The Romero Catholic Academy
Nurturing the Talent of Tomorrow

# Data Protection Policy

| | |
|---|---|
| **Responsible for policy:** | **CC2 Strategy, People and Organisational Development** |
| **Policy status:** | **Compliance** |
| **Policy review:** | **Annually** |
| **Chair of Directors:** | |

## Contents

## Definitions

In this **Data Protection Policy**, unless the context otherwise requires, the following expressions shall have the following meanings:

i **'The Romero Catholic Academy'** means the Company named at the beginning of this **Data Protection Policy** and Procedure and includes all sites upon which the Company is undertaking, from time to time, being carried out. The Romero Catholic Academy includes; **Corpus Christi**, **Good Shepherd**, **Sacred Heart**, **SS Peter and Paul**, **St Gregory**, **St John Fisher**, **St Patrick**, **Cardinal Wiseman**, **Shared Services Team**.

ii **'Romero Catholic Academy'** means the Company responsible for the management of the Academy and, for all purposes, means the employer of staff at the Company.

iii **'Board'** means the board of Directors of the Romero Catholic Academy.

iv **'Chair'** means the Chair of the Board or the Chair of the Local Governing Body of the Academy appointed from time to time, as appropriate.

v **'Governance Professional'** means the Governance professional to the Board or the Governance professional to the Local Governing Body of the Academy appointed from time to time, as appropriate.

vi **Chief Executive Officer'** CEO means the person responsible for performance of all Academies and Staff within the Multi Academy Company and is accountable to the Board of Directors.

vii **'Diocesan Schools Commission'** means the education service provided by the diocese, which may also be known, or referred to, as the Birmingham Diocesan Education Service.

viii **'Local Governing Body"** means the governing body of the School.

ix **'Governing Body Representatives'** means the governors appointed and elected to the Local Governing Body of the School, from time to time.

x **'Principal'** means the substantive Principal, who is the person with overall responsibility for the day-to-day management of the school.

xi **'School'** means the school or college within The Romero Catholic Academy and includes all sites upon which the school undertaking is, from time to time, being carried out.

xii **'Shared Services Team'** means the staff who work in the central team across the Company (e.g. HR/ Finance)

xiii **'Vice-Chair'** means the Vice-Chair of the Governing Body elected from time to time.

xiv **'School DPO'** means the Data Protection Officer responsible for all schools within The Romero Catholic Academy (Warwickshire Legal Services)

xv **'ICO'** means Information Commissioner Office.

xvi **'GDPR'** means General Data Protection Regulation.

xvii **'FOI'** means Freedom of Information Act.

xviii **'SAR'** means Subject Access Request.

## 1. Scope

Romero Catholic Academy is committed to protecting personal data in accordance with UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025. This policy outlines our approach to compliance and safeguarding.

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

This policy applies to all staff, pupils, parents, contractors, and third-party service providers handling personal data on behalf of the Academy.

## 2. Legislation and guidance

We adhere to the seven principles of UK GDPR: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

This policy meets the requirements of the:
UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

Data Protection Act 2018 (DPA 2018)

Data Use and Access Act 2025 (DUAA 2025)

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

It is based on the guidance published by the Information Commissioner Office (ICO) on UK GDPR
It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
It also reflects the ICO's guidance of practice for the use of surveillance cameras and personal information.
In addition, this policy complies with our funding agreement and articles of association.

## 3. Definitions

| Term | **Definition** |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, individual.<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>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:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics |

| | |
|---|---|
| | • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• 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.<br>Processing can be automated or manual. |
| **Criminal Convictions Data** | Personal data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings. |
| **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. |
| **Privacy Notice** | A separate notice setting out information that may be provided to Data Subjects when the organisation collects information about them. |
| **Data Privacy Impact Assessment (DPIA)** | Tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data |

## 4. The data controller

The Romero Catholic Academy processes personal data relating to parents, pupils, staff, governors, volunteers, visitors and others, and therefore is a data controller.

The Romero Catholic Academy is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## 5. Roles and responsibilities

This policy applies to **all staff** employed by The Romero Catholic Academy and to external organisations, volunteers and other individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

### 5.1 Academy Board of Directors

The Academy Board of Directors has overall responsibility for ensuring that The Romero Catholic Academy complies with all relevant data protection obligations.

### 5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for providing advice and guidance to The Romero Catholic Academy in order to assist The Romero Catholic Academy to implement this policy, monitor compliance with data protection law, and develop related policies and guidelines where applicable.

The DPO will carry out an annual audit of The Romero Catholic Academy data processing activities and report to the Academy Board of Directors their advice and recommendations on school data protection issues.

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

Our DPO is the School DPO Service provided by Warwickshire Education Service and is contactable via schooldpo@warwickshire.gov.uk or alternatively;

**School Data Protection Officer**
**Warwickshire Legal Services**
**Warwickshire County Council**
**Shire Hall**
**Market Square**
**Warwick**
**CV34 4RL**

### 5.3 Roles

**The Academy Data Protection Champion and School Data Protection Officers**

The Romero Catholic Academy has nominated the following individuals as designated persons to be contacted internally in relation to all matters relating to data protection issues, and to make referrals, where necessary, to the Data Protection Officer;

- **MAC Academy Data Protection Champion**
  This is Helen Quinn CEO, who is contactable via admin@romeromac.com or 02476 451888
- **School Data Controller/Lead**
  This is usually the principal of the school
- **School Data Protection Officer**
  This is usually someone nominated in the office or administration.

### 5.4 All staff

All members of 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 Data protection Lead 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 GDPR is based on data protection principles that our Academy must comply with.
The Romero Catholic Academy has adopted the principles to underpin its Data Protection Policy:
The principles require that all personal data shall be:

1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
2) used for specified, explicit and legitimate purposes ('purpose limitation');
3) used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');
4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy');
5) kept no longer than is necessary ('storage limitation');
6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

This policy sets out how The Romero Catholic Academy aims to comply with these principles.

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

The Romero Catholic Academy shall only process personal data where it has one of 5 'lawful bases' (legal reasons) available to The Romero Catholic Academy 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 e.g. 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,** and carry out its official functions
- 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 which are set out in the UK GDPR and Data Protection Act 2018.

- 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.

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 guidance set out in the Information and Records Management Society's toolkit for schools.

## 8. Sharing personal data

We will not normally share personal data with anyone else except as set out in The Romero Catholic Academy's Privacy Notice. GDPR and the DPA 2018 also allow information to be shared where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a 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 internationally, we will do so in accordance with data protection law. Transfers outside the UK must comply with UK adequacy regulations and International Data Transfer Agreements (IDTAs). EU SCCs are no longer sufficient under UK law.

## 9. Subject access requests and other rights of individuals

### 9.1 Subject access requests

Under DUAA 2025, schools may 'stop the clock' while awaiting clarification from the requester. Searches must be reasonable and proportionate. Clarification timelines should be documented, and pupils with sufficient maturity may submit SARs without parental consent. Algorithmic Impact Assessments are required for high-risk AI use. Automated decisions must include plain-language explanations and human oversight to prevent profiling without review.

Individuals have a right to make a ‘subject access request’ to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period
- 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. Transfers outside the UK must comply with UK adequacy regulations and International Data Transfer Agreements (IDTAs). EU SCCs are no longer sufficient under UK law.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing. Requests relating to staff should be sent hr@romeromac.com. Requests relating to a student should be directed to the principal.

And include the following:

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

The DPO will send the subject access request to the Data Protection Lead or officer. If staff receive a subject access request, they must immediately forward it to the Schools Data Protection Lead or officer who will ensure that the DPO is informed.

**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 person should have parental responsibility for the child, and the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 13+ can exercise data rights independently. Digital consent for online services must comply with UK age threshold (13 years).

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parent or carers of the pupil at our school aged 13 and above may not be granted without the express permission of the pupil.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parent or carers of pupils at our school [aged under 13] will in general be granted without requiring the express permission of the pupil.

These are not fixed rules and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

**9.3 Responding to subject access requests**

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- 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 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
- 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 considers 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. 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 9.3), 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, where processing is based on the consent of the pupil or parent
- 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
- Object to processing which has been justified on the basis of public task, 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)
- Subject to the complaints procedure set out in section 14 of this policy, you have the right to complain to the ICO.

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 School Data Protection Lead who will send it to the DPO for information purposes.

## 10. 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 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 Romero Catholic Academy 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 Romero Catholic Academy'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 via Arbor parent app at each transaction 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.

## 11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We also use video and audio data for training and professional development purposes. We will adhere to the ICO's guidance for the use of CCTV Including ICO guidance on AI-enabled CCTV and facial recognition. DPIAs are mandatory for any AI-based surveillance systems. 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.

Our lawful basis for using CCTV is legitimate interest and public task. We use surveillance cameras for the safety and security of the school and its staff, students and visitors. 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 and how you can contact us if you have any queries relating to the use of CCTV on our premises.

Our cameras information is available on our CCTV Policy.

We have undertaken a data protection impact assessment in relation to our CCTV system to comply with our legal obligations. Our assessment is reviewed every year.

Only authorised staff are permitted to access the system. Any enquiries about the CCTV system should be directed to the authorised staff on site please see CCTV policy

Any enquiries about the CCTV system should be directed to Helen Quinn, CEO, Academy Data Protection Champion.

## 12. Photographs and videos

As part of our school activities, The Romero Catholic Academy may take photographs and record images of individuals within the School.

The Romero Catholic Academy will obtain 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 (or pupils where appropriate) have agreed to this.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.

- Outside of school by external agencies such as the school photographer, newspapers, local radio, campaigns
- Online on our school 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 unless we have consent not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our school application packs for more information on our use of photographs and videos.

## 13. Inventry Ltd

As part of our security and safeguarding procedures the schools are installed with visitor management software called Inventry Ltd. It is a fully equipped integrated solution which allows the schools to accurately monitor who is in school at any one time. Inventry speeds up the sign in process, identity information is kept secure, and it keeps our pupils and staff safe.

All visitors are asked to sign in using Inventry and this will ask for a full name and take a photograph of the visitor. The visitor will wear the badge for the duration of the time spent in the school to ensure visitors are visible to all pupils and members of staff.

The system will also take a photograph of persons signing pupils in or out of the school, outside of standardised hours. A prominent sign in each school main reception explains this is in place for safeguarding purposes.

Please refer to Inventry GDPR policies and FAQs for further information https://inventry.co.uk/gdpr-policies/

## 14. Data Protection Complaints

We are committed to handling your personal data in a way that is fair, transparent, and in accordance with the law. If you are unhappy with how we have handled your data, this process outlines how you can make a complaint.

**How to Make a Complaint**

If you have a complaint about how your personal data has been handled, please provide as much detail as possible. This will help ensure your concern is fully understood and investigated appropriately.

**Stage 1 – School Level**

All data protection complaints must first be handled by the individual school.

You should contact the **school's Data Protection Lead (DPL) or Data Protection Officer (DPO)**. They will:

- Acknowledge receipt of your complaint **within 5 working days**
- Investigate the matter promptly and proportionately
- Keep you informed of progress
- Request further information where necessary
- Provide a **full written response within 20 working days** (or explain if more time is required, up to a maximum of one calendar month)

**Stage 2 – Trust Level**

If you remain unhappy with the outcome at school level, your complaint can be escalated to the **Trust** for further review.

At this stage, the Trust will:

- Review the handling and outcome of the complaint
- Consider whether the appropriate procedures were followed
- Provide **written response within 20 working days**

**Stage 3 – External Review**

If you remain dissatisfied following the Trust review, you may request an independent external review via:

**SchoolsDPO@warwickshire.gov.uk**

At this stage:

- An independent assessment of the complaint and its handling will be undertaken
- A written outcome will provided

**Final Step – Information Commissioner's Office (ICO)**

If you are not satisfied after completing all stages of this process, you have the right to lodge a complaint with the **Information Commissioner's Office (ICO)**.

- Website: https://ico.org.uk

**What to Expect from Us**

At every stage of the process, we will:

- Act without undue delay
- Handle your complaint fairly and transparently
- Keep you informed of progress
- Provide clear explanations and outcomes

## 15. Data protection by design and default

The Romero Catholic Academy shall put measures in place to show that it has integrated data protection into all of its 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)
- Consideration of whether a data protection impact assessment needs to be undertaken. The school will consider this if any of the following kinds of processing plan to be undertaken:
    - Use of systematic and extensive automated processing
    - Large scale processing of data, particularly where it involves special category or criminal offence data

- Systematic monitoring of publicly accessible areas and any other form of surveillance
- Processing of biometric or genetic data
- Transfer of data outside of the European Economic Area
- Profiling, evaluation or scoring
- Automated decision making with legal or significant effects
- Matching or combining datasets
- Processing of data concerning vulnerable data subjects
- Implementation of new technology or solutions
- If processing would prevent a data subject from exercising a right or using a service or contract

On reviewing these criteria, if the school finds that the processing personal data presents a high risk to the rights and freedoms of individuals we will undertake a data protection impact assessment.

- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- 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, 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. Data security and storage of records

The Romero Catholic Academy 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
- Staff must ensure passwords are hard for anyone else to guess by incorporating numbers and mixed case into it.
- Encryption software is used to protect all portable devices and removable media on which personal information is stored, 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 the Information Security 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)

## 17. Use of AI and Digital Tools

Any use of AI tools must comply with UK GDPR principles, ensuring transparency, fairness, and safeguarding. DPIAs are mandatory for high-risk processing involving AI.

Algorithmic Impact Assessments are required for high-risk AI use. Automated decisions must include plain-language explanations and human oversight to prevent profiling without review.

## 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, The Romero Catholic Academy 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.

## 19. Personal data breaches

The Romero Catholic Academy shall take all reasonable steps 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, The Romero Catholic Academy shall 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

## 20. Training

All staff and governors are provided with data protection training as part of their induction process and annually via national college.

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

## 21. Links with other policies

This data protection policy is linked to our:

- Information Security Policy
- HR – Disciplinary Policy
- Freedom of Information Policy
- CCTV Policy
- Romero Privacy Notices

- Any other individual school policies linked to information security and E-Safety

## 22. Monitoring and Review

This policy is reviewed annually by the Romero Data Protection Officer, and approved by CC2
The Board of Directors delegate the implementation of this policy to the Academy Committee.

## Appendix 1: Personal Data Breach Procedures

**For Staff**

**1. Identify and Report Immediately**

- If you suspect or discover a data breach (e.g., lost documents, unauthorized access, cyber-attack), **report it immediately**.
- **Timeframe:** Report to the Data Protection Officer (DPO) within **24 hours**.

**2. Complete Required Forms**

- **Incident Reporting Form**

**3. Contain and Mitigate**

- Take immediate steps to **secure data**:
    - Recover lost data if possible.
    - Stop unauthorized access.
    - Delete or restrict compromised data.

**Your Data protection Officer will**

- **Check Incident Reporting Form**
- **Complete Required Forms**
    - **Risk Assessment Form** (includes details like nature of breach, root cause, sensitive data involved, and mitigation steps).
    - **School Incident Log** (update after reporting).

**Check which steps have been taken to Contain and Mitigate**

- Take immediate steps to **secure data**:
    - Recover lost data if possible.
    - Stop unauthorized access.
    - Delete or restrict compromised data.

**Assess the Risk**

- Use the Risk Assessment Form to evaluate:
    - **Type of breach:** Confidentiality, Integrity, Availability.
    - **Root cause:** Human error, system malfunction, cyber-attack, lost/stolen equipment.
    - **Impact:** Sensitive data involved? Risk of identity fraud? Vulnerable individuals affected?
    - **Severity:** Low / Medium / High.

**Notify if Required**

- **ICO Reporting:** Complete the ICO self-assessment tool here.
- If ICO reporting is needed, it must be done **within 72 hours**.
- Notify affected individuals if there is a high risk to their rights and freedoms.

**Record and Follow Up**

- Update the **school incident log** and DPO records.
- Document:
    - Actions taken.
    - Risk level.
    - Any notifications (ICO, individuals, police).
- Schedule follow-up actions and additional staff training if required.