The St Gregory the Great Catholic Academy Trust

'Where love exists, it does great things'

Policy

Data Protection

Approved by: Trust Board

Date: June 2026

Review due: June 2028

Version: 2

1. Aims

This Data Protection Policy outlines our commitment to maintaining the privacy and protection of personal data in accordance with the Date Protection Act (2018) and UK General Data Protection Regulation (GDPR) as amended by the Date (Use and Access) Act 2025 and relevant data protection legislation.

The policy is intended for:

- Staff: All employees, including teaching and non-teaching staff, who handle personal data of students, parents, staff and other stakeholders
- Leadership Teams and Governors: Individuals responsible for overseeing and ensuring compliance with data protection practices
- Parents & Guardians: This policy provides essential information on how to manage the children's personal data and outlines their rights regarding that data
- Third Party – Contractors: External organisations or individuals processing data on behalf of the must understand their responsibilities under this policy.

We aim to make sure that all personal information about staff, students, parents, trustees, governors, visitors, and others is collected, stored, and used according to UK data protection laws (the UK General Data Protection Regulation and the Data Protection Act 2018). This policy covers all personal data, whether it is on paper or stored electronically.

2. Legislation and guidance

This policy meets our obligations under the:

Data Protection Act 2018 (DPA 2018)
UK General Data Protection Regulation (UK GDPR)
Date (Use and Access) Act 2025 (DUAA)

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. It also reflects the ICO's guidance for the use of surveillance cameras and personal information.
In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreement for the Academy Trust and its 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.
Term	**Definition**
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.
Academy Council	The local governing body
Trust	The St Gregory the Great Catholic Academy Trust.
Headteacher	The lead person in each school.
Governors	The governors appointed to the Academy Council of the individual school and the Directors of the Trust.
Trustees	The Directors of company number 10785982 (St Gregory the Great Catholic Academy Trust) as registered at Companies House
School/Schools	The academies within SGTG

4. The data controller

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

The Trust is registered with the Information Commissioner's Office (ICO) and pays the appropriate fee annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Board of Trustees

The Board is responsible for ensuring all data protection requirements are met across all CLT academies and the Trust central offices.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They may be required to provide an annual report of their activities directly to the Trustees 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 the ICO.

Our DPO is contactable by email: dpo@bywaterkent.co.uk

The Trust's data protection lead for the day to day management of data protection is the Trust CFO.

5.3 Headteachers

The Headteacher acts as the representative of the data controller on a day-to-day basis at the schools within the Trust.

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 European Economic Area
- 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 the Trust and our schools must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and transparently
- 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 school 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 **health or social care purposes**, 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 **public health reasons**, and the processing is done by, or under the direction of, a health 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.

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 school's record retention schedule.

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 UK data protection law
- Set up a data sharing agreement, either in the contract or as a separate document, if we are sharing significant or sensitive data, to ensure data is handled fairly and legally
- Only share data that the supplier or contractor needs to carry out their service and any necessary information to keep them safe.

We will also share personal data with law enforcement and government bodies including other Academies and schools if 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.

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 Trust and/or our schools hold 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. However, we encourage that requests 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 Trust's data protection lead who will liaise with 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.

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.

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 high 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 up to two forms of identification
- May contact the individual via telephone to confirm the request was made
- Will respond without delay and within one calendar month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary.

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 can't reasonably anonymise, and we don't 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

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 consider 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

Although Academies do not have a legal duty to do so, in the spirit of data protection best practice, Academies in the Trust will respond positively to a request from a parent or someone with parental responsibility to access their child's educational record. Generally, we will ask for the child's consent to the request if they are aged 12 or over. This includes most information about a pupil. Parents or those with parental responsibility can make the request to the administration contact within each school.

If the request is for a copy of the educational record the school may charge a fee to cover the cost of supplying it.

There are certain circumstances in which the Academy may refuse the request. This includes, but is not limited to, where releasing the information might cause serious harm to the physical or mental health of the pupil or another individual or if it would mean releasing exam marks before they are officially announced or if the request is considered vexatious.

In circumstances where a request is refused, the Academy will explain its reasons for doing so and will discuss with the parent or person with parental responsibility whether any more limited information can be provided or whether the information may be provided at a later date.

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.

If, and 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 pay for school dinners in cash 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(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. Artificial Intelligence (AI)

AI tools are now common and easy to use. Staff, students, and parents may be familiar with generative AI chatbots like ChatGPT and Copilot, the Trust/School understands that AI can help students learn and support staff but it also has risks for personal and sensitive information.
To keep this information safe, no one is permitted to enter personal or sensitive data into unauthorised AI tools or chatbots. If anyone does enter such data into an unauthorised generative AI tool, the trust/school will treat it as a data breach and will follow the procedures for handling personal data breaches outlined in Appendix 1

13. CCTV

Where we use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice 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 Head Teacher at the appropriate school.

14. Photographs and videos

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

Under 13 years old

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.

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 have agreed to this.

Over 13 years old (Secondary schools)

We will obtain written consent from parents/carers, or pupils aged 13 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.

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 the Trust and its schools take photographs and videos, uses may include:

- Within schools on notice boards and in school magazines, brochures, newsletters, etc.
- Outside schools by external agencies such as the school photographer, newspapers, campaigns
- Online on the Trust and schools' websites 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.

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
- Putting appropriate checks in place if we transfer any personal data outside the UK where no adequacy agreements are in place.
- Maintaining records of our processing activities, including:
- For the benefit of data subjects, making available the name and contact details of our school 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, 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, 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 that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or trustees and governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (see the schools [online safety policy/ICT policy/acceptable use agreement/policy on acceptable use).
- 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 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 school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

The Trust 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 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. 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

19. Training

All staff and governors are provided with data protection training as part of their induction process. In line with the ICO's recommendation, refresher training will be provided to all staff regularly and not less than biannually.

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

20. Making and Handling Complaints about Personal Data

In accordance with Section 164a of the Data (Use and Access) Act 2025 trust/school are now required to include information on how to raise a complaint relating to data protection – see below.

How to Make a Data Protection Complaint

- **Your Right to Complain**
  You have the right to make a complaint if you believe school have handled your personal data in a way that breaches the UK GDPR or Part 3 of the Data Protection Act.
- **How to Make a Complaint**
  A complaint can be made using the template form in Appendix 2, this is also available directly from the school. Once complete, this should be submitted to the school/trust via insert contact details.
- **Acknowledging a Complaint**
  The DPO will acknowledge receipt of a complaint within **30 days**.
- **Responding to a Complaint**
  Complaints will be investigated as quickly as possible and without undue delay, this will include taking the necessary steps to investigate and deal with any concerns.
- **Keeping You Informed**
  As part of handling your complaint, we may make enquiries to better understand what has happened and keep you updated on the progress of our investigation. Once complete, you will be informed of the outcome.
- **Escalation to the ICO**
  If a complaint is not resolved by the DPO, the data subject can escalate it to the Information Commissioner for further investigation.

21. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and approved every two **years** by the trustees and shared with academy councils.

22. Links with other policies

This data protection policy should be read in conjunction with all other relevant policies at both Trust and school level.

Appendix 1 - Personal data breach procedure

The Trust will investigate and report data breaches to the ICO where, on the advice of the DPO, the breach meets the criteria for reporting, or it would be safer in the context to do so.

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 data protection lead in school.
- The data protection lead will contact the DPO for advice and guidance 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
- If the breach is deemed to be serious enough to be reported to the ICO, unless this has already been done, the DPO will alert the headteacher and the chair of governors
- The DPO and data protection lead in school 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 n individual affected by the breach. Documented decisions are stored on the DPO's computer system/school's computer system, or on a designated software solution.
- Where the ICO must be notified, the DPO will do this (unless the data protection lead in the school agrees to do so) 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 on the school's computer system, or on a designated software solution.
- The DPO, headteacher or designated senior leader 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 that you might want to consider 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 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: Data Protection Complaint Form

Your details

Name:

Email:

Phone:

Date of Incident:

Type of Issue
☐Unauthorised Access
☐Data Loss/theft
☐Improper Sharing
☐Consent Issue
☐Other

Summary of Incident

Declaration:
I confirm this information is accurate

Signature Date:

Submit this form to the Headteacher/Trust Office (tel.: 01132700978) who will acknowledge receipt of the complaint within the period of 30 days from when the complaint is received.

The
St Gregory the Great
Catholic Academy Trust

'Where love exists, it does great things'

All policies are written in line with our Trust Mission Statement:
Within the St Gregory the Great Catholic Academy Trust, our academies are communities where our children and young people are given a clear vision for life, a vision which is rooted in the person and teachings of Jesus Christ and which is faithful to the mission of the Catholic Church.

St Gregory the Great Catholic Academy Trust is a charity and a company limited by guarantee.
Registered in England and Wales.
Company number 10785982
Registered office Holy Rosary and St Anne's Catholic Primary School, Leopold Street, Leeds, LS7 4AW

Website: stgregorythegreatacademytrust.org.uk
Tel: 0113 8246360
Email: info@sgtgcat.org.uk

CSEL: Mr Peter Hughes NLE

Diocese of Leeds
Vicariate of Education