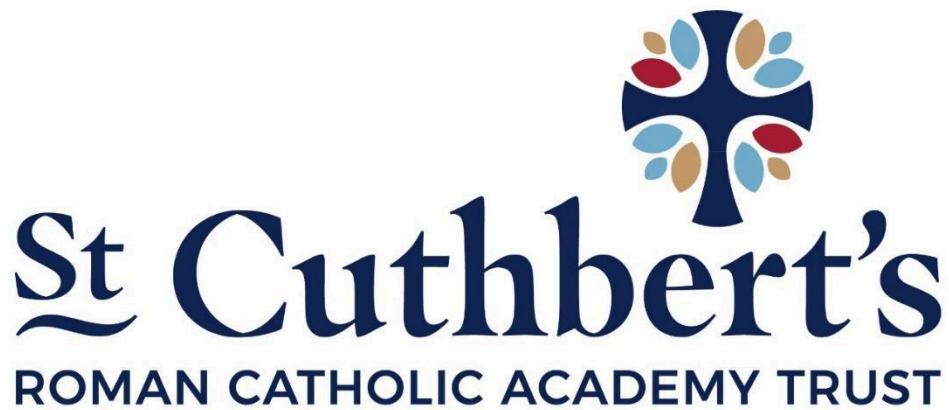




ICT and Internet Acceptable Use Policy (2026-27)

Name and Job Title of Author:	Network Manager and Data Protection Officer
Approval Committee:	Finance, Assets & Audit Committee
Date policy approved:	May 2026
Version number:	v.1
Stakeholders consulted with/comments received:	Yes
Reference Documents:	Statutory Compliance (KCSIE 2025 / Cyber Essentials Certified)
Date of next review:	March 2027

Table of changes

Version Number	Date of Version/Review	Detail changes
V. 1		

1. Introduction and Aims

ICT is an integral part of the way our Academy Trust works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and operational functions of the school.

However, the ICT resources and facilities our Trust uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents and governors in each of our schools.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the Trust's policy on data protection, online safety and safeguarding.
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems.
- Support the Trust in teaching pupils safe and effective internet and ICT use.
- Maintain the technical and behavioural standards required for the Trust's **Cyber Essentials** certification.

This policy covers all users of our Trust schools' ICT facilities and users, including governors, staff, pupils, volunteers, contractors and visitors. Breaches of this policy may be dealt with under our disciplinary policy/behaviour policy or staff code of conduct.

2. Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR).

- Computer Misuse Act 1990 and Human Rights Act 1998.
- **Keeping Children Safe in Education 2025.**
- **DfE Filtering and Monitoring Standards for Schools (2025).**
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- Education Act 2011 and The Education and Inspections Act 2006.
- Freedom of Information Act 2000.
- **NCSC Cyber Essentials Requirements.**
- Searching, screening and confiscation: advice for schools (2022).

3. Definitions

- **“ICT facilities”**: includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.
- **“Users”**: anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
- **“Personal use”**: any use or activity not directly related to the users' employment, study or purpose.
- **“Authorised personnel”**: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.
- **“Materials”**: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

4. Unacceptable Use

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright.
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.

- **Accessing or sharing content related to misinformation, disinformation, or harmful conspiracy theories (KCSIE 2025).**
- **The creation, storage, or distribution of AI-generated indecent imagery (Deepfakes).**
- **Attempting to bypass or disable the Trust's Filtering and Monitoring mechanisms.**
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its pupils, or other members of the school community.
- Connecting any device to the school's ICT network without approval from authorised personnel.
- Setting up any software, applications or web services without approval.
- Gaining, or attempting to gain, access to restricted areas of the network without approval.
- Removing, deleting or disposing of ICT equipment without permission. ● Causing a data breach by accessing, modifying, or sharing data without authorisation.
- Promoting a private business, unless that business is directly related to the school.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's ICT Support Team manages access to facilities. Staff will be provided with unique log-in information and passwords.

- **Multi-Factor Authentication (MFA):** All workforce accounts must use MFA where provided.
- Staff who have access to files they are not authorised to view should contact the ICT Support Team immediately.

5.1.1 Use of phones and email

- The school provides each member of staff with an email address for work purposes only. Staff must not share their personal email addresses or personal phone numbers with parents and pupils.
- All work-related business should be conducted using the school email address.
- Attachments containing sensitive information must be encrypted.
- If staff send an email in error which contains personal information, they must inform the DPO (Sophie Teasdale) immediately and follow the data breach procedure.

5.2 Personal use

Reasonable personal use is permitted provided that it does not take place during contact time, does not constitute 'unacceptable use', and takes place when no pupils are present. Staff may not use the school's ICT facilities to store personal non-work related materials.

5.3 Remote access

Staff accessing materials remotely must abide by the same rules as those on-site. Users must be particularly vigilant against importing viruses or compromising system security when working off-site.

5.4 Monitoring The Trust implements **Active Monitoring** in line with DfE 2025 standards. This includes automated alerts for high-risk activity (radicalisation, self-harm, etc.). Only authorised ICT staff may inspect user activity logs.

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment are available to pupils only under the supervision of staff.
- Specialist equipment must only be used under staff supervision.
- All pupils will be provided with an email account linked to the school's network for educational use.

6.2 Search and deletion

Under the Education Act 2011, the school has the right to search pupils' phones or devices for pornographic images, deepfakes, or any data used to disrupt teaching.

6.3 Unacceptable use of ICT outside of school

The school will sanction pupils if they engage in cyberbullying or activities that disparage the school online, even if the activity occurs off-premises.

7. Parents

Parents do not have access to Trust ICT facilities as a matter of course. Parents are requested to communicate respectfully through official channels and avoid using social media to complain about staff or solve behaviour issues involving other pupils.

8. Data Security and Cyber Essentials

8.1 Passwords

All users must set strong passwords and keep them secure. Disclosing passwords may lead to disciplinary action.

8.2 Technical Safeguards

- **Secure Configuration:** As a Cyber Essentials certified Trust, users are prohibited from altering device security settings, firewalls, or anti-virus configurations.
- **Software Updates:** Devices must be configured to perform security updates automatically.
- **Encryption:** Staff may only use personal USB drives if they are encrypted to Trust standards. Cloud storage (OneDrive/Google Drive) is the primary method for storing data to ensure resilience against ransomware.

9. Internet Access

The Trust wireless connection is secured and filtered to "Education Gold" standards. Users must contact ICT Support immediately if they accidentally access any inappropriate content.

10. Monitoring and Review

The Network Manager and Data Protection Officer monitor the implementation of this policy. It will be reviewed annually and presented to Directors for approval.

Appendix 1: Facebook Checklist for Staff

10 rules for school staff on Facebook:

- 1. Change your display name:** Use a middle name or maiden name to reduce discoverability.
- 2. Change your profile picture:** Ensure your profile picture is professional or unidentifiable.
- 3. Check your privacy settings regularly:** Set visibility to 'Friends only', rather than 'Friends of friends'.
- 4. Be careful about tagging:** Avoid tagging other staff members in personal posts.
- 5. Public vs Private:** Don't share anything publicly that you wouldn't show your pupils.
- 6. Timing:** Don't use social media sites during school hours.
- 7. Discretion:** Don't make comments about your job, colleagues, or pupils online.
- 8. Association:** Don't associate yourself with the school on your profile (e.g. setting as workplace).
- 9. Email Links:** Don't link your work email address to your social media accounts.
- 10. Suggestions:** Consider uninstalling the Facebook app to avoid proximity-based friend suggestions (e.g. suggesting pupils/parents).

What to do if...

- **A pupil adds you:** Ignore and delete the request. Block the pupil. Notify SLT/Headteacher.
- **A parent adds you:** At your discretion, but bear in mind it sets an unwelcome precedent. Drafting a stock refusal response is recommended.
- **You are harassed:** Do not retaliate. Take screenshots. Report to the network and your line manager.

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Name of parent/carers: _____

Name of child: _____

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses official channels including Social Media (Facebook/Twitter/Instagram), Email/Text groups, and the Website. We recognize that parents also use independent unofficial channels (WhatsApp/Facebook groups).

When communicating via official or unofficial channels, I will:

- Be respectful towards members of staff, and the school, at all times.
- Be respectful of other parents/carers and children.
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure.

I will not:

- Use private groups or personal social media to complain about or criticise members of staff.
- Use private groups or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school to speak to the appropriate member of staff.
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers.

Signed: _____ **Date:** _____

Appendix 3: Acceptable use agreement for Secondary Pupils

Name of pupil: _____

When using the school's ICT facilities and internet, I will not:

- Use them for a non-educational purpose or without a teacher present/permission.
- Use them to break school rules or access inappropriate websites.
- Access social networking sites or chat rooms.
- Open attachments or follow links in emails without checking with a teacher.
- Use inappropriate language or share my password with others.
- Bully other people.

I understand that the school monitors the websites I visit and my use of systems. I will tell a teacher immediately if I find anything that upsets me. I understand the school can discipline me for my online actions even if I am not in school when I do them.

Signed (Pupil)_____

Date: _____

Appendix 4: Acceptable use agreement for Primary Pupils

Name of pupil: _____

When I use the school's computers and get on the internet, I will not:

- Use them without asking a teacher first.
- Use them to break school rules or go on inappropriate websites.
- Go on Facebook or social networking sites.
- Open attachments or click links without checking with a teacher.
- Use mean or rude language.
- Share my password or log in using someone else's name.
- Bully other people.

I understand that the school checks the websites I visit to keep me safe. I will tell a teacher immediately if I find anything that upsets me.

Signed (Pupil): _____ **Date:** _____

Appendix 5: Staff, Governors, and Volunteers Agreement^{nt}

Name: _____

When using the school's ICT facilities and internet, I will not:

- Access inappropriate, violent, or criminal material (or share/link to it).
- Use systems in any way which could harm the school's reputation.
- Access social networking sites or chat rooms on work devices.
- Use improper language in any digital communication.
- Install unauthorised software or connect unauthorised hardware to the network.
- Share passwords or log in using someone else's details.
- Share confidential information or access data I am not authorised to see.
- Promote private businesses unrelated to the school.

I will comply with **Cyber Essentials** requirements and use MFA. I will take all reasonable steps to ensure work devices are secure and password-protected outside school. I will report data breaches to the DPO within 24 hours.

Signed: _____ **Date:** _____