could the breach put someone at risk of discrimination, identify theft damage or disadvantage?

YES

NO

Report the breach to the ICO within 72 hours

Risk to someone's rights and freedoms: is it high?  
How serious are the risks? How likely are they to happen?

NO

Inform the affected individual(s) promptly

In writing the following will be set out:  
 The DPO's name and contact details  
 The likely consequence of the breach

The measures you have taken, or will take, to deal with the breach and mitigate any possible adverse effects on individuals

**Notify any third parties who can mitigate the impact of the breach**

For example, the police, insurers, banks or credit card companies

Review and record the breach - **Records of all data breaches are stored centrally**

Discuss with the Headteacher:  
 What happened, how we can stop it from happening again, whether a process or system regularly has minor incidents  
**Record:**  
 Facts and cause, effects, all decisions taken – including whether or not to report to the ICO/individuals affected, action taken to contain the breach and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

**APPENDIX 3: COMPLAINT FORM – DATA PROTECTION**

<b>YOUR DETAILS</b>	
Full name:	
Address:	
Email Address:	
Phone Number (optional):	
Relationship to the School/Trust:	Parent / Employee / Service User ( <i>delete as applicable</i> ) Other:
School:	
<b>DETAILS OF THE COMPLAINT</b>	
Please describe your concern in as much detail as possible (include what happened, when it happened and who was involved, if known)	
What personal data does your complaint relate to? <i>(e.g. name, address, health information, education records)</i>	
How do you believe your data protection rights have been breached?	
<b>SUPPORTING EVIDENCE: Please attach any relevant documents or correspondence that support your complaint (eg emails, screenshots, letters)</b>	

**DESIRED OUTCOME: What outcome are you seeking from this complaint?**  
*(e.g. an apology, correction of data, assurance of future compliance)*

**DECLARATION: I confirm that the information I have provided is accurate to the best of my knowledge. I understand that the school/Trust may need to contact me to discuss this complaint further.**

Signature:

Date:

Please send this form to the Trust DPO, Maxine Gilmartin, [dpo@stcat.co.uk](mailto:dpo@stcat.co.uk) (or via post to St Thomas Catholic Academies Trust, c/o St Martin de Porres Catholic Primary School, Pastures Way, Luton, LU4 0PF)