St Gabriel
the Archangel
Catholic Multi-Academy Trust

DATA PROTECTION POLICY

POLICY TO BE REVIEWED ANNUALLY OR EARLIER DUE TO ANY LEGISLATIVE CHANGES

FOR ALL ACADEMIES PART OF ST GABRIEL THE ARCHANGEL CATHOLIC MULTI-ACADEMY TRUST

Approved by Audit and Risk Committee: 23rd April 2026

Next Review: April 2027

1. Aims

St Gabriel the Archangel Catholic Multi Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, carers, directors, 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)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

The Data (Use and Access) Act 2025

It is based on guidance published by the ICO and the January 2026 DfE Generative AI Product Safety Standards

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data which is used for the cashless catering system in some of our Academies.

It also reflects the ICO's guidance 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
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data

	• Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	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

Each academy in St Gabriel the Archangel Catholic Multi Academy Trust processes personal data relating to parents, carers, pupils, staff, directors, governors, visitors and others, and therefore is a data controller.

St Gabriel the Archangel Catholic Multi Academy Trust is registered with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by St Gabriel the Archangel Catholic Multi Academy Trust, and to external organisations or individuals working on our behalf, including Directors and Governors. Staff who do not comply with this policy may face disciplinary action. Directors and Governors may be asked to resign or be removed from office should they not comply with this policy.

5.1 Board of Directors

The Board of Directors have overall responsibility for ensuring that St Gabriel the Archangel Catholic Multi Academy 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 our 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 of Directors and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

The DPO is Mrs Bhaksho Raj who can be contacted by:

- Telephone: 01782 307510/01902 553550
- E-Mail: DPO@sgacmat.co.uk or
- Letter: Data Protection Officer
  St Gabriel the Archangel Catholic Multi Academy Trust
  c/o Painsley Catholic College
  Station Road
  Cheadle
  Staffordshire
  ST10 1LH

5.3 Principal

The Principal at each academy acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on data protection principles that St Gabriel the Archangel Catholic Multi Academy Trust and each academy must comply with.

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 St Gabriel the Archangel Catholic Multi Academy Trust aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract

- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e., to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) or a third party provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual

- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

St Gabriel the Archangel Catholic Multi Academy Trust - Primary Schools:

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

St Gabriel the Archangel Catholic Multi Academy Trust - Secondary Schools:

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).
Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

St Gabriel the Archangel Catholic Multi Academy Trust - Children of separated or divorced parents:

Where either parent is listed on the school's information management system as having parental responsibility for a child, they are entitled to submit a subject access request relating to their child's personal data. The school will respond to such requests in accordance with UK GDPR requirements, provided the parent can verify their identity and parental responsibility status.

There is no requirement for the school to notify the other parent when a subject access request is made by one parent with parental responsibility, unless there are specific safeguarding concerns or court orders in place that would make such notification necessary. When deciding who to respond to, the school will weigh up factors including: the maturity of the pupil, the nature of the personal data requested, any court orders relating to parental access or responsibility, any confidentiality owed to the pupil, and the likely consequences if the data is given to the parent – particularly if there have been any allegations against the parent of abuse or ill treatment.

Please see the St Gabriel Separated Parents policy for full details.

7.2 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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 St Gabriel the Archangel Catholic Multi Academy Trust Records Management policy.

7.3 Telephone Calls

Please note that all calls made to and from the St Gabriel the Archangel Catholic Multi Academy Trust and the individual academy telephone systems may be recorded for training and monitoring purposes.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 – 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 contract with the supplier or contractor 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

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

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 internationally, we will do so in accordance with UK data protection law.
We will obtain a Data Sharing Agreement from any third-party service provider before any data is shared.

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 right to lodge a complaint with the ICO or another supervisory authority
- 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 safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

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.

St Gabriel the Archangel Catholic Multi Academy Trust - 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 primary 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.

St Gabriel the Archangel Catholic Multi Academy Trust - Secondary Schools:

The ICO recommends that 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 secondary 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 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will conduct a "reasonable and proportionate" search for the personal data requested.
- A charge may be made depending on the volume/complexity of the information to be provided.
- May refuse to act or charge a reasonable fee if a requester repeatedly asks for further copies of information in different formats after already successfully receiving it.
- 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.
- May "stop the clock" on the one month response deadline if we reasonably require clarification from the requester to provide an effective response. The clock resumes once clarification is received.

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we cannot reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- Is vicarious.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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

There is no automatic parental right of access to the educational record. Parents/carers who wish to access this information should submit a request in writing directly to the school. Please note a charge may apply.

- In addition to the right of access under UK GDPR (the SAR), parents of pupils at Maintained Schools have a separate statutory right to their child's educational record.
- As an Academy, while this specific statutory right does not apply automatically, the Trust aims to align with best practice by responding to requests for educational records within 15 school days.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, using finger prints to receive goods and services from the Catering provider 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. We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using an allocated Personal Identification Number (PIN) at each transaction if they wish.

Parents/carers and pupils can 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 use the school's biometric system, we will also obtain their consent before they 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 in writing, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around St Gabriel the Archangel Catholic Multi Academy Trust school sites to ensure they remain 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.

All schools which have CCTV Systems will have a CCTV policy in place.

Any enquiries about the CCTV system should be directed to the Principal.

13. Photographs and videos

As part of school activities, we may take photographs and record images of individuals within our schools. Photographs will only be taken using school issued devices – parents, carers, visitors, staff, directors and governors are not permitted to use personal devices for the taking of photographs. Exceptions may be made during school events at the discretion of the Principal. Consent must be obtained before any photographs are taken.

St Gabriel the Archangel Catholic Multi Academy Trust - Primary Schools:

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

St Gabriel the Archangel Catholic Multi Academy Trust - Secondary 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 do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

All Schools:

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where any school takes photographs and videos, uses may include:

- Within school on noticeboards and in school magazines, brochures, newsletters, and School Information Management Systems.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on the St Gabriel the Archangel Catholic Multi Academy Trust and individual academy websites or social media pages
- Cashless till systems for the identification of pupils and staff. Note this is also to ensure catering staff can clearly identify pupils with allergens or special dietary requirements.

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.

The consent form for the use of photographs and videos can be found at Annex A.

See the individual academy safeguarding policy for more information on the use of photographs and videos.

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. St Gabriel the Archangel Catholic Multi Academy 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, St Gabriel the Archangel Catholic Multi Academy Trust will treat this as a data breach, and will follow the personal data breach procedure outlined in Annex B.

- The Trust recognises that AI poses unique risks to data privacy and safeguarding.
- DPIA Requirement: A Data Protection Impact Assessment (DPIA) must be conducted for any generative AI product before it is introduced for educational or administrative use.
- Product Standards: Only AI tools that meet the DfE Product Safety Standards—including robust filtering, age-appropriate privacy notices, and "human-in-the-loop" oversight for significant decisions—will be authorised.
- Safeguarding: AI products must be configured to raise a safeguarding flag to the school's Designated Safeguarding Lead (DSL) if harmful or distressing content is detected.

15. 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 data protection impact assessments where the 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

16. 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
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords should be secure and contain letters and numbers that are used to access school computers, laptops and other electronic devices. Staff and pupils

are reminded to change their passwords at regular intervals and not to reuse passwords from other sites

- Encryption software is used to protect all portable devices and removable media, such as laptops. Due to the availability of online access to staff work areas, there should be no requirement for the use of USB/portable hard drives. If there is a requirement, these must be encrypted by suitable software.
- Personal information is not to be stored on staff, pupils, directors or governors' personal devices
- 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).

17. 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 paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.
Please see the St Gabriel the Archangel Catholic Multi Academy Trust Records Management policy for retention periods and disposal methods.

18. Personal data breaches

St Gabriel the Archangel Catholic Multi Academy Trust and all the 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 Annex B.

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 staff and/or pupils
- The accidental release of personal data via e-mail.

19. Training

All staff, Directors and Governors are provided with 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.

20. Monitoring arrangements

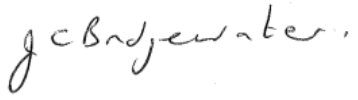
The Data Protection Officer is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Board of Directors.

21. Links with other policies

This data protection policy is linked to our:

- IT Acceptable Use Policy
- School Safeguarding policy
- CCTV policy (where applicable)
- Privacy Notices
- Freedom of information publication scheme
- Records Management policy

Version	Approval Date	Action/Notes	Signature of the Chair of Committee/Board
1	12/02/2026	Approved by BoD	
2	23/04/2026	Approved by Audit & Risk Committee	*P Rushworth*

Annex A: Consent for the use of photographs and videos

Child's name:

Date:

Dear [parent/carer name],

At [school name], we sometimes take photographs of pupils. We use these photos in the school's prospectus, on the school's website and on display boards around school. They are also used to assist catering staff to identify pupils who have allergens or special dietary requirements. The photographs may be used after your child has left the setting. [Add any other uses as appropriate.]

We would like your consent to take photos of your child and use them in the ways described above. If you are not happy for us to do this, it is no problem – we will accommodate your preferences.

Please tick the relevant box(es) below and return this form to the school office:

	Yes	No
I am happy for the school to take photographs of my child.		
I am happy for photos of my child to be used on the school website.		
I am happy for photos of my child to be used in the school prospectus.		
I am happy for photos of my child to be used in internal displays.		
I am happy for photos of my child to be used after they have left the setting		
I am happy for photos of my child to be used to assist catering staff to identify pupils with allergens or special dietary requirements.		

[insert other uses of photos here or delete]

If you change your mind at any time, you can let us know by emailing [email address], calling the school on [phone number], or just popping into the school office.

If you have any other questions, please get in touch.

Why are we asking for your consent again?

You may be aware that there are new data protection which came into effect in May 2018. To ensure we meet this requirement, we need to seek your consent to take and use photos of your child. We really value using photos of pupils, to be able to

showcase what pupils do in school and show what life at our school is like to others, so we would appreciate you taking the time to give your consent.

Parent or carer's Name:

(Please print)

Signature:

Date:

Annex B: Personal data breach procedure

The Data (Use and Access) (DUA) Act 2025 introduced stricter requirements for internal complaint handling before escalation to the ICO.

Complaints and Redress:

- Individuals must be informed of their right to make a complaint directly to the Trust regarding any data protection concerns before escalating to the ICO.
- The Trust will provide an easily accessible format - see Annex D for submitting these complaints and will acknowledge them within 30 days.

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO (DPO@sgacmatco.uk)
- 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
- Staff, Directors and Governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Principal and the Chair of the St Gabriel the Archangel Catholic Multi Academy Trust Audit & Risk Committee
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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 again) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the St Gabriel the Archangel Catholic Multi Academy Trust Gmail site with limited access to Data Protection staff.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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 of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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 on the St Gabriel the Archangel Catholic Multi Academy Trust Gmail site with limited access to Data Protection staff.

- The DPO and Principal will meet (this may be virtually) to review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible
- The DPO will inform the Chair of the St Gabriel the Archangel Catholic Multi Academy Trust Audit & Risk Committee on a termly basis to assess recorded data breaches and identify any trends or patterns requiring action to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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/external IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence), if this is possible
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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 endeavor to obtain 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, the DPO will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners

- The breach will be reported to the ICO where appropriate and applicable to do so.

A school laptop being stolen or hacked

- The user is to notify the schools IT section and DPO immediately on identifying the theft or hack
- The user is to confirm what category of data was contained on the laptop
- All laptops are to be encrypted so the potential for a data breach is minimised
- The incident should also be reported to the Police and a crime number obtained
- The breach will be reported to the ICO dependent on the category of data on the device and likely impact.

The school's cashless payment provider being hacked and parents' financial details stolen

- Parents will be advised as soon as possible following notification of a breach and advised to contact their bank
- The individual schools will liaise with the provider to identify the impact/level of breach
- The breach is to be reported to the ICO

Hardcopy reports sent to the wrong pupils or families

- Parents will be advised as soon as possible following notification of a breach
- The individual schools will liaise with the parties concerned to identify the impact/level of breach
- The breach is to be reported to the ICO dependent on the category of data included.

Annex C: Record of Data Breaches (Template)

Region	
Date of Breach	
Breach by Academy	
Date Reported to DPO	
Breach Reported by	
Brief description of the Nature of Breach & Category [1]	
Individuals Concerned (or Group/class)	
Consequences	
Risk Level [2]	
ICO Informed N/Y (and date)	
Data Subjects Informed (if High Risk)	
Measures to be taken	
Investigation	
Mitigate Adverse Effects	
Prevent Reoccurrence	

[1] Personal data or Special Category data
[2] Low, Medium or High

Annex D: Data Protection Complaint Form

This form should be used if you believe the Trust or one of its Academies has not complied with its obligations under the UK GDPR or the Data (Use and Access) Act 2025.

Section 1: Your Details

Full Name:
Address:
Email Address:
Relationship to the Trust/Academy: (e.g., Parent, Staff Member, Former Pupil)

Section 2: Details of the Complaint

Which Academy does this complaint relate to?

Please describe your complaint: *(Provide as much detail as possible regarding what happened, when it happened, and who was involved)*
What outcome are you seeking?

Section 3: Subject Access Requests (if applicable)

Does this complaint relate to a Subject Access Request (SAR)? (*Please tick)*	[ ] Yes	[ ] No
If yes, please provide the date the original request was made:	_____	

Section 4: Declaration

I confirm that the information provided in this form is correct to the best of my knowledge.

Signature:	**Date:**

Important Information for the Submitter

1. **Acknowledgement:** In accordance with the Data (Use and Access) Act 2025, the Trust will acknowledge receipt of this complaint within 30 days.

2. **Internal Review:** We aim to provide a full response following an internal investigation within 20 working days of the acknowledgement.

3. **Escalation:** Under the 2025 Act, you are required to complete this internal complaint process before escalating your concern to the Information Commission. If you remain dissatisfied after our final response, or if we fail to acknowledge your complaint within 30 days, you may then contact the regulator.