OUR LADY OF LOURDES

CATHOLIC MULTI-ACADEMY TRUST

IT Security Policy

Nottingham Diocese Multi Academy Trusts

CATHOLIC SCHOOLS Moving Forward Together

Contents

Date Issued	09/06/2025
Date of Review	08/06/2028
Reviewer	Will Ottewell – Director of IT Audit and Risk Committee OLoL Trust Board
Author	Will Ottewell – Director of IT

Rationale

ICT systems represent a significant investment of Trust/Academy resources and are vital for day to day administration and learning. As such, they must be protected from any form of disruption or loss of service. Moreover, the integrity and confidentiality of these systems must be maintained at a level that is appropriate for our needs.

1 Policy Objectives

1.1. To ensure equipment, data and staff are protected on a cost-effective basis against any action that could adversely affect the school.

1.2. To ensure that all users of ICT systems are aware of and fully comply with, relevant legislation.

1.3. To ensure that ICT security is an integral part of day to day activities and where all members of the school community understand the need for ICT security and their own responsibilities in this respect.

2 Application

2.1. The ICT security policy is intended for all staff who use school ICT systems. Pupils using the Trust's ICT systems or data are covered in by the 'STUDENT COPY: The Use of School Computers' document, which is included below.

2.2. 'ICT' or 'ICT systems' are defined as any electronic device for storing and processing of data and includes any form of computer such as a hand-held device, portable laptop, desktop or server. Devices may be stand-alone or networked.

2.3. 'ICT data' means any information stored and processed by ICT and includes programs, text, pictures and sound.

2.4. 'ICT user' applies to any employee of the school, pupil or other authorised person who uses the Trust's ICT systems and / or data.

2.5. 'System Manager' may refer to Network Managers, IT Network and Support Manager, Senior Technicians, Director of IT, or external 3rd Party ICT Support organisations.

Scheme Of Delegation Under The ICT Security Policy

This ICT Security Policy relies on management and user actions to ensure all its aims are achieved. Consequently, owner, corporate and individual levels of responsibility for ICT security are defined below.

3 Owner

3.1. All software, data and associated documentation produced in connection with the work of the school are the legal property of the Trust. Exceptions to this will be allowed for software and documentation produced by individual teachers for lesson purposes, this includes scheme of work; lesson plans, worksheets or as otherwise when agreed in writing by the Principal or CEO.

3.2. We also use software and data that are the legal property of external organisations, and which are acquired and used under contract or licence.

4 Trust Board and Governing Body

4.1. The Trust Board and Academy Governing Body has ultimate responsibility for ensuring that the Academy complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters. In practice, the day to day responsibility for implementing these legislative requirements rests with the Director of IT and Academy Principals.

5 Director of IT/Principal

5.1. The Director of IT or Principal is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met within the Trust and individual academies respectively and that the Trust's ICT Security Policy, as may be amended from time to time, is adopted and maintained by the Trust/Academy.

5.2. The Principal is also responsible for ensuring that any special ICT security measures relating to the Academy's ICT facilities are applied and documented as an integral part of the policy. In practice, the day to day functions should be delegated to the IT Network and Systems Manager or external ICT Support company, who is appointed at the behest of the Principal, Governors, or Trust.

5.3. Principal is also responsible for ensuring that the requirements of the Data Protection Act 2018 are complied with in each academy.

5.4. The Trust Data Protection Officer is responsible for ensuring the requirements of the Data Protection Act 2018 are complied with at the Trust offices and ensuring that the requirements for registration under this act are met for the Trust.

5.5. Additionally, the Director of IT/Principal is responsible for ensuring that users of ICT systems and data are familiar with the relevant aspects of the policy and to ensure that the appropriate controls are in place for staff to comply with. This includes the use of personal data at home by staff so that the Data Protection Act 2018, together with stipulations of the GDPR are not contravened.

6 Systems Manager

6.1. The System Manager is responsible for the Trust/Academy's ICT equipment, systems and data and will have direct control over these assets and their use, including responsibility for controlling access to these assets and for defining and documenting the requisite level of protection.

6.2. The System Manager may also be directly responsible for IT Technicians, all of whom, must be well versed in the relevant aspects of this security policy and the sensitivity of the data stored on Academy ICT systems. The System Manager must maintain an up to date knowledge of best practice with regards to ICT Security and follow the approved practices as detailed below.

6.3. The System Manager will administer the practical aspects of ICT protection and ensure that various functions are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting access to systems and data.

6.4. In line with these responsibilities, the System Manager will be the official point of contact for ICT security issues and as such, is responsible for notifying the Principal/Director of IT of any

suspected or actual breach of ICT security occurring within the Academy/Trust. The Principal should ensure that details of the suspected or actual breach are recorded and made available to Internal Audit upon request. This is critical with regards to data breaches or issues relating to financial irregularity where formal investigations may take place by external parties.

7 Users

7.1. All users of the Trust's ICT systems and data must comply with the requirements of this ICT Security Policy.

7.2. Users are responsible for notifying the System Manager, Principal or Director of IT of any suspected or actual breach of ICT security.

Legislation

The responsibilities referred to in the previous sections recognise the requirements of current legislation relating to the use of ICT systems, which comprise principally of:

- Data Protection Act 2018
- General Data Protection Regulation (GDPR)

You can view these legislations on the ICO (Information Commissioner's Office) website: ico.org.uk.
Also relevant are:

- Computer Misuse Act 1990.
- Copyright, Designs and Patents Act

It is important that all staff are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

Physical Security

8

8.1. Consideration should be given to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data. The server rooms should be locked when left unattended, support environmental monitoring and be protected by a class C fire extinguisher.

8.2. The System Manager must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

8.3. Care must be taken in the placement of computers, printers and similar devices. Depending upon the sensitivity of the data they store, they should be positioned.

- So they cannot be viewed by unauthorised persons

- So that data retrieval by unauthorised persons is restricted.

- So that environmental damage such as water, heat, dust etc. is minimal.

8.4. Written instructions must inform users to avoid leaving computers logged on or hard copies of sensitive data left when unattended. The same rules apply to official equipment in use at a user's home.

Asset Tracking

9

9.1. The System Manager, in accordance with the Academy's financial regulations, shall ensure that an inventory of all ICT equipment is maintained, and all items accounted for at least annually.

Systems Security

10 Facilities

10.1. The School's ICT facilities must not be used in any way that breaks the law such as:

- Making, distributing or using unlicensed software or data.
- Making or sending threatening, offensive, or harassing messages.
- Creating, possessing or distributing obscene material.
- Unauthorised private use of the school's computer facilities.

10.2. The Trust's ICT systems will automatically update software where this is possible. No attempt should be made to delay updates as these may be security critical.

10.3. Software installation and licensing will be reviewed regularly by the System Manager. Software which no longer receives security updates – particularly where a new version has been released – will be removed from the Trust ICT Systems, unless specifically authorised by the Director of IT.

11 Private Hardware & Software

11.1. Unlicensed or deprecated software is a security risk. Software, therefore, must be acquired from a responsible source and used in accordance with the terms of the licence. The use of all private hardware for school purposes must be approved by the System Manager.

12 ICT Authorisation

12.1. Only persons authorised by the System Manager, can use the Trust's ICT systems. Access to systems must therefore depend on appropriate identification, authentication and authorisation. Authorisation must be sufficient for the task and no more.

Without adequate identification and authentication, it will be difficult to show definitively who has used systems and data. Meanwhile, failure to establish the limits of authorisation will prevent the Trust's use of the Computer Misuse Act.

12.2. Access eligibility will be reviewed continually and amended as appropriate - such as when an employee changes work responsibilities or leaves the employment of the school.

13 Passwords

13.1. Password requirements will be defined by the System Manager based on the value and sensitivity of the data involved, including the use of "time out" where a system is left unused for a defined period. As a minimum, a password should include at least 3 random words. Further guidance of password structure is available through Password policy: updating your approach - NCSC.GOV.UK.

13.2. A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur, such as:

- When a password holder leaves the Trust or is transferred to another post.
- When a password may have become known to a person not entitled to know it.

The need to change one or more passwords will be determined by the risk of the security breach.

13.3. A user must not reveal their password to anyone, apart from authorised staff. Users who forget their password must request the System Manager to issue a new password or use a secure automated system approved by the same.

13.4. Passwords should be memorised. If an infrequently used password is written down it should be stored securely or should use a Password Manager solution. Passwords should protect access to all ICT systems.

13.5. Wherever possible individual accounts should be used with external systems, however, where this is not possible (eg an external provider billing platform). Passwords should be stored in a secure manner such as the Trust's Password Manager solution.

13.6. Multi-factor authentication methods should be used on any internet accessible accounts for staff members, contractors and governors. The Trust's Password Manager solution can provide this function or a mobile device can be used for this purpose (Microsoft or Google Authenticator app or SMS). Where multi-factor authentication is not available a more significant length password is recommended, or alternative systems should be sought. The Trust locations may be set as "Trusted Locations" within authentication systems to reduce the complexity of login when on a trusted site.

13.7. The Trust accepts the use of password-less login where this is available and the use of PIN login on devices for tablet devices or for devices which are single user and Trust owned.

14 Backups

14.1. In order to ensure that essential services are restored as quickly as possible following an ICT system failure, backup copies of stored data will be taken at regular intervals as determined by the System Manager, dependent upon the importance and quantity of the data concerned.

14.2. Where programs and data are held on external multiuser system (including the use of personal PCs), checks must be made to ensure that secure copies of data are held.

14.3. Backups should be clearly marked as to what they are and when they were taken. They must be secured safely away from the systems to which they relate and include restricted access.

14.4. Instructions for re-installing data or files from backup should be fully documented and copies should be regularly tested to ensure that they work as anticipated.

14.5. Where externally hosted systems are used such as Finance, HR, Payroll, backup and resilience of these systems will form part of the procurement process for such systems and will be the responsibility of the provider where the Trust does not have access to back end systems and data. Minimum specification will include immutable backup of data separate from production systems, redundancy at network and hardware layers and uptime guarantees.

15 Malware Protection

15.1. The Trust/Academy must use appropriate antivirus software for all ICT systems and conform to recommended malware protection standards.

15.2. The Academy will ensure that every ICT user is aware that any digital device with a suspected or actual malware infection must be disconnected from the network and reported immediately to the System Manager who must take appropriate action, including the removal of any infection.

15.3. Any third-party laptops not normally connected to the school network must be checked by the System Manager for malware before being allowed to connect to the network.

15.4. Teachers must take the necessary steps to ensure that the malware protection on their digital device is updated at least weekly, that scans are conducted regularly and that any file or attachment downloaded is checked.

16 Disposal of Waste

16.1. Prior to the transfer or disposal of any ICT equipment, the System Manager must ensure that any personal data or software is purged from the device if the recipient organisation is not authorised to receive such data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal information to enable the requirements of the Data Protection Act to be met.

16.2. Any ICT equipment must be disposed of in accordance with WEEE regulations. The Data Protection Act requires that any personal data held on such a machine be destroyed. Furthermore, any software must be removed lest the school inadvertently distribute unlicensed copies.

16.3. Disposal of ICT hardware or printouts, should be made with due regard to the sensitivity of the information they contain. For example, paper containing Personal Identifiable Information; Personal Health Information, or undisclosed financial information, must be securely shredded.

17 Repair of Equipment

17.1. If a machine, or its permanent storage, is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on external media for subsequent reinstallation, if possible. The Academy/Trust will ensure that third parties are currently registered under the Data Protection Act and therefore bound by the same rules as the Academy/Trust.

Security Incidents

18

18.1. All users of the system must undertake annual training on cyber security to reduce the chance of security incidents. This may be through the Trust training package for staff, Governors and contractors, and may be through curriculum or events such as "Safer Internet Day" for students.

18.2. All suspected or actual breaches of ICT security shall be reported to the System Manager, Principal or Director of IT so that a quick and effective response can be made. Where possible, useable evidence of a security breach should be preserved for the purposes of a formal investigation by internal or external entities.

18.3. If a Cyber Security incident occurs, the Academy/Trust must invoke their Cyber Response Plan, which will involve a response from the Trust Insurance Providers.

19 **Data** Storage

19.1. Cloud or network storage are the preferred methods of storing files and data, such as OneDrive for Business, SharePoint or Google Drive. Cloud storage used for Trust data must be managed by the Systems Manager and not use personal accounts (such as Dropbox, Personal OneDrive).

19.2. USB storage devices should not be used wherever possible. There is an inherent data risk with using portable storage devices of data being lost, damaged or stolen.

19.3. Where there is no other option, with the permission of the Systems Manager, USB storage may be used for transferring data, however, USB devices must be encrypted, their physical security must be ensured and if any personally identifiable data (as defined under GDPR) is to be transferred, this should be removed as soon as the reason for data transfer in this manner has occurred to mitigate the risk of data loss.

19.4. IT personnel may use USB sticks from time to time unencrypted to allow them to update devices and firmware where other solutions are not available. USB sticks used in this manner will be stored securely and access will only be provided to IT personnel.

19.5. The Trust may implement data loss prevention systems to monitor and capture data, especially personal data, being transported outside of Trust controlled systems. However, it is acknowledged that there are ways to capture data that cannot be controlled, and users must not extract personal data from Trust controlled systems.

19.6. Any devices which are likely to be taken offsite or that may store personal data must be encrypted. Where possible, all devices should be encrypted. TPM is a suitable method for securing the device, but additional PIN/passwords may also be used.

Training

20 Staff and Governor Training

20.1. All non-student users of Trust IT systems must undertake Trust provided cyber security training on an annual basis.

20.2. Supplementary training may be provided either where a significant risk is identified or where specific user weaknesses are identified. This training must be completed.

21 Student Training

21.1. Cyber Security and Online Safety will form part of the IT Curriculum within schools, which should cover as a minimum:

- Password Security
- Safe and Responsible Internet Usage
- Phishing and Malware (Secondary)

21.2. Safer Internet Day will be used as a chance for a whole academy focus on Cyber Security and the Trust and academies will promote this within academies and to parents.

Attached Documents

- Student Acceptable Use Policy
- Staff/Governor Acceptable Use Policy

This policy applies to all Trust staff, students and third parties who access school facilities and school related data. Staff members should be issued a copy of this policy together with the 'Staff Acceptable Use Policy'. Usage of ICT systems will be considered agreement with this policy, or a signed copy of the policy will be kept on file.

Students and parent must also sign and return a copy of the 'Student Acceptable Use Policy'.

Appendix 1: KS3 & KS4 acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's IT systems and internet: agreement for pupils and parents/carers

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's IT systems (like computers) and get onto the internet in school I will:

- Always use the school's IT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Connect any device to the school network or equipment without permission
- Attempt to install any software or download any software
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor my activity and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's IT systems and internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's IT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Attempt to install software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school • Use USB storage devices unless approved by the Trust IT Team	
• I will only use the school's IT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. • I agree that the school will monitor the websites I visit and my use of the school's IT facilities and systems including email and file storage. • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy, and acknowledge that any work device is my responsibility whist in transit. • I will let the designated safeguarding lead (DSL) and Trust IT Team know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. • I will always use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too. • I will ensure I undertake assigned Cyber Security training and act accordingly • I will ensure that information on my screen is not viewed by unauthorised people and that my screen is locked whenever my device is left unattended	
Signed (staff member/governor/volunteer/visitor):	**Date:**