EMMAUS
CATHOLIC ACADEMY TRUST

DIOCESE OF SALFORD

IT Acceptable Use Policy

October 2025

Humility • Faithfulness • Service

EXISTING POLICY	
POLICY DOCUMENT	IT Acceptable Use Policy
Legislation/Category: Academy Schools	RECOMMENDED
Lead Member of Staff:	Director of Operations
Approved by:	COO
Date of approval:	October 2025
Date of Renewal:	January 2027

EMMAUS CATHOLIC ACADEMY TRUST

The Diocese of Salford provides Catholic Academy Trusts, schools, and colleges for the following reasons:

1. **To assist in the mission of making Christ known to all people;**
2. **To assist parents and carers, who are the prime educators of their children, in the education and religious formation of their children;**
3. **To be of service to the local Church – the Diocese – the Parish and the Christian home;**
4. **To be of service to society.**

Emmaus Catholic Academy Trust Vision:

To provide great Catholic education across Greater Manchester.

Journey with Emmaus CAT…

Contents

1. Policy Statement

Our core purpose is to create a healthy Catholic organisation serving the pupils in our Catholic schools, communities, families, and parishes across Greater Manchester. We are aligned in our mission to work collegially to ensure that we have great schools, strong in faith, serving society. Schools where every pupil has an equal opportunity to thrive and receive the very best Catholic education and formation. Our guiding principles and this Acceptable Use Policy exist to ensure that each Emmaus CAT school has a clear and compelling vision for all of its pupils, focused on creating an inclusive environment, tailored to the needs and abilities of each and every pupil. At Emmaus CAT we will succeed with our philosophy of aligned autonomy, the belief that talent is key and the sharing of curriculum knowledge and academic rigor.

2. Aim of Emmaus CAT Policies

The aim of this, and all Emmaus CAT policies is to support the seven major themes of Catholic Social Teaching, which include;

- The dignity of work and the rights of the worker;
- Solidarity with all people;
- A preferential option for the poor;
- Stewardship and care for creation;
- The call to community and participation;
- The sacredness of life and the dignity of the human person;
- Human rights and the responsibility to protect them;

as well as ensuring that national legislation and guidance are implemented across all our schools. Our policies should not be viewed in isolation, but along with our guiding principles, as integral to all aspects of school improvement. With our policies we aim to create an effective partnership with parents and carers, the prime educators of their children, to ensure that all children reach their potential whist setting high expectations and aspirations, in a positive and supportive environment. All Emmaus CAT policies will clearly define and communicate the core principles which underpin our Catholic culture, mission and vision.

3. Purpose

This policy outlines the obligations on Emmaus CAT staff regarding the acceptable use of Emmaus CAT owned devices and steps to take to ensure compliance. The policy sets out clear guidelines to mitigate any potential for disruption to teaching and learning, from the misuse or attempted misuse of Information Technology (IT) and procedures if a suspected IT incident does occur.

The purpose of this policy is to recognise the need for staff to be able to utilise Emmaus CAT systems for the legitimate purposes for which they are intended and for you to carry out your professional duties.

4. Introduction

Emmaus CAT considers Information Technology (IT) to be a pillar in how high-quality teaching and learning; collaboration and development can be enabled in all our schools.

With this, IT also can present a significant amount of risk to data protection, online safety and safeguarding if there is misuse or best-practice is not appropriately followed.

The policy is underpinned by other Emmaus CAT guidance and policies including:

- Safeguarding
- Social Media Policy

Aligned to the Emmaus CAT digital and IT strategy, Emmaus CAT strive to follow practices from:

The Department for Education (DfE) IT standards in schools and colleges

National Cyber Security Center (NCSC)

Keeping Children Safe in Education (KCSIE)

Cyber Essentials

5. Acceptable Use for staff

Use of Emmaus CAT issued phone and email address

Emmaus CAT provides each member of staff with an email address. All work-related business should be conducted using the email address provided.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

It is forbidden, at all times, to send files through Emmaus CAT central or individual school communication systems that are offensive, extremist, illegal, or in any way inappropriate for an educational setting.

CAT mobile phones must be secured with a PIN code, Face ID or fingerprint. Services such as 'Find my iPhone' should be enabled to assist in locating a lost or stolen device. Please speak to IT Services if you require assistance in enabling this.

Remote access

Remote working and system access is covered by this policy in the same way as access at any Emmaus CAT school or office. All staff are responsible for ensuring that passwords and any devices necessary for remote access are retained securely. Particular care must be taken when accessing systems remotely in a public space or private spaces that are shared areas to ensure that screens cannot be viewed by others.

6. Safeguarding

All staff will follow Keeping Children Safe in Education (KCSIE) guidance and should ensure that they have read the sections on handling incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology, and social media.

It is the responsibility of all staff to support the safeguarding of pupils and colleagues and report any actions or behaviours that are inappropriate or could lead to individuals being placed at risk to the school Designated Safeguarding Lead (DSL).

Staff must not arrange or attempt to create any virtual meetings, lessons or similar online communications without approval of the school. Recordings and screenshots of meetings or lessons must not be taken unless there is a clear purpose, and this is made clear and agreed to by all parties.

There should be no contact with pupils in any way other than school approved and monitored methods.

Use of images

Images of pupils and/or individuals may only be taken, stored and used for professional purposes in accordance with the law. Particular regard must be given to the provision of written consent of the parent, career or individual to the taking, storage and use of the images.

Social media

Members of staff should make sure their use of social media, either for work or personal purposes is appropriate at all times. All staff should understand the importance of upholding their online reputation, professional reputation, and that of the Emmaus CAT and our individual schools and do nothing to impair them.

Further detail can be found in the Emmaus CAT Social Media Policy.

7. Cyber Security

Email Safety

- **Be cautious with unexpected emails**, especially those urging immediate action, requesting personal information, or containing attachments or links.

- **Do not click on suspicious links**. Hover over links to preview the URL before clicking. If in doubt, contact IT Services.
- **Never open attachments** from unknown or untrusted sources.
- **Report phishing attempts** immediately to IT Services. Do not forward suspicious emails to others.

Passwords

Secure and strong passwords are essential to protect the integrity of IT systems. Guidance from the National Cyber Security Centre (NCSC), suggests using three random words as part of your password and passwords should be unique to the system it is used. They should not be duplicated or disclosed to anyone else. Separate passwords for home and work use are also recommended. The 'Three Random Words' approach ensures that passwords are long enough to be secure and easier to remember than a complex string. The (NCSC) advises against passwords that incorporate recurring symbols and numbers. The use of multi-factor authentication (MFA) must be used wherever possible.

Staff must only use their own login and password when logging into IT systems. Passwords must be changed whenever there is a system prompt to do so or where there is a possibility that there could otherwise be a possible compromise of the system. Passwords should be stored in a secure manner and never written down.

It is recommended that you regularly check if your email address has been included in a data breach using the following website: https://haveibeenpwned.com/

Device Security

- **Lock your screen** when leaving your device unattended.
- **Reboot your device when prompted to apply any necessary security updates.**

Only use **school-approved devices** and software for accessing school systems.

Data Protection

Personal data should be kept secure and always used appropriately. All use of personal and confidential data must be in accordance with the Data Protection Act 2018. This applies equally whether in an Emmaus CAT school or office or accessed remotely.

Emmaus CAT central or school level data should not be stored on a personal device or cloud platform. Removeable storage is explicitly not to be used on any IT systems or hardware (USB's, external hard drives, etc.) In instances where visitors are presenting information, material should be digitally sent across beforehand, to verify integrity and mitigate risk.

Incident Reporting

All cyber security incidents including any data breaches or attempted data breaches, or loss of equipment or data should be reported to the Emmaus CAT central or individual school Data Protection Officer immediately.

Cyber Security Essentials

All staff and governors that access Emmaus CAT central and/or individual school systems must complete the NCSC Cyber Security Essentials training on an annual basis. A certificate must be completed and returned to the School Business Manager as evidence that this training has been completed.

Appendix 1 -Compliance and agreement statements

- I will comply with all IT system policies and procedures that are in place, always.
- When I am being assigned a device, I will ensure that I have returned a signed loan agreement form and will comply to the rules of that agreement.
- I will not attempt to install unauthorised software or hardware on any school or CAT device.
- I will not attempt to bypass security controls.
- When working with outside parties, visitors, volunteers and contractors they must have signed and returned the IT Acceptable Use agreement, before any access is provided.
- I will complete any IT training material that is assigned to me.
- I understand that breach of this agreement may lead to appropriate staff disciplinary action or termination of my contract. Where appropriate, there may be a referral to other relevant authorities.
- I understand that my activity when using IT systems may be monitored to effectively safeguard and identify any potential misuse.

I confirm that I have read, understand and agree to abide by [School Name]'s policies, which may include:

- Acceptable Use Policy
- Online Safety Policy
- Social Media Policy
- Data Protection Policy
- Bring Your Own Device Policy (BYOD)
- **Cyber Security Policy**

Signature:_____ Name:_____

Role:_____ Date:_____

I approve this user to be allocated credentials for school systems as relevant to their role.

Signature:_____ Name:_____

Role:_____ Date:_____

Appendix 2 - Acceptable Use agreement for pupils and parents

The school recognises the value of technology in pupil's learning and provides internet access and access to digital technologies to assist in delivering the effective teaching and learning. In return, I agree to the following the rules below to keep everyone safe.

- I will use only my own login and password and I will not share it.
- I will only access the Internet with the permission and supervision of a member of staff.
- I will not access, copy, or delete other people's files.
- I will only use computers and digital devices for schoolwork and homework.
- I will not bring USB drives or other removable storage media into school without permission.
- I will not try to download programmes or apps or upload content to the internet without permission.
- I will only email or message people my teacher has approved, and any messages will be friendly, polite, and sensible.
- I will not copy other people's work and pass it off as my own.
- I will not share my or anyone else's personal information online, including images without permission.
- I will not arrange to meet in person anyone I have only met online.
- To help protect other pupils and myself, I will tell a teacher if there is anything I am unhappy with or if I see a computer warning message.
- I will ask for help if I am not sure what to do.
- I understand that the school can check my accounts, computer files, and the Internet sites I visit.
- I will not download programs, apps, or files to school devices from the Internet.
- I will not print, unless it is related to my work.
- I will take care of the devices and equipment I use, and I will treat them with respect.

Name of child: _____

Signed by _____ (Child)

Parent/Carer

- I have read through the school's IT policy, and I understand school expectations.
- I have read through the Acceptable Use Agreement with my child and explained what is expected of them.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure young people are safe when using the internet and digital technology.
- I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using digital technologies.
- I will encourage my child to seek help and support if they raise concerns about the online world and I will inform school if I have any online safety concerns.
- I understand that my child's activity on school systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

Signed: _____ (Parent/Responsible Adult)