EMMAUS
CATHOLIC MAC

Information and Cyber Security Policy

Version	1.0
Date created/updated	September 23
Ratified by	Full Board
Date ratified	10.09.23
Date issued	12.09.23
Policy review date	September 2024
Post holder responsible	Chief Finance and Operations Officer

Commitment to Equality:

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

This Information and Cyber Security Policy has been approved and adopted by Emmaus Catholic Multi Academy Company on 10th September 2023 and will be reviewed in September 2024.

Signed by Director of Emmaus Catholic MAC:

Signed by CSEL for Central Team:

Schools to which this policy relates:

Signed by Principal for – Hagley Catholic High School
Signed by Principal for – Our Lady of Fatima Catholic Primary School:
Signed by Principal for – Our Lady & St Hubert's Catholic Primary School:
Signed by Principal for – St Ambrose Catholic Primary School:
Signed by Principal for – St Francis Xavier Catholic Primary School:
Signed by Principal for – St Gregory's Catholic Primary School:
Signed by Principal for – St Joseph's Catholic Primary School
Signed by Principal for – St Mary's Catholic Primary School:
Signed by Principal for – St Philip's Catholic Primary School:
Signed by Principal for – St Wulstan's Catholic Primary School:

Contents

DEFINITIONS

The Company's standard set of definitions is contained at Definition of Terms – please refer to this for the latest definitions.

1. AIMS

1.1 Emmaus Catholic Multi Academy Company (the 'MAC') will ensure the protection of all information assets within the custody of the MAC and its School's.

1.2 High standards of confidentiality, quality and availability of information will be maintained at all times.

1.3 The MAC will demonstrate support for, and commitment to, information and cyber security through the issue and maintenance of an information and cyber security policy within the MAC including the supporting guidance documents which are listed below.

2. PURPOSE

2.1 Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Guidance on e-security is available from the National Education Network. In addition, broader guidance on cyber security including considerations for Directors, Governors and Trustees can be found at Cyber security training for school staff - NCSC.GOV.UK.

2.2 The Dfe recently released the 'Meeting digital and technology standards in schools and colleges' gov.uk 2023 Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) The MAC will ensure we adopt all recommendations set out in the standard and continue to work towards becoming fully complaint.

2.3 Information is a major asset that the MAC has a responsibility and requirement to protect. The secure running of the MAC and MAC School's is dependent on information being held safely and securely.

2.4 Information used by the MAC and MAC School's exists in many forms and this policy includes the protection of information stored electronically, transmitted across networks and printed or written on paper. It also includes any information assets in Cyberspace (The Cloud). UK Cyber Security Strategy 2011 defined Cyberspace as:

"Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but

also the other information systems that support our businesses, infrastructure and services".

2.5 Protecting personal information is a legal requirement under Data Protection Law.

2.6 The MAC must ensure that it can provide appropriate assurances to its pupils, parents and staff about the way that it looks after information ensuring that their privacy is protected, and their personal information is handled professionally.

2.7 Protecting information assets is not simply limited to covering the information (electronic data or paper records) that the school maintains. It also addresses who has access to that information, the processes they follow, and the physical computer equipment used to access them.

2.8 This Information and Cyber Security Policy and associated guidance documents, as listed below, address all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

2.9 The following policy details the basic requirements and responsibilities for the appropriate management of information assets.

3. SCOPE OF POLICY

3.1 This Information and Cyber Security Policy and associated guidance documents, as listed below, apply to all systems, people and school processes that make up the school's information systems. This includes all Directors, Governors, School Staff, Pupils, Parents and Volunteers and agents of the school who have access to Information Systems or information used for school purposes.

4. DEFINITON

4.1 This policy should be applied whenever school information systems or information is used.

4.2 Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically (on site, on a network or in the cloud).
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Speech.

5. RISKS

5.1 The MAC recognises that there are risks associated with users accessing and handling information.

5.2 The MAC is committed to maintaining and improving information security and minimising its exposure to risks. It is the intention of the MAC to use all reasonable, practical and cost effective measures to ensure that:

- Information will be protected against unauthorised access and disclosure.
- The confidentiality of information will be assured.
- The integrity and quality of information will be maintained.
- Authorised staff, when required, will have access to relevant school systems and information.
- Business continuity and disaster recovery plans for all critical activities will be produced, tested and maintained.
- Access to information and information processing facilities by third parties will be strictly controlled with detailed responsibilities written into contract/documented agreements.
- All breaches of information and cyber security, actual and suspected, will be reported and investigated. Corrective action will be taken.
- Information security training will be available to all staff.
- Annual review of Information and Cyber Security Policy and associated guidance documents, as listed below, will be carried out.
- This policy will be reviewed when significant changes, affecting the MAC are introduced.
- An Information Security framework of policies and guidance will be developed and implemented consistent with this policy.
- The school's Information and Cyber Security arrangements will be subject to review by the Senior Information Risk Owner (SIRO) supported by the school's Data Protection Officer

5.3 Non-compliance with this policy could have a significant effect on the efficient operation of the school and may result in financial loss and embarrassment.

6. ROLES AND RESPONSIBILITIES

6.1 It is the responsibility of each member of staff to adhere to this policy, standards and procedures. It is the school's responsibility to ensure the security of their information, ICT assets and data. All members of the school community have a role to play in information and cyber security.

6.2 All staff should report any concerns to the IT Team immediately. If you have mistakenly click on a link in an email please call IT immediately to enable the team to close the system to prevent any further access, where possible.

6.3 Refer to Appendix 1 for information on the role of the Senior Information Risk Owner (SIRO), Data Protection Officer (DPO) and Information Asset Owners (IAO).

6.4 **The Chief Finance and Operations Officer** acts as the MAC Senior Information Risk Owner (SIRO) and is responsible for ensuring all aspects of this policy are communicated to all staff and all staff read, acknowledge, and understand their responsibilities in protecting the MAC systems and data. In the event of a cyber attack the CFOO will report the incident to the relative bodies immediately.

6.5 **The Strategic ICT Lead** is responsible for ensuring all of the standards in the 'meeting digital and technology standards in schools and colleges' are met or working towards with a clear, approved timeline towards full compliance. The Strategic ICT Lead will report any incidents to the CFOO immediately.

6.6 **The Strategic ICT Lead and IT Team** will ensure that the MAC meet the technical requirements of the standard and report back to the Chief Finance and Operations Officer any areas of concern.

7. MEETING DIGITAL AND TECHNOLOGY STANDARDS IN SCHOOLS AND COLLEGES – Cyber standard

7.1 **The Standards (these were accurate as of July 23 however they are updated frequently please refer to the website)** Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

- Protect all devices on every network with a properly configured boundary or software firewall.
- Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date.
- Accounts should only have the access they require to perform their role and should be authenticated to access data and services.
- You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication.
- You should use anti-malware software to protect all devices in the network, including cloud-based networks.
- An administrator should check the security of all applications downloaded onto a network.

- All online devices and software must be licensed for use and should be patched with the latest security updates.
- You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site.
- Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack.
- Serious cyber attacks should be reported.
- You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation.
- Train all staff with access to school IT networks in the basics of cyber security.

7.2 **The importance of meeting the standard**

Security systems are sometimes disabled to make very marginal improvements to user experience. This is an unjustifiable risk calculation in most circumstances.

Attackers scan for and exploit devices where the security features are not enabled. Using the security features that devices already have is the most basic form of cyber security.

Attackers who gain physical access to a network device can exploit a system much more easily, so this should be prevented.

Recording network devices helps schools keep networks up-to-date and speeds up recovery.

Properly configured firewalls prevent many attacks. They also make scanning for suitable hacking targets much harder.

Successful cyber attacks target user accounts with the widest access and highest privileges on a network.

You must limit the numbers and access of network and global administrative accounts.

If you prevent and limit the compromise of these accounts you prevent and limit successful cyber attacks.

Multi-factor authentication only allows access to a service when you present 2 or more different forms of authentication. It reduces the possibility of an attacker compromising an account. This is especially important if an account has access to sensitive or personal data.

In this context, sensitive or personal data is all data that if lost or compromised, would have a serious impact on the establishment, staff or students.

Up-to-date anti-malware and anti-virus software reduces the risk from many forms of cyber attack.

Some applications protect against viruses and general malware, some against one only. You need to protect against both.

Applications can insert malware onto a network or have unintentional security weaknesses. This makes attacks easier to execute against a network.

Users should not download applications. The IT service provider should check them first.

Hackers try to identify and exploit the vulnerability that each new security update addresses. They try to do this before users are able to update their systems. In the last year, several attacks on educational establishments have taken advantage of this.

Unsupported software does not receive security updates and over time it becomes:

- more vulnerable as methods of exploitation are discovered
- less compatible with the security measures integrated into the network operating system

You must not use unlicensed hardware or software.

Unlicensed software may not be a legitimate copy, or it may not be updatable to the latest secure standards.

You must avoid or replace unpatched or unsupported hardware or software, including operating systems. These devices are the most popular targets for successful cyber attacks. If this is not possible, then these devices and software must not be accessible from the internet - so that scanning tools cannot find weaknesses.

A backup is an additional copy of data, held in a different location, in case the original data is lost or damaged. If all copies were held in the same location, they would all be at risk from natural disasters and criminal damage.

Backups of important data are crucial for quick recovery in the event of disaster. The safest way to achieve this is to have a pattern of backing up on a rolling schedule. You should keep these backups off the network when not in use and check them regularly.

Being unprepared for a cyber attack can lead to poor decisions, slow recovery and expensive mistakes.

A good response plan made ahead of time will speed up your response, reduce stress levels and confusion.

Effective response will reduce the material, reputational and safeguarding damage from ransomware attacks.

Cyber attacks are crimes against a school that need to be investigated so perpetrators can be found and counter-measures identified.

A cyber attack is defined as an intentional and unauthorised attempt to access or compromise the data, hardware or software on a computer network or system. An attack could be made by a person outside or inside the school.

This compromise of data might include:

- stealing the data
- copying the data
- tampering with the data
- damaging or disrupting the data, or similar
- unauthorised access

Police investigations may find out if any compromised data has been published or sold and identify the perpetrator.

The most common forms of cyber attack rely on mistakes by staff members to be successful. Avoiding these mistakes prevents the attacks.

Basic cyber security knowledge amongst staff and governors is vital in promoting a more risk aware school culture.

7.3 How to meet the standard (cyber) – Technical Requirements

Protect every device with a correctly configured boundary, or software firewall, or a device that performs the same function.

Change the default administrator password, or disable remote access on each firewall.

Protect access to the firewall's administrative interface with multi-factor authentication (MFA), or a small specified IP-allow list combined with a managed password, or prevent access from the internet entirely.

Keep firewall firmware up to date and check monitoring logs as they can be useful in detecting suspicious activity.

Block inbound unauthenticated connections by default.

Document reasons why particular inbound traffic has been permitted through the firewall.

Review reasons why particular inbound traffic has been permitted through the firewall often, change the rules when access is no longer needed.

Enable a software firewall for devices used on untrusted networks, like public wi-fi. Network devices include routers, switches, access points, servers and similar items.

Record and set up your devices and boot up systems to meet the technical requirements.

Provide a system for recording and reviewing decisions made about network security features.

Keep a register, list, or diagram of all the network devices.

Avoid leaving network devices in unlocked or unattended locations.

Require authentication for users to access sensitive school data or network data.

Remove or disable all unnecessary software according to your organisational need.

Disable any auto-run features that allow file execution.

Set up filtering and monitoring services to work with the network's security features enabled.

Immediately change passwords which have been compromised or suspected of compromise.

Protect against a brute-force attack on all passwords by allowing no more than 10 guesses in 5 minutes, or locking devices after no more than 10 unsuccessful attempts.

If a single staff member controls account access, another senior school staff member or governor should approve that staff member's own account.

There must be a user account creation, approval and removal process. You should make this part of school joining and leaving protocols.

You must control user accounts and access privileges. Including accounts used by third parties, for example, support services or device management.

Only authorised people can have an account which allows them to access, alter, disclose or delete the held personal data. The data owner or controller, or the data protection officer, must identify and authorise these tasks.

Users should have a separate account for routine business, including internet access, if their main account:

- is an administrative account
- enables the execution of software that makes significant system or security changes
- can make changes to the operating system
- can create new accounts
- can change the privileges of existing accounts

Users must be authenticated with unique credentials before they access devices or services. This can include using passwords.

You must enforce password strength at the system level and change default device passwords.

If you use a deny list for automatic blocking of common passwords, use a password with at least 8 characters. If you do not use a deny list, use a password with at least 12 characters or a biometric test. The National Cyber Security Centre recommends using passwords made up of 3 random words. Enforce account lockouts after a number of failed attempts and require service provider or network manager permission to unlock.

You must immediately change any password that has been compromised or suspected of compromise.

You must remove unused accounts. This may include the accounts of users who have left their employment, or accounts that have not been used for a prolonged period of time. This is particularly important for accounts with administrator privileges. You should review this termly.

Unused role privileges must be removed or disabled.

No user’s account should have more access to devices than required to carry out their role.

Use different accounts with specific rights for different purposes or have IT service providers and administrators enable just-in-time access, giving individual users time-limited privileges as required. The National Cyber Security Centre provides detailed guidance on privileged access management.

For younger children or users with special educational needs:

- consider using authentication methods other than passwords
- consider using a separate account accessed by the teacher rather than the student
- segment the network so such accounts cannot reach sensitive data
- consider if the data or service being accessed requires authentication

You should not use global administrator accounts for routine business.

You should only use accounts requiring administrator privileges to complete the tasks that need it.

Where practical, you must enable multi-factor authentication. This should always include cloud services for non-teaching staff. All staff are strongly encouraged to use multi-factor authentication.

Ask users for a second authentication factor when accessing sensitive data. For example, when moving from a lesson plan to financial or personal data.

Multi-factor authentication should include at least 2 of the following:

- passwords constructed in the formats described earlier in standard 3
- a managed device, that may belong to the organisation
- an application on a trusted device

- a device with a trusted network IP address, you should not use this in MFA for accounts with administrator rights or for accessing sensitive data
- a physically separate token
- a known/trusted account, where a second party authenticates another's credentials
- a biometric test

You should use service accounts for running system services and not user accounts.

You must make sure anti-malware software and associated files and databases are kept up to date.

Make sure the anti-malware software:

- is set up to scan files upon access, when downloaded, opened, or accessed from a network folder
- scans web pages as they are accessed
- prevents access to potentially malicious websites, unless risk-assessed, authorised and documented against a specific business requirement

Do not run applications or access data which has been identified as malware. Use the anti-malware software to eliminate the problem.

The IT service provider should approve all code and applications that are deployed and make sure they do not pose a security risk. They should do this in the best way possible given available resources.

Best practice is to maintain a current list of approved applications. Applications with invalid or no digital signatures should not be installed or used.

You could search the internet to check the reputation of the application and the hosting site, or run unknown applications or code within a sandbox environment.

Make sure the network's anti-malware service is scanning all downloaded applications.

All software must be currently licensed.

The licensing of most modern software can be checked through the software itself. Software which successfully updates can be presumed to be licensed. Older software may have to be researched.

You should remove unsupported software. If this is not possible then you must only use the software on parts of the network which prevent all traffic to and from the internet. Support does not have to come from the original manufacturer and can come from third parties as long as this does not invalidate a licence.

Unsupported devices must only access segmented areas of the network which do not grant access to sensitive data.

You must enable automatic updates.

You must complete manual updates to hardware or software, including configuration changes, within 14 days of the release of the patch where the vulnerability is:

- described as high risk or worse
- has a Common Vulnerability Scoring System (CVSSv3) score of 7 or above

The Common Vulnerability Scoring System is the security industry standard for measuring the danger of a vulnerability. The score is a number from 1 to 10 where 10 is the most dangerous. There is a more detailed explanation of CVSSv3 on the NVD website.

When notified by the Department for Education (DfE), patches should be applied within 3 days of notification. This will only be done in instances of dangerous zero-day attacks where institutions are at immediate risk and there is a suitable patch available.

You should have at least 3 backup copies of important data, on at least 2 separate devices. At least 1 of these copies must be off-site (on large sites, these copies should be far enough away to avoid dangers from fire, flood, theft and similar risks).

Remember, you need 3 backup copies, you do not need 3 storage locations or 3 storage devices. For example, 2 backups taken at different times on the same device (as long as they do not overwrite each other) will count as 2 of the 3 backup copies.

You should schedule backups regularly. How often you need to create backups depends on:

- how often the data changes
- how difficult the information would be to replace if the backups failed

At least 1 of the backups must be offline at all times. An offline backup is sometimes known as a cold backup.

A cloud backup is an off-site backup. Cloud data held in separated cloud services are held in separate devices.

If the offline backup is in the cloud, access must be:

- by a secure account identity
- impossible from any device unless an authorised user has logged on in person

Remember, off-site means in an alternative physical or digital location, offline means that is not connected to the network

The number of devices with these access permissions must be kept to an absolute minimum.

A secure account identity is defined as a specified account secured with a username and multi-factor authentication.

A device which cannot access the backup is defined as a device that has no valid credentials.

Where the cloud services allow it, set up the controls to:

- only allow authorised devices to create new or appended backups
- deny connection requests when backup is not in use

Regularly check that the backups work.

All schools and colleges must include a contingency plan for loss of some or all IT systems in their business continuity and disaster recovery plan. This is required by the schools financial value standard.

This plan must include:

- staff responsibilities
- out of hours contacts and procedures

- internal and external reporting and communications plans
- priorities for service restoration
- the minimum operational IT requirements
- where you can find additional help and resources

Keep hard copies of key information in case of total system failure.

Test and review these plans regularly.

Schools and colleges must report cyber attacks to:

- Action Fraud
- DfE

Where applicable schools and colleges must report cyber attacks to ICO.

Academy trusts should incorporate the risk assessment into the risk register.

If you rely upon encryption to protect data, this should be:

- strong encryption
- using encryption systems that are still supported
- with a life appropriate to the sensitivity of the data being stored

The ICO provides advice on how data encryption should be used.

The ICO also provides a template for DPIA.

Additional protection or password protection should meet the technical requirements in the account access standard.

You should limit access to those staff with a specific need. Do this by specific content area, and not blanket permissions.

By achieving all the cyber standards you can meet the additional requirements for:

- confidentiality
- integrity
- availability
- restoration

You should report any suspicious cyber incident the Chief Finance and Operations Officer in the first instance who will then report the incident to Action Fraud on 0300 123 2040 or on the Action Fraud website.

Police investigations may find out if any compromised data has been published or sold and identify the perpetrator.

Staff with access to your IT network must take basic cyber security training every year.

At least one member of the governing body should complete the training.

Remember that the training may change over time with changing cyber threats.

Staff who require access to your IT network must take basic cyber security training every year. The training should be part of the induction training for new staff

- Cyber security training for school staff - NCSC.GOV.UK
- Infographics at the NCSC - NCSC.GOV.UK

This training should focus on:

- phishing
- password security
- social engineering
- the dangers of removable storage media

At least one current governor must complete the same basic cyber security training. These governors should read the NCSC publication School cyber security questions for governors - NCSC.GOV.UK

8. SUPPORTING GUIDANCE

8.1 The National Cyber Security Centre has published guidance on: Public sector - NCSC.GOV.UK

8.2 Reporting fraud and cyber crime | Action Fraud

8.3 These incidents should also be reported to the DfE sector cyber team at Sector.Incidentreporting@education.gov.uk.

8.4 Exercise judgement in reporting. Incidents where any compromise may have taken place or other damage was caused should be reported. But receipt of a phishing email alone, for example, does not require reporting to DfE but can be reported to Action Fraud at report@phishing.gov.uk.

8.5 Where the incident causes long term school closure, the closure of more than 1 school or serious financial damage, you should also Report a Cyber Incident - Report a Cyber Incident - NCSC

8.6 Academy Trust Handbook - Part 6: The regulator and intervention - Guidance - GOV.UK (www.gov.uk)

8.7 Personal data breaches | ICO

8.8 The following guidance documents are directly relevant to this policy.

- Data Protection Policy
- Homeworking Guidance
- Information Asset Registers
- Protective Marking
- Policy Governing the operation of CCTV

Appendix 1.

Role of the Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff within the school who is familiar with information risks and the school's response. The SIRO for Emmaus Catholic Multi Academy Company is the Chief Finance and Operations Officer and can be reached at ahodder@emmausmac.com or 01384 210 542

The SIRO has the following responsibilities:

- own and maintain the Information Security Policy
- establish standards, procedures and provide advice on their implementation.
- act as an advocate for information risk management
- appoint the Information Asset Owners (IAOs)

Additionally, the SIRO will be responsible for ensuring that:

Staff receive appropriate training and guidance to promote the proper use of information and ICT systems. Staff will also be given adequate information on the policies, procedures and facilities to help safeguard the school's information. A record of the training provided to each individual member of staff will be maintained.

Staff are made aware of the value and importance of school information particularly information of a confidential or sensitive nature, and their personal responsibilities for information security.

The associated guidance relating to information security and the use of particular facilities and techniques to protect systems and information, will be disseminated to staff.

The practical aspects of ICT protection are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

There are appropriate controls over access to ICT equipment and systems and their use including defining and recording the requisite level of protection.

They are the official point of contact for ICT or information security issues and as such have responsibility for notifying the Senior Leadership Team, Data Protection Officer and Chair of Governors of any suspected or actual breach occurring within the school.

Role of the Data Protection Officer (DPO)

Article 37 of the UK General Data Protection Regulation (UK GDPR) mandates that schools and academies have a Data Protection Officer (DPO) in place.

The role of the DPO within school is to:

- Advise the school, their data processors and their employees of their responsibilities.
- Monitoring school's compliance with UK GDPR and other data protection legislation and internal policies.
- Advising on data protection impact assessments.
- Monitoring performance.
- Identifying safeguards to apply to mitigate any risks identified.
- Maintain a record of processing activities.
- Maintain records and evidence of the schools compliance with the UK GDPR.
- Conduct audits to ensure compliance and address potential issues (including an annual benchmark audit).

The DPO will also be the contact point for the Information Commissioner's Office (ICO).

The schools Data Protection Officer is:

YourIG Data Protection Officer Service
Dudley MBC, The Council House, Dudley, DY1 1HF

Email: YourIGDPOService@dudley.gov.uk tel: 01384 815607

Role of the Information Asset Owner (IAO)

Once the School has identified its information assets, including personal information and data relating to pupils and staff, for example, assessment records, medical information and special educational needs data, schools should identify an Information Asset Owner (IAO) for each asset or group of assets as appropriate.

The role of an IAO is to understand:

- what information is held and for what purposes.
- how information will be amended or added to over time.
- who has access to the data and why.
- how information is retained and disposed of.

The IAOs within a school is the Business Manager / Business Partner and centrally it is the Strategic ICT Lead.

The IAO is responsible for managing and addressing risks to the information and ensuring that information handling both complies with legal requirements and is used to fully support the delivery of education.

Important information assets will include, but are not limited to, the following:

- Filing cabinets and stores containing paper records e.g. archives
- Computer databases
- Data files and folders

On the introduction of this policy Information Asset Owners may need to conduct a thorough information risk assessment to identify any necessary operational or technological changes that may be required within the school and report back to the SIRO – Chief Finance and Operations Officer and concerns.