Ascend Learning Trust

E-mail Policy

Policy Owner:	Director of IT
Date of issue:	November 2024
Policy Level:	Tier 1
Approved by:	Full Trust Board
Next Review:	November 2025

Contents

Version Control

Version	Details	Author	Date
1.0	Policy formation	Kyle Gaskin	1st September 2024
2.0	Amendments to wording around Email Management and Storage	Jeremy Masson (following advice from DPE)	1st November 2024
2.1	Amendment to Email Retention to facilitate auto deletion of Emails post 12 months.	Jeremy Masson	20th November 2024

Related Policies

- Ascend Cyber Security Policy
- Ascend Data Protection Policy
- Ascend Online Safety Policy

T 01793 781485 | E info@ascendlearningtrust.org.uk | www.ascendlearningtrust.org.uk
Ascend Learning Trust, The Hive, Clarendon Drive, Royal Wootton Bassett, Wiltshire SN4 8BT
Registered Company No. 07569743

- Ascend Acceptable User Policy
- Ascent Privacy Notice

Introduction

This Ascend Learning Trust Policy applies to Ascend Learning Trust as a whole and to all the schools in the Trust.

It is the responsibility of the Local Governing Body and Headteacher of each school, and the Board of Trustees and CEO for Trust Shared Services, to ensure that everyone adheres to this policy. In implementing the policy and associated procedures the Local Governing Body, Headteacher and Trust staff must take account of any advice given to them by the ALT Trust IT Lead, the ALT CEO and/or Board of Trustees.

This Policy is subject to the Scheme of Delegation approved for Ascend Learning Trust. If there is any ambiguity or conflict then the Scheme of Delegation and any specific Scheme or alteration or restriction to the Scheme approved by the Board of Trustees, takes precedence.

If there is any question or doubt about the interpretation or implementation of this Policy, the ALT Trust Data Protection Lead should be consulted.

Policy Statement

Ascend Learning Trust and its schools understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, can provide pupils with the opportunity for learning through collaboration. Whilst the Trust recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

The Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils, staff, members, Trustees and volunteers.

The Trust is committed to providing a safe learning and teaching environment for all pupils, staff, members, Trustees and volunteers and has implemented controls to reduce any harmful risks.

Email is a universal electronic communication system. Email is about person-to-person communications, but the outcome of an email exchange can have a much wider significance.

For example, a member of staff could inadvertently commit the Trust to an action by an email message; an email can cause illegal material to be transmitted through the Trust's systems for which the Trust may be liable; all emails held at the Trust are legally discoverable following a request under the General Data Protection Regulation (GDPR) or the Freedom of Information Act (FOI) and may be cited as evidence in legal proceedings.

The Data Protection Act 2018 and Freedom of Information Act 2000 has highlighted that it is timely to adopt more formal policies for email retention.

There are key situations where an obligation to retain emails arises: Under Freedom of Information law – The Freedom of Information Act, section 77, contains an offence of altering, defacing, blocking, erasing, destroying, and concealing any records held by a public authority with the intention of preventing the disclosure of records in compliance with a FOI access request or a GDPR access request. Therefore, staff, governors or volunteers must not alter or delete emails after a relevant FOI/SAR has been received.

The Trust, pupils, staff, members, Trustees, and volunteers will retain only personal data that is appropriate for the function of the organisation. This will ensure the Trust meets its Data Protection Act obligations set out in law.

This document sets out the policy that the Trust, pupils, staff, members, Trustees, and volunteers will follow to ensure data is not kept longer than needed, ensuring the Trust meets its legal obligations and endeavours to safeguard business critical information.

Managing and Storing Emails

Email Retention

Mailbox owners are responsible for managing their own mailbox and the data held within. If you have concerns regarding the storage or deletion of an email, please contact your Data Protection Lead for guidance.

Emails must be deleted 12 months after being received unless required for business-critical needs or for other operational purposes. In this situation, necessary emails need to kept in a folder or archived and stored by other means. Please consider the other systems that are in place to store information longer term and whether email ius the most appropriate method of retaining that information. There will be automatic rules created and managed by your IT support department to ensure any e-mail older than 12 months is deleted, this will be communicated to staff; this is to safeguard information and manage the risk of data breaches occurring.

Email content MUST be assessed and stored in line with the Ascend Learning Trust Data Retention Policy.

Deleted emails - Where a “Recycle Bin” is in use, emails held within the Recycle bin will need to be permanently deleted.

Devices used to store emails MUST meet the ICT Security requirements associated with the device type. These devices MUST not be shared in a manner that allows unauthorised access to your school emails.

Composing/Sending an Email

When sending emails only include users that are required and where the content is appropriate for the recipient. Emails must NOT be sent to recipients where the

content is not appropriate or where there is no beneficial need or business requirement.

When composing an email, it is advised that the address book will be used to locate the correct email address for intended recipients, rather than typing an email directly into the address box. Browser cache history will store email addresses that have been previously used, and it is a common data breach amongst organisations where emails have been sent to an incorrect recipient through quickly typing a name into an address box. It is the mailbox owner's responsibility to double check the recipient's email address is accurate before sending.

The trust encourages the use of the email subject line to categorise confidential emails. For example: "Confidential" or "Private/Sensitive" can be included within the email subject line to alert the recipient that the email content contains private or sensitive information.

Where an email contains any confidential, private or sensitive information please consider if an email is the most appropriate method to deliver this information and if so, please use the encryption features built into Microsoft 365 to further protect the information ensuring it only reaches the intended users. If you need assistance or clarification on how to use these encryption features, please speak with your IT support team.

Forwarding Emails

The trust discourages the use of auto-forwarding emails; whilst this can be a useful feature for more infrequent users to avoid logging into email accounts, auto forwarding exposes both the mailbox owner and the trust to sensitive and confidential information leaving the security of trust systems.

When forwarding emails, you MUST ensure that the recipients are correct, and the content is appropriate for the recipient including any historical content contained within the mail.

Replying to an email

Only reply to the original sender do not send replies to the CC address/es – Avoid 'reply to all' unless it is necessary for all recipients to know the content of the email.

Attachments/Sending Documents via Email

The trust discourages the use of email attachments. By linking a document to an email, this increases the risk of a data breach.
Where it is necessary to send additional documents, or information using email, and where it cannot be contained within the body of the text, the following is advised:

1) Send the document with appropriate password protection where the password is then communicated separately to the recipient
2) Send the document via a sharepoint link that expires after a pre-set amount of time.

3) Send the document via a link that means the document does not leave the trusts system – for example, host the document on one drive/teams and share the file with a colleague, setting access permissions accordingly.

Email Etiquette

Use appropriate language in emails. Be aware of your tone and use of capital letters as they can be construed as 'shouting'. Also think about professional language when writing or replying to emails as these can be included into Subject Access Requests.

It is useful to remember that emails can often be misinterpreted; it is advisable to consider the tone of written email correspondence carefully, and where particular sensitivity around the topic may exist, it is worth considering whether a face to face conversation might allow for clearer communication.

Potential Breaches

If you believe you have received an email in error, you MUST contact the sender only immediately to confirm. Under no circumstances should this email be shown or forwarded to any recipient until confirmation has been provided from the original sender. In the event of the email being sent in error the recipient MUST delete the email immediately from all devices and your data protection lead must be notified.

If you believe you have sent an email to an incorrect recipient then you must, if possible, recall the offending email, then contact the appropriate recipient(s) informing them of the error and requesting that it be removed immediately. You MUST also contact your data protection lead and inform them of the error and add to your data protection breach register.

Email account access

The school will give all staff, students & governors their own email account as a work-based tool. The Trustees and Members will be provided email accounts by the central Trust staff. This email account should be the account that is used for all school or Trust business. This is to minimise the risk of non-compliance with the Trust Data Protection policies and associated data breaches.

The following rules will apply:

- Under no circumstances should staff contact students, parents or conduct any school business using any personal email addresses.
- It is the responsibility of each account holder to keep their password/s secure and if they believe their password has been compromised to inform their IT Support lead and Data Protection lead immediately.
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Email accounts of student, staff and governors that have left the Trust will be suspended immediately upon their leaving date and deleted after adhering to the following schedule:

Account Type	Retention Period	Notes/Exceptions
Students	30 days	Year 11 accounts will be retained until the October half term of the ensuing year.
Staff	30 days	Accounts will be retained for 30 days, unless deemed a senior or key member of staff where information may need to be retained longer.
Senior/Key/Exceptional Circumstance Accounts	Maximum 12 months	Accounts should be converted to a shared mailbox upon the leaving date and access given to the most appropriate member of staff for a maximum period of 12 months. Each account should be assessed for how long it is to be retained for example financial members of staff accounts may need to be kept for 12 months for auditing purposes. The Data Protection Lead, Headteacher or designated member of SLT should liaise with their IT support team to define the retention period of these accounts, however it must not exceed a 12-month period.
Governors	30 days	Accounts will be retained for 30 days, unless deemed an exceptional circumstance where information may need to be retained longer.

Spotting spam and phishing emails

The following guidance will help staff, governors and volunteers to spot spam

The sender's address does not tally with the organisation website or is a new/different from previous emails. Look at the email address of the sender not just the name.

The greeting is impersonal. Phishing emails typically use generic salutations such as Dear valued member, Dear account holder, Dear customer or Dear (Surname).

Corporate branding is different from previous genuine emails. Phishing/scam emails often try to copy the format of official emails to trick you in believing they are genuine. It may be difficult at times to distinguish based on appearance alone if an email is fake. However, you can do this by asking:

- Are they using their normal font/size or does this change throughout the email?
- Is it consistent with previous messages I've received from this person/company?
- They contain spelling and grammatical errors. Look for grammatical mistakes mainly.

Window User Alert

Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated it was found out that someone from foreign IP Address was trying to make a prohibited connection on your network which can corrupt you windows licence key.

Sign-details:

Country/region: Lagos,
Nigeria IP Address:
293.09.101.9
Date: 9/07/201602:16AM
(GMT)

If you are not sure this was you, a malicious user might be trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately. 1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ – 1190** in order for technicians to assist you better. Our Microsoft certified technician will provide you the nest resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Our Microsoft certified technician will provide you the nest resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

In the above example, no individual word is spelt incorrectly, but the message is full of grammatical errors that a native speaker wouldn't make, such as "We detected something unusual to use an application". Any supposedly official message that's written this way is almost certainly a scam. That's not to say any email with a mistake in it is a scam. Everyone makes typos from time to time, especially when they're in a hurry.

It's therefore the recipient's responsibility to look at the context of the error and determine whether it's a clue to something more sinister. You can do this by asking:

- Is it a common sign of a typo (like hitting an adjacent key)?
- Is it a mistake a native speaker shouldn't make (grammatical incoherence, words used in the wrong context)?
- Is this email a template, which should have been crafted and copy-edited?

- Is it consistent with previous messages I've received from this person?

If you weren't expecting an attachment or email from the sender this may be a sign of scam/phishing email. A good example of this would be an email informing you that you have won the lottery, and you didn't even enter the lottery.

Trying to rush you into performing an action. Often phishing/scam emails will cause stress and panic by introducing a sense of urgency often use phrases such as your account will be disabled, security breach, needs prompt action, act now or action required.

What should you do if you receive a suspicious email:

- Delete the email and report it to your IT support team and if required your Data protection lead. If you are unsure do not act and take advice as soon as possible from your IT support team
- DO NOT click any links contained within the email
- DO NOT enter your username, password or any other personal data
- DO NOT open or download any accompanying attachments
- DO NOT forward

Email Disclaimer Text

This needs to be on the bottom of all emails and it should be set automatically by your IT Department.

Confidentiality Notice:

"The contents of this message do not necessarily represent the opinions, views, policy or procedures of Ascend Learning Trust. This message is private and confidential. If you have received this message in error, please notify us and remove it from your system. If you are not the intended recipient of this email, you must neither take any action based upon its contents, nor copy or show it to anyone. Please note that Ascend Learning Trust does not warrant that any attachments are free from viruses or other defects and accepts no liability for any losses resulting from infected email transmissions."