NEWMAN CATHOLIC TRUST

HEART SPEAKS TO HEART

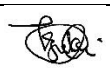
Data Protection Policy

2026-27

Review Cycle	Date of Policy	Reviewed by	Review Date
Annual	April 26	FAR	April 27

Changes and updates are highlighted in GREEN

Ratification

Role	Name	Signature	Date
Chair of Board	**Chris Izuka**		**April 26**
CEO	**Dr Daniel Doyle**		**April 26**

Commitment to Equality:

The Trust and its schools are committed to providing a positive working environment which is free from prejudice and unlawful discrimination and any form of harassment, bullying or victimisation. We have developed a number of key policies to ensure that the principles of Catholic Social Teaching in relation to human dignity and dignity in work become embedded into every aspect of school life and these policies are reviewed regularly in this regard.

"Rooted in faith, we ignite a love of learning, foster inclusive education and empower every individual to achieve their utmost potential."

At the Newman Catholic Trust, we stand united in our unwavering mission to nurture a transformative educational experience, where every child is seen, valued, and cherished as a unique gift from God. Rooted in faith, we ignite a love for learning that awakens curiosity, sparks imagination, and fuels a lifelong journey of discovery.

Guided by the teachings of Christ and inspired by the profound wisdom of our namesake, Saint John Henry Newman, we strive to foster a community where inclusion is lived, diversity is embraced, and every individual is empowered to fulfil their highest potential. As Newman said, *"To live is to change, and to be perfect is to have changed often."* We believe that education is a sacred journey of continual transformation—intellectually, spiritually, and personally. We believe that true education is not just about knowledge, but about shaping hearts and minds, cultivating resilience, and nurturing the whole person.

Our vision is simple yet profound: To be a beacon of **Hope** and **Excellence**, where pupils are not only academically accomplished but spiritually enriched and personally inspired to make a difference in the world.
In all that we do, we seek to embody our Trust's **HEART Values**, which define who we are and guide how we serve:

- **Hope** – Believing in the boundless potential of every child, and striving to build a future filled with possibility, courage and faith.
- **Excellence** – Pursuing the highest standards in learning, leadership and love, so that every action reflects our calling to greatness.
- **Authenticity** – Living truthfully and faithfully, ensuring our words, actions and decisions are grounded in integrity and the Gospel.
- **Responsibility** – Caring for one another and for creation with compassion, stewardship and a deep sense of duty to the common good.
- **Truth** – Seeking wisdom and understanding through Christ, who is the Way, the Truth and the Life.

Together, **Heart to Heart and Hand in Hand**, we build communities of faith and learning where every child flourishes — intellectually, spiritually and morally — for the greater glory of God.

Contents

The Cardinal Newman Catholic Trust collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be legal requirements to collect and use information to ensure that the school complies with its statutory obligations.

The Cardinal Newman Catholic Trust is registered as a Data Controller with the Information Commissioner's Office (ICO) detailing the information held and its use.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the UK General Data Protection Regulation and the Data Protection Act 2018. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, irrespective of whether it is held in paper files or electronically.

Contents

1. Definitions

We have set out below the key definitions that are contained within the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). You will find this useful in understanding their meaning and effect when interpreting your rights and our obligations under the UK GDPR and DPA.

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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.

2. The Data Controller The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

3. Roles and Responsibilities This policy applies to all staff employed by the Trust and to external organisations or individuals working on our behalf.

3.1 Governing Board The Cardinal Newman Catholic Trust has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

3.2 Chief Executive Officer (CEO) The CEO is responsible for overseeing the implementation of this policy, ensuring appropriate leadership oversight of data protection compliance and developing related policies and guidance where applicable.

The CEO retains overall executive accountability for data protection across the Trust. Day-to-day data protection queries, operational matters and individual rights requests should be directed to the Trust's named operational lead and/or Data Protection Officer. Trust contact details can be found on the Trust website.

The CEO acts as the Trust's Data Protection Lead and is the main point of contact for day-to-day data protection matters, individual rights requests and significant data protection concerns. Where appropriate, the CEO will seek advice from the Trust's external Data Protection Officer or data protection adviser.

The CEO is also the first point of contact for individuals whose data the Trust processes and for the ICO. **Contact details of the CEO and Trust can be found at www.newmancatholictrust.com**

3.3 Trust Data Protection Support

The Trust may delegate aspects of the administration and co-ordination of data protection work to other senior leaders or central staff as appropriate. However, overall leadership and oversight remains with the CEO as the Trust's Data Protection Lead.

3.4 Data Protection Officer (DPO)

The Trust will appoint a suitably qualified Data Protection Officer, either internally or through an external provider, to fulfil its statutory obligations under UK GDPR.

The DPO will:

• advise the Trust on its obligations under data protection law
• support compliance monitoring and policy development
• advise on data protection impact assessments where required
• provide advice in relation to personal data breaches and reporting obligations
• act as an independent point of contact where required by law

As a small Trust, the Newman Catholic Trust may obtain external Data Protection Officer or specialist data protection advice where appropriate. External support may be used to advise on compliance, support data protection impact assessments, provide advice on personal data breaches and assist the Trust in meeting its obligations under UK GDPR and the Data Protection Act 2018.

3.5 All Staff Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the **Estates & Operations Lead or CEO** 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 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

4. Data Protection Principles The UK GDPR is based on data protection principles that the Trust must comply with.
The principles state that personal data must be:

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

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

5. Collecting Personal Data
5.1 Lawfulness, Fairness and Transparency We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual, e.g. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest and carry out its official functions
- The data needs to be processed for the legitimate interests of the Trust 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 and explicit consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.
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) or from the pupil if they are aged 13 and over.
5.2 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.

6. Sharing Personal Data We will not normally share personal data with anyone else but may do so where:

- There is an issue that puts the safety of our staff, pupils or stakeholders 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 data-sharing agreement 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 and necessary information to keep them safe while working with us

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

7. Subject Access Requests and Other Rights of Individuals
7.1 Subject Access Requests Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust 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
- 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

Subject access requests should include:

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

If staff receive a subject access request, they must immediately forward it to the **CEO or Operations & Estates Manager**.

7.2 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 or be aged 13 and under.

7.3 Responding to Subject Access Requests When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- 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 will not disclose information if it:

- Might cause serious harm to the physical or mental health of the individual or another person
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why and inform them of their right to complain to the **ICO**.

7.4 Other Data Protection Rights of the Individual In addition to the right to make a subject access request and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision-making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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 **CEO or Operations & Estates Manager**. If staff receive such a request, they must immediately forward it to the **CEO or Operations & Estates Manager**.

8. Parental Requests to See the Educational Record Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 Trust working days of receipt of a written request.

9. Biometric Recognition Systems Where the Trust uses biometric data as part of an automated biometric recognition system (for example, using fingerprints for access to services), it will comply with the requirements of the **Protection of Freedoms Act 2012**.
Parents/carers will be notified before any biometric recognition system is implemented or before their child first takes part in it. The Trust will obtain written consent from at least one parent or carer before collecting and processing any biometric data from their child.
Parents/carers and pupils have the right to opt out of the Trust's biometric recognition system(s). Alternative means of accessing the relevant services will be provided for those who do not wish to participate. For example, pupils may be given alternative authentication methods.
Parents/carers and pupils may object to the use of biometric data or withdraw consent at any time, in which case the Trust will ensure that any relevant data already captured is securely deleted.
As required by law, if a pupil refuses to participate in or continue participation in the processing of their biometric data, the Trust will not process that data, regardless of any consent given by a parent or carer.
Where biometric systems are used for staff or other adults, their consent will be obtained prior to participation. Staff and other adults can withdraw their consent at any time, and any biometric data will be securely deleted upon withdrawal.

10. CCTV The Trust uses CCTV in various locations to maintain safety and security. The presence of CCTV will always be clearly signposted to ensure individuals are aware that they are being recorded.
The Trust does not require individuals' permission to use CCTV for security purposes, but clear signage will indicate where recording is taking place. Security cameras will remain visible, and notices will explain their purpose.
Any enquiries about CCTV should be directed to the **CEO**.

11. Photographs and Videos As part of its operations, the Trust may take photographs and record images of individuals within its schools and offices.
Written consent will be obtained from parents/carers, or where appropriate, the pupil, before taking and using photographs or videos for communication, marketing or promotional purposes. The intended use of these images will be clearly explained.
Photographs and videos may be used:

- Within Trust schools on noticeboards, newsletters or promotional materials
- By external agencies such as school photographers, newspapers or educational campaigns
- Online, including the Trust's website or official social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, the Trust will delete the photograph or video and ensure it is no longer distributed.
To protect privacy, photographs and videos used for promotional or online purposes will not include any additional personal data about the pupil that would allow them to be identified.

12. Data Protection by Design and Default The Trust is committed to integrating data protection into all data processing activities. Measures include:

- Appointing a suitably qualified **Data Protection Officer (DPO)** and ensuring they have the necessary resources to fulfil their duties
- Processing only personal data that is necessary for each specific purpose, ensuring compliance with UK GDPR principles
- Conducting **Data Protection Impact Assessments (DPIAs)** for any processing that may pose high risks to individuals' rights
- Embedding data protection into all internal policies, procedures and privacy notices
- Providing regular training to staff on data protection law, ensuring compliance and awareness

- Conducting periodic audits to test the effectiveness of privacy measures and ensure compliance
- Maintaining records of all processing activities, including details of:
    - The type of data processed
    - The purpose of processing
    - Data subjects and third-party recipients
    - Data storage methods and retention periods
    - Security measures in place to protect personal data

13. Data Security and Storage of Records The Trust will ensure that all personal data is stored securely and protected against unauthorised access, loss or damage. Measures include:

- Keeping paper-based records and portable electronic devices (such as laptops and hard drives) in locked storage when not in use
- Ensuring confidential personal data is not left on desks, noticeboards or in public areas
- Implementing strict access controls for all personal data stored digitally
- Using password protection for all Trust computers, laptops and mobile devices
- Enforcing regular password updates for staff and pupils
- Encrypting portable devices and removable media such as USB drives to protect stored data
- Requiring any personal data taken off-site to be formally checked out and tracked
- Conducting due diligence before sharing personal data with third parties to ensure they have appropriate security measures in place

14. Disposal of Records Personal data that is no longer needed will be securely disposed of in accordance with data retention guidelines. Any inaccurate or outdated data that cannot be corrected will also be securely destroyed.
Where a third-party provider is used to dispose of records, the Trust will ensure that the provider complies with **UK GDPR** and has appropriate data disposal measures in place.

15. Personal Data Breaches
The Trust will take all reasonable steps to prevent personal data breaches. Any actual or suspected personal data breach must be reported immediately to the CEO.
The CEO will take immediate steps to contain the breach, establish the facts and, where appropriate, seek advice from the Trust's external Data Protection Officer or data protection adviser.
The CEO will determine, with external advice where required, whether the incident amounts to a personal data breach, whether it is reportable to the ICO and whether affected individuals must be informed.
Where required, the Trust will notify the ICO within 72 hours of becoming aware of a reportable personal data breach.
Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Trust will inform affected individuals without undue delay.
All personal data breaches, whether reportable or not, will be documented along with the actions taken, lessons learned and steps implemented to reduce the risk of recurrence.

16. Training All current and new staff and governors will receive data protection training as part of their induction and ongoing professional development. Training will cover:

- UK GDPR principles and individual rights
- How to manage and protect personal data
- Identifying and reporting potential data breaches
- Best practices for secure data handling

17. Monitoring Arrangements
The CEO is responsible for monitoring and reviewing this policy, seeking external data protection advice where appropriate. The policy will be reviewed annually and updated as necessary to ensure compliance with UK GDPR, the Data Protection Act 2018 and relevant guidance.

18. Links with Other Policies This data protection policy is linked to other policies that the Trust may implement from time to time, such as the **ICT policy**.

Appendix 1: Personal Data Breach Procedure This procedure is based on guidance on personal data breaches produced by the **ICO**.

- On discovering or suspecting a personal data breach, the staff member or any external data processor must immediately notify the CEO.
- The **CEO** will investigate the report and determine whether a breach has occurred. To decide, the **DPO** will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The **CEO** will alert the **Chair of Governors**.
- The **CEO** will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- The **CEO** will assess the potential consequences based on their severity and likelihood.
- The **CEO** will determine whether the breach must be reported to the **ICO**. This must be judged on a case-by-case basis. To decide, they will consider whether the breach is likely to negatively affect people's rights and freedoms and cause any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identity 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 is likely that there will be a risk to people's rights and freedoms, the **DPO** must notify the **ICO**.

- The **CEO or** will ensure that a record of security breaches is maintained and document all decisions taken in respect of the management and conduct of such breaches.
- Where the **ICO** must be notified, the **CEO** will do this via the **'report a breach'** page of the **ICO website** within **72 hours**. As required, the report will include:
    - 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 **CEO**
    - 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 individuals concerned
- If all the above details are not yet known, the **CEO** will report as much as possible within **72 hours**. The report will explain any delay, the reasons why, and when further information is expected. The remaining information will be submitted as soon as possible.
- The **CEO** 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 **CEO** 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 **CEO**
    - 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
- The **CEO** will notify any relevant third parties who can help mitigate the loss to individuals, such as the police, insurers, banks, or credit card companies.
- The **CEO** will document each breach, irrespective of whether it is reported to the **ICO**. For each breach, this record will include:
    - Facts and cause
    - Effects

    - Actions taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The **CEO** will meet to review what happened and how it can be prevented in the future. This meeting will happen as soon as reasonably possible.
- Where appropriate, action will be taken to recover or retrieve lost or stolen data using expert help if necessary.