The Romero Catholic Academy
Nurturing the Talent of Tomorrow

Information Security Policy

Responsible for policy:	**CC2: Strategy, People and Organisational Development**
Policy Status:	**Compliance**
Policy Review:	**Annually**
Chair of Directors	

Contents

Definitions

In this **Information Security 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 **Information Security Policy** 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 Term**.

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 or 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 Local 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 Local 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)

1. Introduction

This policy reflects current UK data protection and cyber-security legislation, including the UK GDPR as amended by the Data (Use and Access) Act 2025, the Data Protection and Digital Information Act 2025, and current reforms under the forthcoming Cyber Security and Resilience Bill (2026).

This Policy applies to:

- All members of staff, directors and local Governing Body representatives; “Staff” includes all employees, locum staff, volunteers, work experience and any other individuals working for The Romero Catholic Academy on a contractual basis.

The Importance of this Policy:

- This information Security Policy lets you know what your Information Security responsibilities are at The Romero Catholic Academy everyone has a role to play and it’s vital you understand yours.

The Objective of this Policy is to:

- Inform staff, directors and Local Governing Body representatives and protect The Romero Catholic Academy from security issues that might have an adverse impact on our organisation. Achieving this objective will rely on all staff, directors and Local Governing Body representatives of The Romero Catholic Academy complying with this policy.

2. Key Principles

The Romero Catholic Academy has adopted the following six principles to underpin its Information Security Policy:

These principles operate in conjunction with new lawful bases and compliance mechanisms introduced by the Data Protection and Digital Information Act 2025.

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').

3. Creating, storing and managing information

The Romero Catholic Academy has adopted both a Clear Desk and Clear Screen Policy to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when work areas and computers are unattended.

The purpose of this section is to establish The Romero Catholic Academy's requirements to ensure that information is not disclosed by being made available in any form to unauthorised individuals.

3.1 Paper information

Keep clear desks as this is an obvious way of preventing any confidentiality problems arising from having pupils or other staff members at desks, or disclosure when desks are left unattended. A clear desk will help to protect against the disclosure of information.

- Confidential documents must not be left on display or unsupervised.
- Store confidential information in locked cabinets or a locked office, returning them to these cabinets when not required.
- Take measures to prevent accidental damage to important documents, for example, through the spillage of liquids.
- Do not leave paper by printers or photocopiers where other people may take it or read it accidentally.
- Spoiled photocopies and prints may still be confidential. Do not put them straight into the wastepaper bin, dispose of them as confidential waste. Always check that originals have been removed from the device as well as copies.
- Dispose of confidential paper by shredding or put in a confidential waste bag and follow confidential waste disposal procedure. Do not dispose of confidential waste in a wastepaper bin or anywhere else.
- Destroying information earlier than necessary may be a breach of the law so it is important that retention periods are checked before destroying any records.

3.2 Electronic information

Any cloud, IT, or managed service provider must meet enhanced security obligations in line with the Cyber Security and Resilience Bill (2026), including stricter incident reporting and supply chain security duties.

- All confidential information must be stored on The Romero Catholic Academy's approved electronic devices or systems with access controlled/restricted, e.g. The Romero Catholic Academy' network(s), with appropriate restricted access, The Romero Catholic Academy approved systems.
- Confidential information must be stored as directed by the Romero Catholic Academy.
- No portable devices are to be used unless authorised by the Romero Catholic Academy. Portable devices should only be used as a "last case resort" and where possible the Romero Catholic Academy supplied cloud storage should be used.
- PC screens/laptops/tablets must be sited away from public areas so that pupils and visitors cannot read the screens, e.g., through windows or while waiting in public areas.
- Notebook PCs, handhelds or any other portable ICT device must not be left unattended in any public area (see Mobile Computing below).
- Individual user id/passwords must not be shared with anyone, including other staff members and governors, and do not use anyone else's password. You as an individual are responsible for all transactions undertaken on The Romero Catholic Academy network(s) using your network id.

- Passwords must not be written down and left with any equipment or accessible by anyone else.
- Make passwords hard for anyone else to guess by incorporating numbers and mixed case into it. Some systems will force this already. The Romero Catholic Academy will be introducing a password strength checker which must be used when setting passwords.
- Lock screens whenever leaving any ICT equipment unattended. This will prevent anyone accessing any restricted information on the equipment while it is unattended.
- If you find you have access to confidential information that you believe should be restricted, you should notify The Romero Catholic Academy immediately.
- All devices accessing personal data must use encryption and meet DfE Cyber Security Standards (updated February 2026)

4. Receiving, sending and sharing information

4.1 Post – receiving and sending

- Post should be opened and dealt with away from public areas and securely, if dealing with confidential information. Do not leave unsealed confidential documents in open post trays and 'pigeon holes'.
- Staff must ensure that any mail to an individual marked: Private, Confidential or Personal, or any combination, is only passed to the named recipient unless a prior delegation arrangement has been made.
- If outgoing post contains confidential information to an individual, the envelope should be marked as 'Private and confidential' and 'to be opened by addressee only'. A return address must be shown on the envelope and you should consider double bagging the package.
- Print each letter separately making use of any printing security and use window envelopes. Check the address is the current, correct one – don't copy previous letters. Double check that the letter and papers are for the correct recipient and address.
- When using a mailshot or multiple mailings, have a procedure in place to check you haven't included anyone else's personal information in the wrong envelope. Another person or supervisor should check mailings against address lists and sign-off before dispatch.
- Consider using signed for/tracked post, if it contains sensitive or confidential documents and/or the volume justifies secure delivery.
- Post containing very high risk/Confidential-Restricted information should only be sent to a named person and use of tracked and signed for mail or a courier to deliver to the name person with signature of receipt.
- If post goes astray or is issued to the incorrect address, notify your line manager immediately and if the information contains personal or confidential information report using the security incident procedure.

4.2 Email and Other Electronic Communications (e.g. text messages) – receiving and sending

- The Romero Catholic Academy does not have total control over emails received, so staff must be aware of the dangers of opening messages from unknown or untrusted sources. Do not click on links in emails unless you know they are from a trusted source and never provide passwords in response to email requests.
- If you are not the intended recipient, the sender should be informed that the message has not reached its intended destination and has been deleted.
- Check the email address is the correct one – there are staff with similar names and your email contacts will also have external email contacts. Double check that the email is for the correct recipient before sending.

- Check that the "trail of any e-mails that you will be forwarding, does not contain personal data that should not be forwarded to the new recipient(s).
- If sending to a list/group of parents or others, send using 'blind carbon copy' (bcc) so the recipients are not copied into a large list. This especially applies to mailshots. This would ensure confidentiality and to reduce risk of a data breach being reported.
- Confidential and Confidential-Restricted information must not be emailed externally using normal email unless;
    a) you are using an encrypted email service provided by The Romero Catholic Academy, or
    b) the information is encrypted / password protected in an attachment (the password must be confirmed by phone to the recipient and NOT forwarded in a separate e-mail), or
    c) you are sending to an approved The Romero Catholic Academy email address, e.g. a school email address, or
    d) you are sending to an e-mail address which utilises the same Domain

- Records of personal data sent by email or other electronic communications (internal or external) are accessible to the data subject if they request access under the GDPR. If a permanent record is required, they should be saved to the appropriate file and the email removed from the email inbox. Do not use personal email as a permanent filing system for pupil, parent or staff records. When a member of staff leaves or moves to another job, the line manager must go through the Leavers Checklist and save and secure any emails needed to be kept as The Romero Catholic Academy records.
- The Romero Catholic Academy Confidential email must not be forwarded to your own personal email account for private use.

4.3 Telephone calls

- Ensure that you are talking to who you think you are speaking with by verifying their details. It may be appropriate to call them back to verify their credentials.
- If it becomes necessary to leave the phone for any reason, put the caller on hold so that they cannot hear other potentially confidential conversations that may be going on in the office.
- If the call received or being made is of a confidential or sensitive nature, consider who else may be listening to the conversation.
- If a message needs to be taken where possible, please send the message via e-mail. If you need to leave a message on someone's desk, ensure that the message does not in itself contain confidential information.
- Do not leave confidential messages on an answer machine as these can be reviewed by people other than the intended person.
- All external calls are recorded for safety purposes and the greeting message notifies the callers.

4.4 Conversations

Staff should remember that even though they may be on The Romero Catholic Academy premises there may be pupils and visitors around.

- When having a meeting or interview with someone where confidential information will be discussed, ensure that there is sufficient privacy. Check that the room is suitable.
- Confidential information should only be discussed with colleagues who need to know the information in order to carry out their job.
- Always consider your surroundings and the proximity of others who may be able to hear in public places.

4.5 Information sharing/processing

When confidential or personal data is shared with other agencies, for example with local authorities or external providers, then arrangements must be made for that information sharing to be done in a controlled way that meets ethical and legal obligations in one of two ways:

1) If a service is commissioned with an external provider that needs confidential information to operate then the contract must contain clauses that list the commissioned organisation's responsibilities for confidential and personal data, including data protection and security. This must include whether the organisation is processing personal data on behalf of The Romero Catholic Academy or has sole or joint responsibilities for the personal data with The Romero Catholic Academy. All staff involved in such data commissioning/sharing must be aware of the details of any existing information sharing agreements/contractual agreements and the obligations that it places on them.
   All purchases of service/systems that will use personal data must be referred to the Romero Catholic Academy Data Protection Champion Helen Quinn on 02476 451888 or admin@romeromac.com to ascertain whether a Data Protection Privacy Impact Assessment is required.

2) If information has to be shared with another organisation on a regular basis for legal reasons then this should be done under an information sharing agreement that sets out how the sharing will operate and the standards of management that all parties to the agreement must comply with. Such an agreement will define exactly what information will be shared and how, including the method, transmission or communication between agencies or any shared access security arrangements. The aim is to ensure that appropriate arrangements operate in the participant agencies and ensure the continued confidentiality of shared information. If staff are unclear on what basis information is being shared with another agency, whether an information agreement exists and what obligations that might place on them, it should be clarified with their manager.

4.6 Incident reporting timelines

The Cyber Security & Resilience Bill places tighter expectations on prompt reporting.

Cyber-security incidents must be reported promptly in accordance with evolving national requirements, including enhanced incident reporting duties outlined in the Cyber Security and Resilience Bill (2026)

5. Working Away from School

The purpose of this section is to ensure that information assets and information processing facilities, used to access personal and confidential information, are adequately protected with logical, physical and environmental controls. This includes working away from the school, at home and use of own devices to access personal and confidential information. Remote working practices must align with the DfE Digital & Technology Standards (updated February 2026), including stronger Wi-Fi security and reinforced access controls

Work-related information must not be kept permanently at home. Wherever staff are working on, or in possession of, work-related information they are responsible for it, e.g. in school, on the phone, at home, en route to or from school or home, at meetings, conferences, etc. If confidential information is handed out in conferences or meetings, the same person is responsible for collecting it back in at the end, or ensuring it is only in the hands of those authorised to keep it.

- Take only the confidential papers/files with you that you need and keep out of sight in a bag, do not carry around loose or in clear folder.
- Store confidential paper files/records securely in an envelope or bag. Try to use electronic files on an encrypted device or access via secure connection to the network or approved storage location instead.
- Keeping information in cars: lock away paper files and equipment (laptop/notebook) in the boot, do not leave overnight. Take only the equipment/papers/files with you that you need, leave rest locked away.
- Travelling by public transport: make sure you take all information and equipment when leaving. Be aware of conversations on mobile phone about personal and confidential information.
- You may use your own personal devices or a school device for remote working. When using your own device, you must create a separate log in and password to that device that must not be accessed or shared with anyone else.
- Do not write down passwords/pin numbers. You must not use the 'remember me' option to save user and password details on your device when accessing The Romero Catholic Academy system. Make sure these are unticked and sign out/logout after using a system. Do not save login or passwords if asked. Remember any confidential files opened may be downloaded before closing down your device, so delete them from 'downloads'. If files are not accessed directly (e.g. Google drive format files), then all confidential files must be stored and accessed locally via Romero Catholic Academy approved encrypted media.
- Working at home: Store paper and equipment securely after use, as you would your own personal valuables. Don't leave open confidential files on a table. Lock screen on laptop/tablet and close down after use. All confidential information must be safeguarded from access, no matter how unintentional, by anyone who has no need to know such as family and friends. This would be an unauthorised disclosure. Don't leave any Romero Catholic Academy equipment or information in a car overnight at home, bring into the house and secure. Do not dispose any confidential information at home, bring back into an office for confidential waste disposal. Use strong security on any external Wi-Fi connection.

6. Premises security

- All staff must have their ID badge available for inspection whilst on school premises and report losses or thefts immediately to their line manager.
- Make sure that all visitors sign in and out at all times and disclose who they are coming to see. Visitors should be supervised at all times and display a visitor/contractor ID badge unless authorised by way of a clear DBS check.
- Staff should be encouraged to challenge anyone in the school if they do not know who they are, e.g. if they are not accompanied by a member of staff or they are not wearing an ID badge.
- Staff should be aware of anyone they do not know attempting to follow them through a security door and if appropriate be prepared to escort them back to reception if necessary.
- Managers should ensure that all paper-based records and any records held on computers are adequately protected. Risk assessments should identify any potential threats and an appropriate risk management strategy should be produced
- Parents and others who do not want to discuss their private matters with a receptionist in a public area should be offered the opportunity to be seen elsewhere.

Physical security supports cyber-security resilience expectations set out under current UK legislation including the Cyber Security & Resilience Bill (2026)

7. Portable Media Devices

The purpose of this section is to establish control requirements for the use of removable media devices within and across The Romero Catholic Academy Portable media devices include but are not limited to USB sticks or memory cards. Use of portable media must comply with the DfE Cyber Security Standards, emphasising encryption, restricted use, and secure disposal

- Connection of non-Romero Catholic Academy -supplied removable media devices to The Romero Catholic Academy computing infrastructure is NOT permitted.
- Staff must not alter or disable any controls applied to any computing device by The Romero Catholic Academy IT Service as part of the deployment of a removable media device.
- Removable media devices must not be used for the primary long-term storage of The Romero Catholic Academy information.
- Passwords applied to encrypted devices must conform to the minimum standard required stated in section 3.2 Electronic Information of this Policy.
- Romero portable media devices must only be used in Romero supplied IT devices with encryption enabled.
- Pupil's/Students portable media devices must NOT be used in Romero supplied IT devices.

8. Anti-Malware

The purpose of this section is to establish requirements, which must be met by all devices within The Romero Catholic Academy's computing infrastructure, to protect the confidentiality, integrity and availability of The Romero Catholic Academy software and information assets from the effects of malware. Anti-malware controls must reflect modern threat levels identified in the NCSC 2025–2026 reports and expanded requirements under the Cyber Security & Resilience Bill

- Unless undertaken by or following instruction from IT support staff, staff must not disable anti-malware software running on, or prevent updates being applied to devices.
- The intentional introduction of viruses The Romero Catholic Academy's computing infrastructure will be regarded as a serious disciplinary matter.
- Only software that has been authorised by The Romero Catholic Academy can be installed upon The Romero Catholic Academy systems.
- Each member of staff is responsible for immediately reporting any abnormal behaviour of The Romero Catholic Academy computing systems to their school Principal who must then report it to the IT Team
- Prior to any encryption, all files must be scanned for and cleaned of viruses before being sent to any third party.

9. Access Control

- Access to information shall be restricted to users who have an authorised need to access the information.
- Users of information will have no more access privileges than necessary to be able to fulfil their role.
- All requests for access to The Romero Catholic Academy computer systems must be via a formal request to your line manager.
- The Romero Catholic Academy reserves the right to revoke access to any or all of its computer systems at any time.
- Users must not circumvent the permissions granted to their accounts in order to gain unauthorised access to information resources. Should access be required to a service for legitimate school reason proper authorisation should be sought before the service is accessed. Romero devices must not be used for personal use.
- Users must not allow anyone else to use their account, or use their computers while logged in with their account.
- Computer screens should be 'locked' or the user logged out before leaving any workstation or device unattended.

Users and systems operating through managed service providers must comply with extended access-control obligations introduced under the Cyber Security & Resilience Bill (2026)

10. Monitoring System Access and Use

The purpose of this section is to establish control requirements for the monitoring and logging of information security related events relating to the use of The Romero Catholic Academy's information and information systems.

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. The Romero Catholic Academy will put in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy.

Any monitoring will be undertaken in accordance with the Human Rights Act and any other applicable law.

Monitoring will take into account enhanced regulatory expectations for auditability and reporting under the evolving NIS regulatory framework

11. Potential breaches of security or confidentiality

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it immediately to their school Principal who must in turn report it to The Romero Data Protection Champion Helen Quinn on admin@romeromac.com or 02476 451888.

For losses of equipment or if you believe your email or the network may be at risk, contact your school Principal immediately who will in turn advise The Romero Data Protection Champion Helen Quinn on admin@romeromac.com 02476 451888.

If equipment or confidential information has been stolen report to the Police and obtain a crime reference number.

Use The Romero Catholic Academy procedure in our Data Protection Policy to report and record incidents.

If you are aware of a potential incident or if you are not sure whether the issue is a security breach, then please report it within 4 hours.

Some incidents may require statutory reporting under the Cyber Security & Resilience Bill (2026), including high-severity cyber events impacting digital services

12. Links to other policies

This Information Security Policy is linked to our;

- Data Protection Policy
- Disciplinary Policy
- E Safety Policy
- Acceptable Use Policy
- Freedom of Information Policy
- TRCA Cyber Incident Response Plan (aligning with national requirements)
- DfE Digital & Technology Standards (updated Feb 2026)

13. Monitoring and Review

The Board of Directors delegate the implementation of this policy to the Local Governing Body.
This policy will be reviewed by CC3 Quality, Provision and Performance Standards.