OUR LADY OF LOURDES

CATHOLIC MULTI-ACADEMY TRUST

IT Security Policy

May 2020

Contents

Trust Mission Statement

We are a partnership of Catholic schools and our aim is to provide the very best Catholic education for all in our community and so improve life chances through spiritual, academic and social development.

We will achieve this by:

- Placing the life and teachings of Jesus Christ at the centre of all that we do
- Following the example of Our Lady of Lourdes by nurturing everyone so that we can all make the most of our God given talents
- Working together so that we can all achieve our full potential, deepen our faith and know that God loves us
- Being an example of healing, compassion and support for the most vulnerable in our society

Psalm 122:7 ESV

Peace be within your walls and security within your towers

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.

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.

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' documents, 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, ICT 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

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.

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.

Director of IT/Principal

4.2 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.

4.3 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 System Manager' or external ICT Support company, who is appointed at the behest of the Principal, Governors, or Trust.

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

4.6 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.

4.7 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.

Systems Manager

5.1 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.

5.2 The System Manager may also be directly responsible for assistant 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.

5.3 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.

5.4 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.

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

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

Legislation

6.1 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

6.2 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

7.1 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.

7.2 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.

7.3 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.

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

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

Systems Security

Facilities

9.1 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.

9.2 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.

9.3 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.

Private Hardware & Software

10.1 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.

ICT Authorisation

11.1 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.

11.2 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.

Passwords

12.1 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.

12.2 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

12.3 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.

12.4 Passwords should be memorised. If an infrequently used password is written down it should be stored securely. Passwords should protect access to all ICT systems.

Backups

13.1 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.

13.2 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.

13.3 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.

13.4 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.

Malware Protection

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

14.2 The school 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.

14.3 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.

14.4 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.

Disposal of Waste

15.1 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.

15.2 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.

15.2 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.

Repair of Equipment

16. 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

17. 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.

Attached Documents

- Student Acceptable Use Policy
- Staff Acceptable Use Policy
- Security Guidelines

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'.

Date Issued/ Last Reviewed	May 2020
Date of Review	(3 yearly) May 2023
Reviewer	Audit & Risk Committee / Exec Board
Author	Will Ottewell – Director of IT

OUR LADY OF LOURDES

CATHOLIC MULTI-ACADEMY TRUST

Student Acceptable Use Policy

May 2020

The school computer system provides Internet access to students for learning.
This document is designed to protect students and the school by clearly stating what is acceptable and what is not.

- The use of school computers and Internet connection must be for educational purposes only.
- Students must use their own account and must not give their password to any other person.
- Storage media, such as USB drives, CDs, or portable hard drives, must not be brought into school unless permission has been given.
- Students must respect the work of other pupils or teachers who might also store work in common shared areas on the system. Students should only use shared areas of the system when given permission to do so, otherwise they must store files and data in their own secure area. Files in the shared area will be periodically removed.
- Students are responsible for the email they send and for the contacts they make. Email should be written carefully and politely. Emails may be forwarded and therefore are best regarded as public property. Anonymous messages and chain letters must not be sent.
- Students should report any unpleasant material or messages received. The report will be confidential and will help protect others.
- The use of public chat rooms or instant messaging is not allowed.
- The school ICT systems cannot not be used for private business purposes, personal financial gain, gambling, political purposes or advertising.
- No pupil should attempt to undermine the security of school ICT systems, whoever they belong to.
- Copyright and intellectual property rights must be respected.
- Irresponsible use may result in the loss of Internet access or even account suspension.

The school will monitor the use of its computer systems, including websites visited, emails sent and files stored. The school will take action where it believes unauthorised use of the school's computer system is or may be taking place, or when the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

You must accept these rules when you log onto the school network.

Internet & Email

You must:

- Only access websites that are relevant to your school work.
- Respect copyright and trademarks, give credit to anyone whose work you use.
- Check with a member of staff before completing online questionnaires.
- Do not fill out subscription forms unless otherwise stated by a member of staff.
- Ensure that all email messages that you send are not offensive.
- Regularly delete unwanted email messages.

You must not:

- Play or download games from the Internet.
- Download applications from the Internet in any file format.
- Use online chat or web-based email messaging such as Hotmail or Yahoo.
- View offensive content such as pornography, violence, racial or extremist material.
- Use online community websites such as Facebook or Twitter.
- Cyber bully, we have zero tolerance for any such behaviour.
- Use any type of proxy to bypass the network filtering systems.
- Send, access or display offensive messages.
- Send any personal information to anyone, even if you know them.
- Use or send language of an inappropriate nature.
- Open email attachments, even if they are from a reliable source.
- Send messages to group email aliases such as the all student setup.

Printing

You must:

- Only print documents that are relevant to your work.

You must not:

- Print excessive copies of documents unless stated by a member of staff.
- Print entire documents where a single sentence is required.

User Area

You must:

- Only store files in your area that are relevant to your work
- Delete files that are no longer required
- Keep your user area organised and indexed correctly

You must not:

- Store offensive or prohibited content in your area, including executables
- Store songs/videos in any format unless you have permission from staff

Passwords

You must:

- Ensure that your password is a combination of three random words. However, special characters and / or numbers can be added if you wish
- Ensure that only you know your password. If you, for any reason, suspect that this is not the case, you must report the problem to a teacher or the System Manager.

You must not:

- Log onto the network as anyone else but yourself
- Write your password down where it can be viewed by others.

Removable Storage

You must:

- Ask a member of staff before using any type of removable storage

You must not:

- Plug any type of removable media into the computer's USB ports unless told to
- Use the USB ports on any of the computers to charge your USB device

What will happen if these rules are broken?

- Your user account and/or access to the Internet will be disabled.
- If you repeatedly break the rules, then you could be suspended.
- Parents and senior management will be involved with serious breaches of the rules.

The Police will be involved with any criminal related issues.
All computer use is being monitored and records will be kept of inappropriate computer usage.
Please report all breaches in security to a teacher.

Pupil Name:	Form:
Pupil Agreement: I have read and understand the school Student Acceptable Use Policy'. I will use the computer system, email and Internet in a responsible way and obey these rules at all times	
Signed :	Date :

Parent / Carer Name :	
Please tick each box that you agree to: Parent/Carer Consent for Email & Internet Access ☐ I have read and understood 'The Student Acceptable Use Policy' and give permission for my son / daughter to access school computers, email and Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.	
Signed :	Date :

OUR LADY OF LOURDES

CATHOLIC MULTI-ACADEMY TRUST

Staff Acceptable Use Policy

May 2020

Code of Conduct Declaration

1.1 Please read this policy carefully and make sure that you understand it. You then need to sign the declaration/consent form to confirm that you have read, understood and will keep to the policy. You must also understand that we may take action against you if you wilfully break the conditions of the policy

1.2 The school will keep the signed declaration in your personal file. Sometimes, we may ask you to confirm that you still understand and accept the rules.

1.3 Employees logged into a computer shall be considered to be the person using the system or resources provided. Under no circumstances, therefore, should any employee use an account belonging to another person.

Access to School Network, Email and Internet Services

2.1 Your connection to email or the Internet must be authorised by your System Manager. All school Internet access will be via an approved Internet Service Provider (ISP). Any variations to this must be authorised in writing by the Principal/Director of IT.

2.2 The Trust email and Internet facilities are for school/Trust purposes only.

2.3 The Trust has the right to monitor and log the use of ICT facilities, email and Internet and to disclose this information to any relevant authority

2.4 If you intentionally access a computer system or information without proper authorisation, you could be breaking the law under the Computer Misuse Act 1990

Specific Conditions of Use

3.1 You must not use, or try to use, our E-mail and Internet facilities to create, distribute or display in any form, any activity that is or may be considered to be against the law or against our rules and policies. In this context, you are not allowed to use the E-mail and Internet facilities for reasons that are:

- Pornographic or obscene.
- Intimidating, hateful and discriminatory (for example; racist, sexist, homophobic, ageist) or that break our anti-harassment and equal opportunities policies in any other way.
- Defamatory, slander and libel.
- Encouraging extremism, violence, criminal acts or strong feelings.
- Fraudulent.
- Unethical or may give the school a bad name.
- A deliberate harmful attack on systems we use, own or run.
- Sexually explicit messages, images, cartoons, jokes, audio or movie files.

3.2 We will only allow you to do the above if:

- It is part of your job to investigate illegal or unethical activities.
- The Director of IT, Principal or System Manager asks you to in writing.
- It is in the public interest.

If you find or suspect anyone of using the computer system illegally or unethically, you must report it to your System Manager who will advise your Principal, Chair of Governors, CEO, Chair of Trust Board or Internal Auditing parties.

Malware

4.1 It is a crime to deliberately introduce malware, under the Computer Misuse Act 1990. You must not use school/Trust resources to

- Intentionally access or transmit computer viruses or other damaging software.
- Intentionally access or transmit information about, or software designed for, creating malware.

4.2 You must scan any material you receive or download from the Internet to make sure it is malware free. The school will ensure that malware protection exists on any standalone or locally networked computers that can access the Internet and train you in its use. You must not email material that has not been scanned to other users. If you find a virus, or you think the material has one, you must immediately break the connection, stop using the computer and tell the System Manager.

4.3 You must always follow the instructions that your System Manager gives you about malware attacks.

4.4 If you are not sure how to use the malware protection system, you must get advice from the System Manager.

4.5 You must not use or try to use the school facilities for

- Accessing or transmitting information about, or software designed for, breaking through security controls on any system.
- Accessing, without permission, any system, data or email that is not for you, even if it is not protected by security controls. If you are unsure of your network permissions, please consult HR.

Passwords

5 You must not tell anyone your password and follow the advice given by the Systems Manager.

Publishing Information

6 You must get authorisation from the Principal for any school information that is to be published on school web pages or social media. Written permission must also be sought from any individual who will feature in such publications to comply with the Data Protection 2018.

Copyright

7 It is illegal to break copyright protection under the Copyright, Designs and Patents Act 1988. Therefore, you must not knowingly download or transmit any protected information that was produced by another person or organisation without first getting permission from the owner. Nor can you transmit or permit the use of software for which there is no licensed agreement.

Confidential or Sensitive Information

8.1 The confidentiality of sensitive school data such as Personal Identifiable Information, Personal Health Information or undisclosed financial data should always be protected when working remotely. Data should not be transmitted to, downloaded by or stored on personal devices unless:

- Written permission has been sought from the Head of School
- The security of such devices can be controlled and tested by the Systems Manager.

8.2 A footer will be automatically applied to all email communications. Although this disclaimer will be applied, must ensure that you check the address details and information sent via email before sending.

8.3 You should make sure that the Internet is suitable for transmitting information that you feel is confidential, sensitive or legally privileged. If you allow anyone to see this type of information without permission, you may be breaking the law.

8.4 If you are unclear what constitutes sensitive data or the what the constraints of the Data Protection Act 2018 and GDPR 2018, you must seek the advice of the school's data owner and/or Systems Manager.

Recording Internet Use

9.1 You should be aware that your use of email and internet services should have no expectation of privacy in anything you create, store, send or receive using the Trust's ICT system.

9.1 The monitoring of internet and email services are undertaken without prior notification or authorisation from staff

9.2 If you access a prohibited Internet site unintentionally, you must break the connection immediately and report it to your System Manager or Principal. If you do not do this, the school may take action against you.

9.3 You should protect yourself by not allowing unauthorised people to use your school account.

Additional Notes

1	This policy applies to official equipment used at home.
2	You must be aware that any infringement of the legislation below may result in disciplinary, civil and/or criminal action. • GDPR, Data Protection Act 2018 • Computer Misuse Act 1990 • Copyright, Designs and Patents Act 1988 • Communication Act 2003 If you require further information on such legislation, please speak to your line manager.
3	ICT resources are valuable and the confidentiality, integrity, availability and accurate processing of data are of considerable importance to the school. As such all users have a personal responsibility for ICT security. Consequently, you must ensure that you receive appropriate training and documentation in the use of your ICT system and in the protection and disclosure of the data held.
4	Follow the local rules determined by the Director of IT/Principal in relation to the use of private equipment and software. All software must be used strictly in accordance with the terms of its licence and may only be copied if specifically approved by the System Manager.
4	Ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. Do not leave your computer logged on or otherwise accessible to unauthorised users (for example, leaving classroom doors unlocked when not in attendance).
6	You must not exceed any access rights to systems or limitations on the use of data granted to you by the System Manager.
7	Do not divulge your password to any person, or use another person's password, unless specifically authorised to do so by the System Manager, e.g. in cases of shared access. Do not write your password down, unless it is held securely on your person at all times or kept in a locked receptacle/drawer to which only you have access.
8	The System Manager will advise you on what backups you need to make of the data and programs you use and the regularity and security of those backups.
9	Ensure that newly received, CDs, USB drives and emails have been checked for computer malware before use. Any suspected or actual computer malware infection must be reported immediately to the System Manager.
10	Due regard must be given to the sensitivity of the respective information in disposing of ICT printouts, or any electronic devices that stores data.
11	Users must exercise extreme vigilance towards any suspicious event relating to ICT use and immediately report any suspected or actual breach of ICT security to the System Manager or, in exceptional cases, the Principal, Chair of Governors or Internal Audit committee.

Rules and Agreements for Staff

You must read, understand and sign this form if you use school/Trust ICT facilities, services and data. We will keep the completed form in your personal file.

Declaration

I confirm that, as an authorised user of the Trust's ICT facilities, email and Internet services, I have read and understood the 'Acceptable Use Policy' for staff.

Your Details:

Name: _____

Job title: _____

Signature: _____

Date: _____/_____/_____