# Email Protocol and Email Policy

Updated 16th October 2025

| | |
|---|---|
| **Policy reference:** | A38 |
| **This policy is to be reviewed:** | 3 yearly |
| **The next review date is:** | October 2028 |
| **Review is the responsibility of:** | Trust Board |

**Review History**

| | |
|---|---|
| **Review ratified:** | May 2018, May 2021 |
| **Review ratified:** | October 2022 |
| **Review ratified:** | 16th October 2025 |

**Authorised by:** Full Trust Board

| Revisions: | | |
|---|---|---|
| **Date:** | **Page no.** | **Description of changes:** |
| 3/10/2022 | | Complete re-write following up to date requirements |
| October 25 | 6 | 8.6 added |
| | | |
| | | |
| | | |
| | | |
| | | |

# Contents

# 1. Policy Overview

The purpose of this policy is to describe the acceptable use of the Trust's email and related services, systems, and facilities.

The Policy will be made available to users of email and related services and facilities. There will also be 3 yearly review of the Policy and, if necessary, amendment from time to time. This will be necessary with regards to the expected development of the system, the operational use of the system and generally recognised best practice.

Email services are provided by the Trust to support its primary role of education and associated functions related to this role.

# 2. Statement of Authority & scope

This policy is intended to detail the rules of conduct for all members (generally staff and students) of the Trust who use email and related services. This Email Policy applies to the use, for the purpose of sending or receiving email messages and attachments, of any IT facilities, including hardware, software, and networks, provided by the Trust. The Policy is applicable from any location and covers all members of the Trust including staff, students, and other authorised users of Trust IT facilities.

Only authorised users of the Trust computer systems are entitled to use email facilities. All members of the Trust who agree and abide by the Trust regulations, are entitled to use, computing facilities and email systems when the network is available.

The Trust complies with and adheres to all its current legal responsibilities including Data Protection Act 2018, Electronic Communications Act 2000, Regulation of Investigatory Powers Act 2000(RIP), Human Rights Act 1998, Computer Misuse Act 1990, Copyright, and Intellectual Property.

# 3. Statement of Responsibilities

Individual users are responsible for their own actions. The use of email facilities by individuals at the Trust assumes and implies compliance with this policy, without exception. Every user of email systems has a duty to ensure they practice appropriate and proper use and must understand their responsibilities in this regard.

# 4. Acceptable Use

## 4.1 General

The Trust's main purpose in providing IT facilities for email is to support the teaching, learning and approved business activities of the Trust. IT facilities provided by the Trust for emails should not be abused. An absolute definition of abuse is difficult to achieve but certainly includes (but is not limited to):

- creation or transmission of material which brings the Trust into disrepute
- creation or transmission of material that is illegal
- the transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind
- the unauthorised transmission to a third party of confidential material concerning the activities of the Trust
- the transmission of material such that this infringes the copyright of another person, including intellectual property rights
- activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users
- activities that corrupt or destroy other users' data or disrupt the work of other users
- unreasonable or excessive personal use (See 4.2 below)
- creation or transmission of any offensive, obscene or indecent images, data, or other material (other than for reasons specified in 4.3 below)
- creation or transmission of material which is designed or likely to cause annoyance, inconvenience, or anxiety
- creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates, or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs
- creation or transmission of defamatory material or material that includes claims of a deceptive nature
- activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals
- creation or transmission of anonymous messages or deliberately forging messages or email header information, (i.e., without clear identification of the sender) or for 'flaming'
- the unauthorised provision of access to Trust services and facilities by third parties

## 4.2 Personal use

The Trust permits the use of its IT facilities for email by students, staff, and other authorised users for a reasonable level of personal use. An absolute definition of abuse is difficult to achieve but certainly includes (but is not limited to):

- a level of use that is not detrimental to the main purpose for which the facilities are provided
- priority must be given to use of resources for the main purpose for which they are provided
- not being of a commercial or profit-making nature, or for any other form of personal financial gain
- not be of a nature that competes with the Trust in business
- not be connected with any use or application that conflicts with an employee's obligations to the Trust as their employer
- not be against the Trust's rules, regulations, policies, and procedures and in particular this email policy

## 5. Logging

Traffic through the email gateways is logged. Logs include details of the flow of email but not the email content. However, in extreme circumstances when requested by SLT for investigation an eDiscovery can be performed on set criteria which will show the content of emails.

## 6. Spam & junk mail

Spam can be defined as "the mass electronic distribution of unsolicited email to individual email accounts". Junk mail is usually a result of spamming. Spam and junk mail are regarded as interlinked problems. The email gateway will scan for spam and mark appropriately based on its spam score.

## 7. Incident handling & data protection

The Trust will investigate complaints received from both internal and external sources, about any unacceptable use of. It should be noted that logs are only kept for limited periods of time so the prompt reporting of any incidents which require investigation is recommended.

Where there is evidence of an offence it will be investigated in accordance with the Trust's disciplinary procedures applicable to all members of the Trust. That is, accounts may be closed, or email may be blocked to prevent further damage or similar occurring.

## 8. Best Practice & Expectations

### 8.1 Sending emails

Before sending emails consider:

- The maintenance of the highest professional standards
- Whether email is the correct medium for communication
- The content and design, consider level of formality
- To whom should the email be sent, consider expected communication style
- Only copy in people who have an immediate need for the information
- The length of the email, avoid long detailed emails
- Time required for the recipient to respond

**Always read & reflect upon your email before sending**

### 8.2 Receiving and Managing emails

- Staff should become ‘responsible communicators’ i.e., they should check their emails at the start of each day as they currently would their pigeonholes or trays
- Always set time aside to deal with emails
- Consider whether they need you to respond, retain print and/or delete
- If they require retention, place emails and attachments in folders
- If they require response, carefully consider the use of the “reply to all” button
- Delete unwanted emails promptly
- Protect yourself from viruses when emailing from home
- Never open links in emails you are not expecting or do not recognise

## 8.3 Sensitive Information

- Emails are the electronic equivalent of a postcard. Anyone can read the content along the delivery path. Sensitive information should be password protected or via a secure transfer system. Any passwords should be sent in separate emails, so they are not all in the same one
- Child Protection issues should not be reported via email
- Never email in haste, consider the facts and consequences of the message
- Be professional and careful about what you say about others, as email is easily forwarded Only put in writing what you would say to someone's face
- Be aware of copyright and libel issues e.g., when sending scanned text, pictures or information downloaded from the internet
- An email can be contractually binding. Therefore, care should be taken when expressing personal views that these cannot be misinterpreted as belonging to Trust, as the email address will partly contain the Trust name
- If an urgent email is sent, you may want to follow this with a phone call
- Never send emails that are offensive, threatening, defamatory or illegal. Emails have been used successfully as evidence in libel cases

**All confidential emails MUST be sent securely**

## 8.4 Security

- Staff are responsible for the security of their computer, and for protecting any information or data used and/or stored on it.
- Do not to leave a mailbox open and unattended, always keep it password protected. The account holder/s needs to strive to keep their passwords confidential; to prevent other users from accessing and sending emails from their account. If access to an email account is required due to prolonged absence this should be done by delegation which can be requested from IT Services. Passwords should not be shared under any circumstances
- Staff should be responsible for changing passwords on an agreed schedule to maintain security
- Absent staff are aware that their email account may be opened by another member of staff

## 8.5 When to use other methods of communication

- Never discuss performance appraisal or review **issues** by email, always do it face-to-face
- Human Resource issues (salary, job, career progression)
- Private or privileged client materials
- Complex issues should be discussed at meetings
- Topics that require interactive dialogue – or robust discussion on certain issues
- When needing to vent frustration about a workplace situation particularly if you are angry wait to calm

## 8.6 How to spot a Spoofed Email

- Check the Sender's Email Address: Scammers often use misspellings of legitimate domains (e.g., "micros0ft.com" instead of "microsoft.com") or use unfamiliar domains like Gmail or Outlook for official communications.
- Look for Suspicious Language: Be wary of emails with urgent, threatening, or overly alarming tones.

- Inspect Links Carefully: Before clicking, hover your mouse over links to see the actual destination URL. If it looks different from the displayed link, it's a red flag.
- Watch for Requests for Personal Information: Spoofed emails are often a tactic for phishing scams to get your bank details, passwords, or other personal data.
- Check for Grammatical Errors and Poor Formatting: While not always present, unusual language or significant errors can indicate a scam.

## 9. Aspire Learning Trust Email Disclaimer:

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, this message may contain confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute, or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing, or taking any action in reliance on the contents of this information is strictly prohibited.

WARNING: Although the company has taken reasonable precautions to ensure no viruses are present in this email, the company cannot accept responsibility for any loss or damage arising from the use of this email or attachments. The recipient should check this email and any attachments for the presence of viruses.

**Aspire Learning Trust Limited registered address is c/o Sir Harry Smith Community College, Eastrea Road, Peterborough PE7 1XB**