Achieving together in faith

Holy Cross Catholic MAC

MAC Information Security
2025 - 2028

Responsible for Policy	Chris Connoll
Resources Committee Approval Date	08 October 2025
Posted on Website	10 October 2025
Sent out to Schools	10 October 2025
Date of Policy Review	October 2028 / Significant Change

Document Control:

Version History

Version	Status	Date	Author	Department	Summary of Changes
1.0	Draft	11/2020	J Parry	HCCMAC, Central Team	Creation of document from template
2.0	Draft	12/2020	C Connoll M Newell	HCCMAC, Central Team Bishop Ullathorne	Review of Document for best IT practice
3.0	Draft	02/2021	C Connoll	HCCMAC, Central Team	Final review for submitting to board for approval
3.0	**Approved**	203/2021	BoD		Approved by Board of Directors
4.0	Draft	26/03/2021	C Connoll	HCCMAC, Central Team	Feedback from MAC IT Strategy Group Section 3.3 Screensaver lock times USB devices block Section 9 Updated Screensaver lock times
4.1	**Approved**	26/05/2021		C-BoD	Approved by Chair of the Board of Directors
4.2	Draft	29/06/2021	C Connoll	HCCMAC, Central Team	Added/updated Section 7.1 Section 9.1
4.3	**Approved**	16/10/2024		MAC Resources Committee	**No Change**
4.3	**Approved**	08/10/2025		MAC Resources Committee	**No Change**

Information Security Policy

Contents

Contents

1. Scope 4
2. Key Principles 4
3. Creating, storing and managing information 5
   3.1 Paper information 5
   3.2 Electronic information 6
   3.3 Password security policy 6
4. Receiving, sending and sharing information 6
   4.1 Post – receiving and sending 6
   4.2 Email and Other Electronic Communications (e.g. text messages) – receiving and sending 7
   4.3 Telephone calls 8
   4.4 Conversations 9
   4.5 Information sharing/processing 9
5. Working Away from School 10
6. Premises security 11
7. Portable Media Devices 11
   7.1 Portable Media Devices – Exceptions 12
8. Anti-Malware 13
9. Access Control 13
   9.1 - Access Control – Screen Lock / Screen Saver 13
10. Monitoring System Access and Use 14
11. Potential breaches of security or confidentiality 14

1. Scope

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 Holy Cross Catholic MAC on a contractual basis.

The Importance of this Policy:

- This information Security Policy lets you know what your Information Security responsibilities are at Holy Cross Catholic MAC. 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 Holy Cross Catholic MAC 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 Holy Cross Catholic MAC complying with this policy.

2. Key Principles

Holy Cross Catholic MAC has adopted the following six principles to underpin its Information Security Policy:

All Personal data shall be:

a. processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');

b. used for specified, explicit and legitimate purposes ('purpose limitation');

c. used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');

d. 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');

e. kept no longer than is necessary ('storage limitation');

f. 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

Holy Cross Catholic MAC encourages all staff to adopt clear desk and clear screen practices 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 Holy Cross Catholic MAC's requirements to ensure that information is not disclosed by being made available in any form to unauthorised individuals.

3.1 Paper information

a. 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.

b. Confidential documents must not be left on display or unsupervised.

c. Store confidential information in locked cabinets or a locked office, returning them to these cabinets when not required.

d. Take measures to prevent accidental damage to important documents, for example, through the spillage of liquids.

e. Do not leave paper by printers or photocopiers where other people may take it or read it accidentally.

f. Spoiled photocopies and prints may still be confidential. Do not put them straight into the waste paper bin, dispose of them as confidential waste. Always check that originals have been removed from the device as well as copies.

g. 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 waste paper bin or anywhere else.

h. 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

a. All confidential information must be stored on devices owned by Holy Cross Catholic MAC or it's schools. Systems must have access controls/restricted, e.g. Holy Cross Catholic MAC' network(s), with appropriate restricted access, Holy Cross Catholic MAC approved systems.
b. Confidential information must be stored as directed by Holy Cross Catholic MAC.
c. 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.
d. Laptops, handhelds or any other portable ICT device must not be left unattended in any public area.
e. 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 activity undertaken on Holy Cross Catholic MAC network(s).
f. Lock screens whenever leaving any ICT equipment unattended. This will prevent anyone accessing any restricted information on the equipment while it is unattended.
g. If you find you have access to confidential information that you believe should be restricted, you should notify DPO/Headteacher or Holy Cross Catholic MAC immediately.

3.3 Password security policy

a. Passwords should be changed every 90 days.
b. Staff should where possible receive a 14-day reminder of expiring password.
c. You should not be able to use the last three passwords.
d. Passwords should be eight characters long and include a number and special character.
e. All systems where possible will enforce two factor authentication for staff.
f. Passwords must not be written down and/or left with or on any equipment or accessible by anyone else.

4. Receiving, sending and sharing information

4.1 Post – receiving and sending

a. 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'.

b. 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.

c. 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.

d. 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.

e. When using mail merge 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.

f. Consider using signed for/tracked post, if it contains sensitive or confidential documents and/or the volume justifies secure delivery.

g. 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.

h. 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 to the Headteacher and DPO.

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

a. Holy Cross Catholic MAC 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 usernames and/or passwords in response to email requests.

b. 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.

c. 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.

d. 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).

e. If sending to a list/group of parents or others, send using ‘blind copy’ (bcc) so the recipients are not copied in to a large list. This especially applies to mailshots.

f. Confidential and Confidential-Restricted information must not be emailed externally using normal email unless;

- 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

- you are sending to an approved Holy Cross Catholic MAC email address, e.g. a school email address, or

g. 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 save and secure any emails needed to be kept as Holy Cross Catholic MAC records.

h. Holy Cross Catholic MAC 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 / Voice Mail as these can be reviewed by people other than the intended person.

- All external calls are recorded and kept as per the MAC Retention Policy

4.4 Conversations

- Staff should remember that even though they may be on Holy Cross Catholic MAC premises there may be other staff and visitors around.
- When meeting or interviewing someone and confidential information could 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 role.

- 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:

a. 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 Holy Cross Catholic MAC or has sole or joint responsibilities for the personal data with Holy Cross Catholic MAC. 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.

b. All purchases of service/systems that will use personal data must be referred to the School GDPR Champion to ascertain whether a Data Protection Privacy Impact Assessment is required.

c. 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.

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.

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.

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 Holy Cross Catholic MAC 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 Holy Cross Catholic MAC approved encrypted media.

- Working at home: Store paper and equipment securely after use, as you would your own personal valuables. Don't leave confidential files visible. 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 Holy Cross Catholic MAC equipment or information in a car overnight at home, bring into the house and secure. Don't bin confidential information at home, bring back into an office for confidential waste disposal. Do not use public Wi-Fi or public hotspots. Use strong security on any external Wi-Fi connection.

6. Premises security

- All staff must have their ID badge on display with their given school/MAC lanyard 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.

7. Portable Media Devices

The purpose of this section is to establish control requirements for the use of removable media devices within and across Holy Cross Catholic MAC Portable media devices include, but are not limited to USB sticks or memory cards.

- The use of media storage devices is not permitted in Holy Cross Catholic MAC Schools for all users. This includes USB memory sticks or mass storage devices.

- Staff must not alter or disable any controls applied to any device to allow the use of portable storage devices.

7.1 Portable Media Devices – Exceptions

Where the curriculum allows and there is no other technical solution for not using a USB storage device, an exception could be considered. This exception must be agreed with the MAC Chief Finance and Operating Officer and risk assessed.

IT Technical staff are exempt only when a USB storage device is required to complete a technical task. This exception will be reviewed yearly by the MAC ICT, Communication & Compliance Manager and the MAC Chief Finance and Operating Officer

8. Anti-Malware

The purpose of this section is to establish requirements, which must be met by all devices within Holy Cross Catholic MAC's computing infrastructure, to protect the confidentiality, integrity and availability of Holy Cross Catholic MAC software and information assets from the effects of malware.

- Unless undertaken by or following instruction from IT support staff, staff must not disable antimalware software running on, or prevent updates being applied to devices.
- The intentional introduction of viruses Holy Cross Catholic MAC's computing infrastructure will be regarded as a serious disciplinary matter.
- Only software that has been authorised by Holy Cross Catholic MAC can be installed upon Holy Cross Catholic MAC systems.
- Each member of staff is responsible for immediately reporting any abnormal behaviour of Holy Cross Catholic MAC computing systems to their school Headteacher and IT Provider who must then report it to the Chief Finance and Operating Officer and MAC Strategic IT Lead.

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 Holy Cross Catholic MAC computer systems must be via a formal request to your line manager.
- Holy Cross Catholic MAC 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.
- Users must not allow anyone else to use their account or use their computers while logged in with their account unless it's an authorised MAC IT support provider.

9.1 - Access Control – Screen Lock / Screen Saver

- Computer screens should be 'locked' or the user logged out before leaving any workstation or device unattended.
- Screen savers (lock) should be used, and any inactivity after 10 minutes should result in a device being locked pending unlock with a password.
- Screen savers (lock) for Classrooms should be set for 15 minutes.

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 Holy Cross Catholic MAC's information and information systems.

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. Holy Cross Catholic MAC 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.

11. Potential breaches of security or confidentiality

Protecting data and the security of data is everyone's responsibility. If you suspect any of the following

- losses of equipment or if you believe your email or the network may be at risk.
- You have become aware that information has not been handled according to procedures and there is a data breach or potential security incident.

You must report it immediately to the Headteacher and MAC Chief Finance and Operating Officer. The MAC Chief Finance and Operating Officer with the MAC Data Protection Officer will review and report onto the ICO if needed in line with the GDPR policy.

- **MAC Chief Finance and Operating Officer**
  Martyn.Alcott@hcmac.co.uk - Tel: 02475 186 555

- **MAC Data Protection Officer**
  schooldpo@warwickshire.gov.uk

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

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.

If equipment or confidential information has been stolen from your home or while on your person, report to the Police and obtain a crime reference number.