

# St Christopher's Trust

## Data Protection Policy 2025



Policy Updated: September 2025  
Policy Approved: 29<sup>th</sup> September 2025  
Date of Next Review: September 2027

## Contents

Introduction.....	3
What is the General Data Protection Regulation (UK GDPR)? .....	3
Who does it apply to? .....	3
What are the key principles of UK GDPR? .....	3
Progress Check (Nurseries).....	4
Who is a data 'subject'? .....	4
Data subjects' rights.....	4
Subject Access Requests (SAR) .....	5
Who is a 'data controller'?.....	6
Who is a 'data processor'?.....	6
Processing data.....	6
Data sharing.....	7
Breaches & non-compliance .....	7
Consent.....	7
Consent & renewal .....	7
For pupils & parents/carers .....	8
Pupil consent procedure .....	8
Withdrawal of consent.....	8
CCTV Policy .....	8
Data Protection Officer .....	8
Physical security.....	9
Secure disposal.....	9
Complaints & the Information Commissioner Office (ICO) .....	9
Review .....	9
Appendix One – Breach and Non-Compliance Procedure .....	10
Appendix Two – Data Usage Act 2025: Complaint Process .....	12
Appendix Three – Data Usage Act 2025: Complaint Form.....	14

## **Introduction**

St Christopher's CofE (Primary) Multi Academy Trust and our schools are committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data, and we take that very seriously. This policy, and the Privacy Notices, set out how we look after and use data. Each school will be responsible for the day-to-day management of data that is held about pupils, staff, parents, carers, and other individuals in connection with that school. The Trust central team are responsible for data held centrally about individuals.

Where we use the phrase 'we' that refers to the Trust and the individual schools.

## **What is the General Data Protection Regulation (UK GDPR)?**

This is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. It was brought into line with changes to the UK leaving the EU on 31 December 2020. The UK GDPR and DPA 2018 exist to look after individuals' data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure. The UK GDPR exists to protect individual rights in an increasingly digital world.

## **Who does it apply to?**

Everyone, including schools. As 'Public Bodies' schools and trusts have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and provisions in the Data Protection Act 2018. We want to make sure information about pupils, parents, staff, and volunteers is kept secure and within the law.

## **What are the key principles of UK GDPR?**

- 1) Lawfulness, transparency, and fairness – Schools must have a legitimate reason to hold the data, we explain this in the Privacy Notices. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent, we have a form to complete to allow us to process your request. There are times when you cannot withdraw consent as explained in 'Data Subjects' Rights.'
- 2) Collect data for a specific purpose and use it for that purpose – Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.
- 3) Limited collection – Data Controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.
- 4) Accuracy – Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when pupils join the school and is reviewed on an annual basis. If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms. Initially an approach should be made directly to the individual school.
- 5) Retention – A retention policy is in place that governs how long records are held for.
- 6) Security – We have processes in place to keep data safe. That might be paper files, electronic records, or other information.

Please see the following linked policies and notices:

- Retention Policy
- Acceptable Use for Staff
- Acceptable Use for Pupils and individual school ICT agreement (where applicable)
- Social Media Policy
- Privacy Notice for Staff
- Privacy Notice for Pupils
- Privacy Notice for Governors
- Privacy Notice for Visitors

### **Progress Check (Nurseries)**

When a child is aged between 2 and 3, their progress will be reviewed, and the parents and/or carers will be provided with a written summary of the child's development in the 3 prime areas. This 'progress check' highlights the areas in which a child is progressing well and the areas in which additional support is needed.

### **Who is a data 'subject'?**

An individual whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

### **Data subjects' rights**

Whilst Privacy Notices set out details about why data may be collected, stored, and used, there are some overriding principles that apply to every person (the Data Subject) when a school stores data.

Data subjects' rights are also subject to child protection and safeguarding concerns and sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases, these obligations override individual rights.

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

As Data Subjects, sometimes our consent is necessary for a school to process data about us. That might relate to photographs in school, reports in local press or similar. Consent is dealt with in the separate parts of the policy and can be accessed on the website or through the school office. There are other occasions when data about us or our children may be used by the school to fulfil a legal obligation, a contract, or some other lawful usage.

We all have other rights.

- 1) The right to rectification. Where data held about us is inaccurate, we have a right to apply for it to be amended and put right. This has to be done within one month, or within three

months if it was complex. To do this we have to contact the data compliance manager within school, or the data protection officer. We have a right to complain if this is not done.

- 2) The right of access. This is a subject access request and is dealt with in more detail as part of the data protection policy. In essence, we have a right to see information about us that is classed as "personal data." There is a separate process for us to make this request within school, and the school may ask us to clarify or be more specific about what kind of data we are asking for if there is a lot of it. Again, there is a one month timeframe for this that can be extended for three months in complex cases.
- 3) We have a right to erasure. This means that in certain circumstances we can ask for data about us to be permanently deleted. However, this can be limited if the data needs to be kept for some official or lawful purpose. The right to erasure sometimes occurs if we withdraw consent to a process.
- 4) We sometimes have the right to restrict processing. If we believe that data is inaccurate, and we have asked for it to be erased, we can ask the data processor and controller to stop any processing until the investigation into erasure or amendment has taken place.
- 5) There is also the right to data portability, this has little bearing in the school setting. Transfer of data for pupils is regulated by guidance from the Department for Education. Data about staff is part of HMRC contractual obligations. Data portability would usually apply to things like utility companies or bank accounts.
- 6) Individuals also have the right to object to personal data being used for marketing. Again, in the school setting this is likely to be very limited as the only marketing tends to be limited to school fetes, fairs, and plays. Schools and academy trusts should not be sharing data with commercial third party entities to enable direct marketing of individuals. If this was the case, then an individual could object and ensure that the data was no longer used for that purpose.
- 7) As individuals we also have the right to ask that decisions are made about us on the basis of our data, rather than by an automated process. Again, any application of this in schools would be extremely limited. This tends to be regarding situations such as reference agency checks for loans and mortgages for example. These rights are important and sit alongside the school or trust's legal obligations to manage our data properly.

Please also see the Privacy Notices. If you feel that any of the Rights set out here are not being managed properly, or if that information held of our files is inaccurate or should not be there or should be changed or amended, please do let us know.

### **Subject Access Requests (SAR)**

You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). This SAR process is set out separately on our schools and Trust website. once you have made a request you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if the request is complicated, or the data cannot be accessed.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases, we cannot share all information we hold on file if there are contractual, legal, or regulatory reasons. We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information by paper or electronic form.

If you wish to complain about the process, please see our Complaints Policy and later information in this DPA policy.

### **Who is a 'data controller'?**

The school and or Trust is the data controller. They have ultimate responsibility for how the school and Trust central team manage data. They delegate this processing to individuals to act on their behalf, that is the Trust central team and the relevant staff in each school setting. The data controller can also have contracts and agreements in place with outside agencies who are data processors.

### **Who is a 'data processor'?**

This is a person or organisation that uses, collects, accesses, or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the Local Authority. Data controllers must make sure that data processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that data controllers require contractual agreements to ensure that this is the case.

### **Processing data**

The Trust and the schools must have a reason to process the data about an individual. Our Privacy Notices set out how we use data. The UK GDPR has six conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach, we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:

- consent obtained from the data subject or their parent/carer
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law

In addition, any special categories of personal data are processed on the grounds of:

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations

- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data

Processing data is recorded within the school systems.

### **Data sharing**

Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education (DfE), health, the police, local authorities, and other specialist organisations may be used to determine whether data is shared. The basis for sharing or not sharing data is recorded in school.

### **Breaches & non-compliance**

If there is non-compliance with the policy or processes, or there is a DPA breach as described within the UK GDPR and DPA 2018 then the guidance set out in the Breach & Non-compliance Procedure and Process needs to be followed. See Appendix One. Protecting data and maintaining Data Subjects' Rights is the purpose of this policy and associated procedures.

### **Consent**

As a Trust, where required, we will seek consent from staff, volunteers, parents, and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory, and regulatory occasions when consent is not required.

We may process personal and sensitive data without consent if another provision applies.

Consent is defined by the UK GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

We may seek consent from young people also, and this will be dependent on the child and the reason for processing. This will largely be managed in the individual schools.

### **Consent & renewal**

On the Trust/school websites we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

<https://www.stchristophersmat.org/privacy-notice/>

Obtaining clear consent, where required, and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

## **For pupils & parents/carers**

On joining the school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in-school purposes, as set out on the data collection and consent form.

The contact and consent form are reviewed on an annual basis. It is important to inform school if details or your decision about consent changes. This can be done by contacting the school office. This is the obligation of each individual to notify the school of changes.

### **Pupil consent procedure**

Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child as required.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared, and used in certain situations.

### **Withdrawal of consent**

Consent can be withdrawn, subject to contractual, statutory, or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of UK GDPR and also child welfare, protection, and safeguarding principles.

Please speak to the school office or your line manager where appropriate.

### **CCTV Policy**

Each school has its own tailored CCTV Policy.

### **Data Protection Officer**

We have a Data Protection Officer (DPO) whose role is to:

- inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR
- monitor compliance with the UK GDPR and DPA
- provide advice where requested about the data protection impact assessment and monitor its performance
- be the point of contact for Data Subjects if there are concerns about data protection
- cooperate with the supervisory authority and manage the breach procedure
- advise about training and CPD for the UK GDPR

Our DPO is Jo Wilkey whose contact details are below.

Address: St Christopher's CofE (Primary) Multi Academy trust, St Sidwell's Primary School, York Road, Exeter EX4 6PG

Email: [office@stcmat.org](mailto:office@stcmat.org)



## **Physical security**

As a Trust we are obliged to have appropriate security measures in place.

In each school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The senior leadership team is responsible for authorising access to secure areas. All staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches. All sites and locations need to have the suitable security and review measures in place.

## **Secure disposal**

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure UK GDPR and DPA compliance.

## **Complaints & the Information Commissioner Office (ICO)**

The Trust Policy for Data Complaints can be found in appendix 2 and 3.

There is a right to complain if you feel that data has been shared without consent or lawful authority. The trust complaints policy sets out the complaints process. This will be the basis for dealing with Data Protection Complaints and appeals. A written outcome will be provided.

You can complain if you have asked to us to erase, rectify, or not process data and we have not agreed to your request.

If the school or Trust does not comply with a Subject Access Request within 1 month (subject to any extension), or refuses all or part of the request, written reasons will be provided setting out the principles for refusal.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

In the UK it is the Information Commissioner (ICO) who has responsibility for safeguarding and enforcing the DPA obligations. If you feel that the trust has not dealt with your matter satisfactorily you can complain to the ICO:

Email: [casework@ico.org.uk](mailto:casework@ico.org.uk) Helpline: 0303 123 1113 web: [www.ico.org.uk](http://www.ico.org.uk)

## **Review**

A review of the effectiveness of UK GDPR compliance and processes will be conducted by the DPO every 12-24 months.

## **Appendix One – Breach and Non-Compliance Procedure**

### **Breach management guidance**

All staff, governors and trustees must be aware of what to do in the event of a DPA/UK GDPR breach. The guide 'How to Manage a Data Breach' outlines the process. Most breaches, aside from cyber-criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable. Everyone needs to understand that if a breach occurs it must be swiftly reported so that risks to the data subjects are minimized and well managed.

### **What is a breach?**

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. Examples of breaches are:

- information being posted to an incorrect address which results in an unintended recipient reading the information
- loss of mobile or portable device, unencrypted mobile phone, USB memory stick or similar
- sending an email containing personal data to the wrong person
- dropping or leaving documents containing personal data in a public place
- personal data being left unattended at a printer enabling unauthorised persons to read that information
- not securing documents containing personal data (at home or work) when left unattended
- anything that enables an unauthorised individual access to school buildings or computer systems
- discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- deliberately accessing or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial, or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack which results in unauthorised access to, loss, destruction, or damage to personal data

### **What staff and governors should do?**

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter. Report the breach to the data controller and DPO as soon as possible, this is essential.

### **How is the breach managed?**

The incident will be logged on the GDPRis portal. Advice will be sought from the Data Protection Officer as required. A plan to effectively manage the breach, who to inform and how to proceed will be put in place. If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO. Actions and changes to procedures, additional training or other measures may be required to be implemented and

reviewed. The breach report will be within 72 hours of becoming aware of the breach to the Information Commissioner if it is serious. It may not be possible to investigate the breach fully within the 72-hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO. The DPO is to advise the Chair of the Board/Risk & Audit if there are any ICO reportable breaches.

### What happens to the people whose data has been breached?

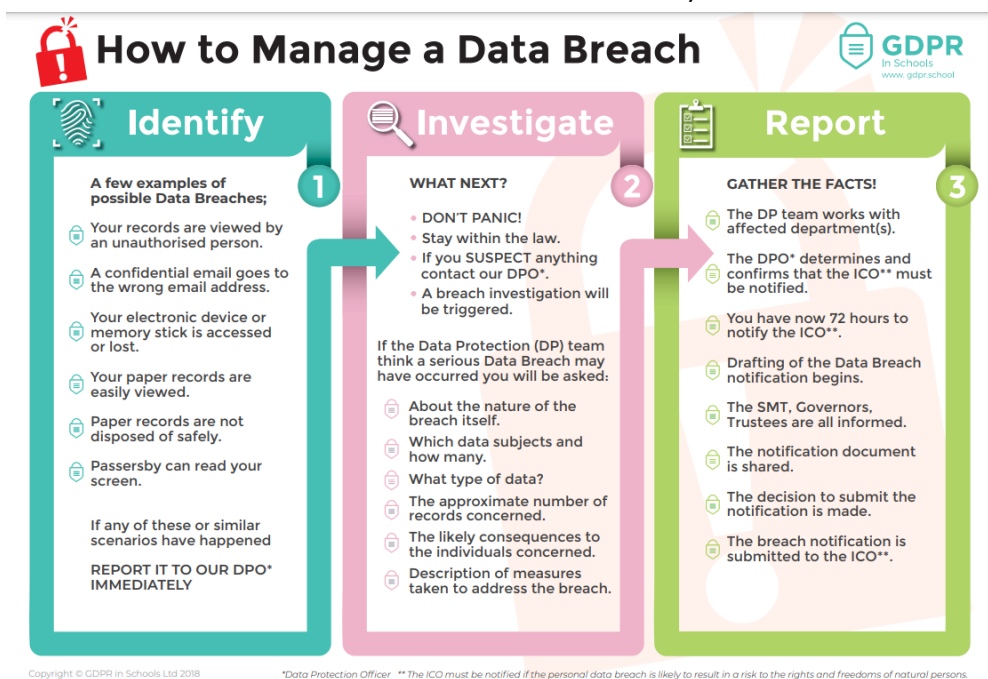
For every breach, the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes. The breach and process will be described in clear and plain language. If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used. Advice may be taken from the ICO about how to manage communication with data subjects if appropriate.

### Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings. This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer but will be determined depending on the nature of the breach. Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence. A record of what evidence has been gathered, stored, and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

### What happens next?

The impact of a serious breach will need to be assessed. It may be necessary to change some processes and procedures. Additional training may be required. IT protocols may need to be reviewed. The school will work with the Data Protection Officer to ensure that any changes are made to protect and secure information and to learn from any breaches.



## **Appendix Two – Data Usage Act 2025: Complaint Process**

### **Introduction**

St Christopher's is committed to protecting the privacy and personal data of its students, staff, parents/carers, governors and the wider school community. This policy outlines the procedure for handling complaints related to data usage and access, in accordance with the Data Usage Access Act (DUAA) and other relevant UK data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The UK GDPR documents as set out on our website provide an overview of how personal data is managed across our schools.

This is an appendix to the main complaint policy and reflects the requirement for standalone data usage complaints to be handled using a separate procedure. Any complaint that is linked to other matters whether raised as a formal or informal complaint are to be dealt with under the standard complaint process as outlined within the main complaint policy.

### **Roles and responsibilities**

The Data Controller (DC) is responsible for ensuring compliance with this policy and the legal obligations imposed by the UK GDPR, Data Protection Act 2018, Data Usage and Access Act 2025 and other relevant legislation. The DC will delegate day to day management of this to the relevant staff member and the DC will expect that staff member to investigate any complaint unless there is a conflict of interest, in which case the DC will appoint a suitable person.

The headteacher and leadership team are responsible for ensuring all staff are aware of this policy and their data protection obligations.

All staff members are responsible for handling personal data in a secure and lawful manner and for co-operating fully with any investigation into a data usage or access complaint.

### **Scope**

This policy applies to all individuals who have dealings with St Christopher's and believe that their personal data has been used or accessed inappropriately, or that their rights under the DUAA and other data protection laws have been infringed.

This includes but is not limited to:

- current and former students
- parents/carers
- school staff (teaching, support, and administrative)
- governors
- volunteers
- contractors and suppliers

### **Principles**

**Fairness and transparency:** All complaints will be handled in a fair, impartial, and transparent manner.

**Confidentiality:** Complaints and all related information will be treated with the utmost confidentiality, unless disclosure is required by law.

**Timeliness:** Complaints will be acknowledged and investigated in a prompt manner.

**Compliance:** All actions taken will comply with the DUAA, UK GDPR, DPA 2018, and other relevant legislation.

## **The complaint procedure**

### **Step 1: Informal resolution**

We encourage individuals to first attempt an informal resolution of their concerns. If you have a concern about data usage or access, you should, in the first instance, raise it with the relevant member of staff or senior person at the school.

In many cases, issues can be resolved quickly and informally at this stage.

### **Step 2: Formal complaint submission**

If the informal approach is not successful or deemed inappropriate, a formal complaint should be submitted in writing using the complaint form attached.

The complaint should be addressed to the Trust DPO on [office@stcmat.org](mailto:office@stcmat.org)

The written complaint should be made on the form that can be accessed in Appendix 3 or shall include the following information:

1. your full name and contact details.
2. a clear and concise description of the complaint, including what happened, when it happened, and who was involved.
3. a description of the data involved and how you believe it was used or accessed inappropriately.
4. any relevant dates, times, or evidence.
5. details of any informal steps you have already taken to resolve the issue.
6. the desired outcome of the complaint.

### **Step 3: Acknowledgment and investigation**

You will receive an acknowledgment of the written complaint within 5 school days of the setting receiving it.

The DC will conduct a thorough and impartial investigation into the complaint.

This may involve:

- interviewing the complainant
- interviewing relevant staff members
- reviewing school records, logs, and policies
- consulting with external legal or data protection experts if necessary

The Trust will aim to complete the investigation and provide a substantive response within 20 school days of the complaint's acknowledgment. If the investigation is complex and requires more time, the DC will write to the complainant to explain the reason for the delay and provide a new estimated completion date.

## Response

The DC will provide a formal written response to the complainant.

This response will include:

- the findings of the investigation.
- a clear and reasoned conclusion as to whether the DUAA or other data protection laws have been breached.
- details of any corrective action taken or planned to prevent a recurrence of the issue.
- the outcome of the complaint, including whether it has been upheld, partially upheld, or not upheld.
- information on the next steps available to the complainant if they remain dissatisfied.

## Escalation

If the complainant is not satisfied with the Trust's final response, they have the right to escalate their complaint to the Information Commissioner's Office (ICO).

The ICO's contact details are as follows:

- Website: <https://ico.org.uk>
- Telephone: 0303 123 1113
- Postal Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

## Appendix Three – Data Usage Act 2025: Complaint Form

*To be completed by the complainant – Please return this form to St Christopher's CofE (Primary) Multi Academy Trust: [office@stcmat.org](mailto:office@stcmat.org)*

### Part 1: Complainant's Details

Please provide your full contact information so we can communicate with you regarding your complaint.

<b>Full Name:</b>	
<b>Relationship to the Trust/school:</b> (e.g. student, parent/carers, staff member, former student, volunteer, contractor)	
<b>If student:</b>	
year group:	
form/class:	
<b>If parent/carers:</b>	
student's full name:	
student's year group:	
<b>Contact telephone number:</b>	
<b>Email address:</b>	
<b>Postal address:</b>	
<b>Preferred method of contact:</b> (e.g. email, phone or post)	

## Part 2: Details of the complaint

Please provide a clear and concise description of your complaint.

<b>Date(s) of the incident(s)</b>	
When did the misuse occur or when did you become aware of it?	
<b>Nature of the complaint</b> Please tick all that apply and provide details below:	
Unauthorised access to personal data	
Unauthorised disclosure of personal data	
Incorrect or inaccurate personal data	
Unlawful processing or use of personal data	
Failure to respond to a data subject request e.g. Subject Access Request or Right to Erasure	
Other (please specify)	
<b>Description of the incident(s)</b>	
What happened? Provide a detailed narrative of the events.	
Who do you believe was involved? e.g. specific staff member, department, external party	
What personal data was involved? e.g. name, address, medical information, academic records, disciplinary records, financial details, sensitive personal data	
How do you believe your data was misused or accessed inappropriately?	
Where did the incident occur (if applicable)	
Has there been any previous attempts to resolve this issue informally? e.g. discussed with a teacher, GDPR lead, Headteacher	<b>Yes or No</b>
If yes, please provide details of who you spoke to and when.	

## Part 3: Supporting evidence

Please list and attach any evidence that supports your complaint. This could include:

- emails or correspondence
- screenshots
- dates and times of relevant events
- witness statements (if applicable)

*Please list attached documents here:*

**Part 4: Desired outcome**

Please specify the resolution that you are seeking as a result of this complaint?

<input type="checkbox"/>	Investigation and explanation of what happened
<input type="checkbox"/>	Correction of inaccurate data
<input type="checkbox"/>	Deletion of unlawfully processed data
<input type="checkbox"/>	An apology
<input type="checkbox"/>	Assurance that similar incidents will not occur in the future
<input type="checkbox"/>	Other (please specify):

**Part 5: Declaration**

I understand that St Christopher's Trust will investigate this complaint in accordance with its Data Usage Access Act 2025 Complaint Process.

**Signature:**

**Date:**