The Newman Catholic Collegiate

Data Protection Policy

Version 5: 07.02.2025

Contents

1. Aims 1
2. Legislation and guidance 1
3. Policy Statement 1
4. Definitions 2
5. The Data controller 3
6. Roles and responsibilities 3
7. Data protection principles 5
8. Collecting personal data 6
9. Sharing personal data 7
10. Subject access requests and other rights of individuals 8
11. Parental requests to see the educational record 10
12. Biometric recognition systems 10
13. CCTV 11
14. Photographs and videos 11
15. Data protection by design and default 11
16. How to decide whether you need to do a Data Protection Impact Assessment (DPIA) 12
17. Data security and storage of records 14
18. Disposal of records 14
19. Right of erasure 15
20. Personal data breaches 15
21. Training & Awareness 15
22. Monitoring arrangements 15
23. Links with other policies 16
Appendix 1: Personal data breach procedure 17
Appendix 2 - Data Protection Breach/Incident Reporting Statement 20
Appendix 3 – Data Protection Impact Assessment template 23

Approved by: **Board of Directors**	**Date:** 07.02.2025
Last reviewed on:	31.01.2025
Next review due by:	31.01.2027

Document Control

Date	Revision/Amendments	Author
31.01.2025	Page 7 – Sharing Personal Data	K Davies
31.01.2025	Page 10 – Responding to Subject Access Requests	K Davies

1. Aims

The Newman Catholic Collegiate is registered as a data controller with the information Commissioners Office (ICO) to process personal information to enable us to provide education, educational support services and manage our employees. The Collegiate aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and will be reviewed every 2 years.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data for St Margaret Ward who use biometric data for the cashless catering system and photocopying. It also reflects the ICO's code of practice for the use of surveillance cameras for those schools in the Newman Catholic Collegiate who operate CCTV and the collection of personal information.

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

3. Policy Statement

The Collegiate will hold the minimum amount of personal information necessary to enable it to perform its functions and information will be erased once the need to hold it has passed. Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay. All personal data will be fairly obtained in accordance with the Collegiate Privacy Notice, which is available to all students, staff and parents. Data will be lawfully processed in accordance with the principles for processing personal data lawfully and fairly.

4. Definitions

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.

5. The Data controller

Our collegiate processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Newman Catholic Collegiate are registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6. Roles and responsibilities

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

6.1 The Board of Directors

The Board of Directors for the Newman Catholic Collegiate have overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

Directors must ensure that the collegiate:

- Monitors their data protection performance
- Supports the data protection officer
- Has good network security infrastructure to keep personal data protected
- Has business continuity and cyber security plans in place

6.2 Data protection officer

The data protection officer (DPO) & Chief Operating Officer (COO) 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/COO are also the first point of contact for individuals whose data the collegiate processes, and for the ICO.

The COO is responsible for:

- Advising school leaders and staff about their data obligations
- Monitoring compliance
- Conducting regular data audits alongside the third party DPO
- Developing and updating data protection policies and procedures
- Advising when data protection impact assessments (DPIA) are needed
- Answering data protection enquiries from staff, parents, pupils and governors with support form the third party DPO
- Making sure privacy notices are regularly reviewed and updated
- Communicating with the Information Commissioner's Office (ICO)
- Reporting to the directors about data protection

The Collegiate Data Protection contact is:

Chief Operating Officer

Telephone: 01782 821995

Email: kdavies@newmancc.co.uk

Address: 83 Little Chell Lane

Tunstall

Stoke on Trent

ST6 6LZ

Our DPO is provided by a third party and can be contacted by:

Telephone: 01785 277005

Email : dpo.schools@staffordshire.gov.uk

Address: Information Governance Unit

IGU | Staffordshire County Council

4th Floor, Staffordshire Place 1,

Tipping Street, Stafford, ST16 2DH

6.3 Principal

The principal acts as the representative of the data controller on a day-to-day basis.

Principals are accountable for:

- Deciding how the school uses technology and maintains its security
- Deciding what data is shared and how
- Understanding what UK GDPR and the Data Protection Act covers and getting advice from the COO & third party DPO, as appropriate
- Assuring governors that the school has the right policies and procedures in place
- Making sure staff receive annual training on data protection, including Subject Access Requests (SARs) and Freedom of Information request (FOI)

6.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school/collegiate of any changes to their personal data, such as a change of address. The personal data held about staff will include contact details, employment history, information reacting to career progression, information relating to DBS checks, information relating to eligibility to work in the UK, photographs, occupational pensions and next of kin.
- Contacting the Chief Operating Officer/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

7. Data protection principles

The GDPR is based on data protection principles that our collegiate 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 the collegiate aims to comply with these principles.

8. Collecting personal data

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

8.2 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.

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 Collegiate Record Retention Schedule.

9. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- A pupil transfers to a new school
- 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, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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

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

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

Before we share any data, we will:

- consider all the legal implications
- check if we need permission to share the data
- confirm who needs the data, what data is needed and what they'll use it for
- make sure that we have the ability to share the specified data securely
- check that the actions cannot be completed or verified without the data

10. Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the collegiate holds about them. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system".

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 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 must be submitted in writing either by email or letter to the DPO contact named in 5.2 and the Chief Operating Officer for the collegiate.

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 DPO and inform the Chief Operating Officer.

10.2 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.

The Newman Catholic Collegiate 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.

The Newman Catholic Collegiate Secondary School:

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 secondary school 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.

10.3 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
- May ask for clarification with regards to what personal data the individual wants
- All requests will be sent to the DPO within 3 working days of receipt and the Chief Operating Officer must be made aware of the SAR.
- Will respond without delay and within 1 month of receipt of the request
- All files must be reviewed by the DPO before any disclosure takes place. Access will not be granted before this review has taken place.
- Where all the data in a document cannot be disclosed, a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- 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
- 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
- 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 within one month, and tell them they have the right to complain to the ICO.

Keep a record of any subject access request, including:

- The request itself
- The date you received it
- All correspondence relating to the request (do not keep personal documents used to confirm identity)
- What you provided
- When you provided it
- Confirmation that the requester received the data in question
- Details of your decision-making rationale in case of challenges

Delays to SAR processing

In some cases, the calendar month response time can be paused if we are unable to progress with the request.

We may need to pause the request if:

- we are waiting for a requester to confirm their identification
- we are waiting for the requester to provide evidence of their authority to act on behalf of another individual
- we are seeking reasonable clarification about the request

10.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- 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 DPO and Chief Operating Officer. If staff receive such a request, they must immediately forward it to the DPO and Chief Operating Officer.

11. Parental requests to see the educational record

Parents, or those with parental responsibility, may request their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

12. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints 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 collegiate schools will obtain 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 biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners online via Tucasi if they wish.

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

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

Where staff members or other adults 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.

13. CCTV

We use CCTV in various locations around the Newman Catholic Collegiate school sites 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 Academy Manager at the individual school site.

14. Photographs and videos

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

The Newman Catholic Collegiate 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.

The Newman Catholic Collegiate 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.

Uses may include:

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

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

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

See our safeguarding policies for more information on our use of photographs and videos.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all 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 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. This will take place as part of our internal audit processes.
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our collegiate and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

16. How to decide whether you need to do a Data Protection Impact Assessment (DPIA)

A data protection impact assessment (DPIA) helps you to identify and minimise data protection risks to comply with your obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage.

The DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance.

Schools must conduct a data protection impact assessment (DPIA) where a proposed data processing activity is likely to result in a high risk to people's rights and freedoms. In consultation with the data protection officer, it is up to the school to work out whether the processing meets this description.

Data Protection should be treated in the same way as any other risk, so a DPIA should be conducted in the same way as a risk assessment.

Listed below are the types of processing that will always require a DPIA under the GDPR. All your processing activities may not fit the criteria for 'high risk' processing and therefore do not legally require a DPIA. It is good practice to conduct one whenever you change your data processing.

The person undertaking the processing activity should carry out the DPIA and consult with relevant individuals and experts as required.

If a DPIA needs to be completed, please use the DPIA template in appendix 3.

Type or Processing	Example
Large scale use of sensitive 'special category' data, or data on criminal convictions	• Trade union membership data • Health records • Social care records • Research projects
Monitoring of a publicly accessible area	• Audio/video surveillance of public areas e.g. CCTV in and around school
Processing of biometric data	• Facial or thumbprint recognition systems • Building access systems • Identity verification • Access control and identity verification for hardware and applications (e.g. Voice, fingerprint & facial recognition)
Matching, combining or comparing personal data obtained from multiple sources	• Monitoring use or uptake of statutory services or benefits
Tracking an individual's location or behaviour	• Data processing at the workplace • Data processing in the context of home and remote working
Targeting children or other vulnerable individuals, particularly for marketing purposes, to create a profile of them, or if you intend to offer online service directly to them	• Social networks and applications
Processing that puts people at risk of physical harm if there was a data breach	• Whistleblowing/complaint procedures • Social Care records
Changes in school processes	• New visitor sign-in system
New technology purchased or implemented	• ICT hardware or software e.g. your management information system (MIS) • Changes to the ICT infrastructure e.g. moving to the cloud • New devices purchased e.g. tablets for lessons, laptops for staff
Changes to suppliers or service providers	• Switching catering or payroll providers

16.1 Decide whether the data processing activity can go ahead

The DPIA should be monitored as it is being carried out and once completed the Academy Manager should meet with the Principal/SLT and decide whether to proceed with the proposed activity. The outcome of the DPIA should be scrutinised by completing the following steps.

- RAG rate the risks (red, amber or green) after the safeguards have been put into place
- Analyse whether the risk is acceptable by weighing up the impact on people's rights and freedoms
- If there is a risk that you cannot take measures to reduce, then seek advice from the ICO.

16.2 Consulting the ICO

If the DPIA has identified a high risk that the school cannot mitigate then the ICO must be consulted before the data processing activity starts. A copy of the DPIA will need to be sent to the ICO if you need to consult with them.

16.3 Monitoring the implementation of the processing activity

You must monitor the ongoing performance of the processing activity that required the DPIA.

- Set a review date
- Refer to the record of safeguards implemented and check they are proving effective
- If there are any substantial changes to the nature, scope, context or purposes of the processing activity then the school will need to repeat the DPIA.
- Publishing a DPIA is not a legal requirement of the GDPR, it is the controller´s decision to do so. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA.

17. 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 that are at least 12 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our acceptable use policy)
- 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)

18. 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 collegiate behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19. Right of erasure

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

19.1 When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which it was originally collected or processed
- you must do it to comply with a legal obligation (e.g. following recommended retention periods)

19.2 When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for the establishment, exercise or defense of legal claims

20. Personal data breaches

The collegiate 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. 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
- Staff payroll information

21. Training & Awareness

All staff and governors are provided with data protection training and data handling awareness 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.

22. Monitoring arrangements

The Chief Operating Officer along with the DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary, when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our collegiate practices. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the Board of Directors.

23. Links with other policies

This data protection policy is linked to our:

- IT Acceptable Use Policy
- Safeguarding policy
- CCTV policy
- Privacy Notice
- Information Security Policy
- Anti-Fraud Policy
- Cyber-Security Response Plan

Appendix 1: Personal data breach procedure

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 Chief Operating Officer/Data Protection Officer, who will notify the third party DPO.
- The COO/DPO and where necessary the third party DPO (Entrust) will investigate the report and determine whether a breach has occurred. To decide, the COO/DPO/Entrust 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 Chief Operating Officer/DPO will communicate with the Principal
- The Chief Operating Officer/DPO will notify the Catholic Senior Executive Leader and Chair of the Board of Directors
- The third party DPO (Entrust) will assist the COO to 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 COO/DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The COO/DPO & third party DPO (Entrust) will review and decide whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the COO/DPO/Entrust 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 is likely that there will be a risk to people's rights and freedoms, the DPO/COO must notify the ICO.
- The COO/DPO will document the decision (either way), to ensure that evidence is available in the event of a challenge at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the schools/collegiate computer system.
- Where the ICO must be notified, the COO/DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the COO/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 COO/DPO & third party DPO (Entrust)
    - 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 COO/DPO will report, considering all information currently available, as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the COO/DPO expects to have further information. The COO/DPO will submit the remaining information as soon as possible.
- The COO/DPO & third party DPO (Entrust) 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 COO/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 COO/DPO & third party DPO (Entrust)
    - 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 COO/DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers or banks.
- The COO/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 schools/collegiate computer system in a secured area.
- The Principal, Catholic Senior Executive Leader and Chief Operating Officer/Data Protection Officer will meet to review details of the incident and consider options for any repeat occurrence. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

The Newman Catholic Collegiate 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 Chief Operating Officer/DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Chief Operating Officer/DPO will ask the ICT Manager to recall it
- In any cases where the recall is unsuccessful, the Chief Operating Officer/ 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 Chief Operating Officer/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 COO/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
- The breach will be reported to the ICO

Academy/collegiate laptop being stolen or hacked

- The staff member should notify the IT Manager and Principal immediately
- The staff member to confirm what documents/software are on the laptop and confirm whether any known persons had access to the laptop other than themselves.
- Report the incident to the police and obtain a crime number.
- COO/DPO to investigate the potential consequences and report the breach to the ICO if necessary
- All laptops/USB sticks are encrypted to minimise the risk.

SIMs being hacked and pupils and staff details being stolen

- Notify the IT Manager and Principal immediately
- Parents/carers/staff will be advised as soon as possible about the breach
- Contact the schools Safeguarding lead and any outside agencies and advise them of the breach
- Contact the third party provider to ascertain how much data has been affected
- Report the incident to the police and obtain a crime number
- COO/DPO to investigate the level of impact and consequences and report the breach to the ICO

The collegiate online payment system being hacked and parents' financial details being stolen

- Notify the Chief Operating Officer/Data Protection Officer, Catholic Senior Executive Leader and Principals immediately
- Parents will be advised as soon as possible about the breach and advised to contact their bank
- Contact the third party provider to ascertain how many parents have been affected and which schools
- Report the incident to the police and obtain a crime number
- Depending upon the level of financial information obtained this may be reportable to the ESFA
- COO/DPO to investigate the level of impact and consequences and report the breach to the ICO

Appendix 2 - Data Protection Breach/Incident Reporting Statement

Immediate Action (Within 24 Hours)

If a collegiate employee, agency staff, Director, academy governor or other third party is made aware of an actual data breach, they must report it to their line manager and the principal within 24 hours and they must complete the Data Protection Breach/Incident Reporting Statement below.

Staff name: **Job Role:**	
Description of breach: Please explain as much as possible about what happened, what went wrong and how it happened.	
Was the breach caused by a cyber-Incident?	
How did you find out about the breach?	
When did the breach occur? (Date & Time)	
When was the breach discovered? (Date & Time)	
Has there been any delay in the reporting of the breach and why?	
Which categories of personal data are included in the breach: • Basic personal identifiers (e.g. name & contact details) • Identification data (e.g. usernames & passwords) • Data revealing racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Sexual orientation data • Health data • Economic & financial data (e.g. credit card numbers, bank details) • Official documents (e.g. driving licence) • Location data • Genetic or biometric data • Criminal convictions, offences • Not yet known • Other, please specify	

Number of personal data records concerned	
Which data Subjects are involved? • Pupils • Parents • Staff	
Date reported to data subjects	
Potential consequences of the breach: Please describe the possible impact on data subjects as a result of the breach and whether there has been any actual harm to any data subjects.	
What is the likelihood that data subjects will experience significant consequences as a result of the breach?	
In the case of cyber incidents, has the confidentiality, integrity and/or availability of the academy systems been affected?	
Describe any measures in place before the breach with the aim of preventing a breach of this nature.	
Corrective actions taken	
Actions approved by & Date approved	

Appendix 3 – Data Protection Impact Assessment template

Step 1: Identify the need for a DPIA

Explain broadly, what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: • How will you collect, use, store and delete data? • What is the source of the data? • Will you be sharing data with anyone? • What types of processing identified as likely high risk are involved?

Describe the scope of the processing:

- What is the nature of the data, and does it include special category or criminal offence data?
- How much data will you be collecting and using?
- How often?
- How long will you keep it?
- How many individuals are affected?

Describe the context of the processing:

- What is the nature of your relationship with the individuals?
- Do they include children or other vulnerable groups?
- How much control will they have?
- Would they expect you to use their data in this way?
- Have there been any prior concerns or previous security flaws to do with this type of processing?
- Is it novel in any way?
- What is the current state of technology in this area and are there any current issues of public concern that you should factor in?

Describe the purposes of the processing: • What do you want to achieve? • What is the intended effect on individuals? • What are the benefits of the processing for you, and more broadly?

Step 3: Consultation Process

Consider how to consult with relevant stakeholders: • When and how you will seek individuals' views on your data processing activity? • If you feel it is not appropriate to consult with relevant stakeholders, how can you justify the decision? (Make sure you always record any decision not to consult) • If you are consulting, who else within your organisation do you need to involve? • Do you need to ask your processors or any other third parties to help with the consultation? • Do you plan to consult information security experts, or any other experts? •

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: • What is your lawful basis for processing the data this way? • Does the processing actually achieve your purpose? • Is there a less intrusive way to achieve the same outcome? • How will you ensure the data is good quality and limited to what is necessary? • What information will you give individuals about how their data is used? • How will you help to support their rights under GDPR? • What measures do you take to ensure processors and other third parties comply with data protection law? • How do you safeguard any international transfers of the data?

Step 5: Identify and assess risks

Describe the source of risk and the nature of potential impact on individuals. Risks may include: • A privacy breach caused by technical issues or human error, where individuals are at risk of discrimination, identity theft, fraud, loss of confidentiality, physical or emotional harm. • Poor processes or inadequate due diligence leading to non-compliance with the GDPR, resulting in financial or reputational damage to the school	Likelihood of harm (remote, possible or probable)	Severity of harm (minimal, significant or severe)	Overall risk (low, medium or high)

Step 6: Identify measures to reduce risk

For risks identified as medium or high, you must identify additional measures you will take to reduce or eliminate the risk				
Risk	Options to reduce or eliminate risk	Effect on risk (eliminated, reduced or accepted)	Residual risk (low, medium or high)	Measure approved (yes or no)

Step 7: Sign off and record outcomes

Item	Name/Date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead.
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or overruled by:		
If overruled, you must explain why?		
Consultation responses reviewed by:		
If your decision is not the same, explain why, and why you have decided to continue with the processing:		
This DPIA will be kept under review by:		
Date:		