'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: November 2024

Date of Review: November 2025

Date of next Review: November 2026

Version	Date	Author	Change Description

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 and ensuring that email data is handled in accordance with the Trust's Data Retention Policy. Routine emails should be deleted within 12 months unless there is a justified operational or legal need to retain them for longer. Records may be archived where this complies with UK GDPR principles, including purpose limitation and storage limitation. However, legal and safeguarding records are exempt from archiving and must be retained for the statutory periods required by law and relevant safeguarding guidance.

2.2 **Storage Compliance**:
Emails containing sensitive or confidential information must be encrypted. Only relevant recipients should be included when sending emails, and email trails should be checked for appropriateness before forwarding.

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 belonging to staff or governors who leave the Trust will be suspended immediately and permanently deleted after six months. The IT provider is responsible for managing the closure of these accounts and implementing any authorised forwarding rules, where applicable.

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 encryption and 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. Recommendation would be adding multi-facotr authentication where feasible.

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. Monitoring will be lawful, proportionate and staff are notified.

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 annually, 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