'They will soar on wings like eagles …'
Isaiah 40:31

collaborate | enrich | trust | innovate | aspire | nurture

AQUILA Diocese of Canterbury Academies Trust

Multi Academy Trust Policy

Common Trust Policy, Use as Published

ICT Security and Email Policy

Date adopted by Trust Board: October 2024

Date of Review: October 2024

Date of next Review: October 2025

Version	Date	Author	Change Description
1.0	20/12/2024	T.Howard	Agreements and Acknowledgements added Appendices 1-4 added

Contents

1. Introduction and Aims

The Trust recognises that ICT is a critical tool for supporting teaching, learning, and administration. Email and other digital technologies are essential resources but also pose risks related to data protection, online safety, and misuse. This policy outlines how the Trust ensures safe and appropriate use of ICT resources, including email, to protect both individuals and the organisation.

Key Aims:

- Establish clear guidelines on ICT and email usage.
- Protect the Trust from data breaches, legal liabilities, and inappropriate behaviour.
- Ensure the security of personal and sensitive data as per the Data Protection Act 2018 and GDPR.
- Ensure that all members of the school community use ICT resources responsibly, and are aware of the risks involved.

2. Managing and Storing Emails

2.1 **User Responsibility**:
Each user is responsible for managing their own mailbox, ensuring data is stored in line with the **Trust Data Retention Policy**. Emails should be deleted within 12 months unless retained for operational or legal reasons.

2.2 **Storage Compliance**:
Emails containing sensitive or confidential information must be encrypted (Encrypted Email Help) only relevant recipients should be included when sending emails, and email trails should be checked for appropriateness before forwarding. Where emails are used as a record of conversation, a shared mailbox should be used to store them.

2.3 **Email Account Usage**:
All school-related emails must be sent using Trust-issued email accounts. Staff must not use personal email accounts for school business. Passwords must be secure and regularly updated.

2.4 **Email Retention**:
Email accounts of staff members or governors who leave the Trust will be suspended immediately and deleted after six months.

2.5 **Handling Email Errors**:
If you send an email to the wrong recipient, you must notify them and your **Data Protection Officer (DPO)** immediately. All instances of email errors must be recorded in the data breach register.

3. Acceptable Use of ICT

3.1 **Unacceptable Use**:
All users must refrain from:

- Using the Trust's ICT facilities to access or share inappropriate, offensive, or illegal content.
- Engaging in behaviour that breaches intellectual property rights, Trust policies, or legal obligations.
- Sharing confidential information without authorisation.
- Installing unauthorised software or using unauthorised devices on the network.

3.2 **Personal Use**:
Occasional personal use of ICT facilities is permitted provided it does not interfere with job responsibilities or breach policy terms. Personal emails should not be used for school business, and personal data must not be stored on school ICT systems.

4. Data Security and Access

4.1 **Password Protection**:
All users must use strong passwords and should be at least 10 characters long, include upper and lowercase letters, numbers, and symbols. Passwords must be updated every 90 days.

4.2 **Encryption and Data Security**:
Devices accessing Trust data must use up-to-date security measures, including firewalls and antivirus software. Access rights to files, systems, and devices are defined based on role and managed by ICT support.

4.3 **Monitoring**:
The Trust reserves the right to monitor ICT use, including email, internet access, and user activities. Monitoring ensures compliance with policies and detects breaches of security. Email communications may be subject to Freedom of Information and Subject Access Requests.

5. Spotting Spam and Phishing Emails
5.1 **Recognising Phishing**:
Be cautious of:

- Unfamiliar email addresses.
- Impersonal greetings.
- Unexpected attachments or emails.
- Urgent requests for action.

5.2 **Handling Suspicious Emails**:
If you suspect an email is spam or phishing, report it to IT support and the DPO. Do not click any links, enter personal information, or download attachments.

6. Internet Access

6.1 **Pupils**:
Students may only access the internet via school-provided ICT resources and under supervision. Personal devices must not be used to access the internet unless pre-authorised.

6.2 **Parents and Visitors**:
Parents and visitors do not automatically have access to the school's Wi-Fi. In cases where access is granted, they must comply with the school's ICT and security policies.

7. Monitoring and Review

This policy will be monitored by the Head Teacher, ICT support, and the Trust's governance team. It will be reviewed every three years or sooner, if necessary, to remain in line with legislative changes and best practices.

8. Related Policies

This policy should be read in conjunction with the following Trust policies:

- Data Protection Policy
- Freedom of Information Policy
- ICT Acceptable Use Policy
- Online Safety Policy
- Safeguarding and Child Protection Policy

9. Agreements and Acknowledgements

All users of Aquila Trust ICT systems must sign an agreement confirming that they have read, understood, and agree to comply with this Policy.

Appendix 1: Social media cheat sheet for staff

Don't accept friend requests from pupils or relatives of pupils on social media

10 guidelines for school staff on Social Media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the apps from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'** or similar, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A current or former pupil adds you on social media

- Notify the senior leadership team or the headteacher about what's happening
- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages

A parent of a current or former pupil adds you on social media

- Notify the senior leadership team or the headteacher about what's happening
- Check your privacy settings again, and consider changing your display name or profile picture
- Decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so
- Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

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

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Facebook page • Email/text groups for parents (for school announcements and information) • Our virtual learning platform Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, 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, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • 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 younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Share my password with others or log in using someone else's name or password • Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT 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 ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, 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 • Install any unauthorised 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 • 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	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. 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. I will let the designated safeguarding lead (DSL) and ICT manager 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 ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**