Policy for

Email retention

Prepared by:	Adopted by Board of Directors
CEO	**Autumn 2025**

Contents

1. Statement of intent

All AET policies are written to support our schools and communities. We do this by ensuring they are always in line with our Colleague Values:

Applying these values to everything we do means always acting with integrity, in the interests of others, being honest, open and transparent and putting the safety of our children first.

2. Introduction

The Aspire Educational Trust understands 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 and staff.

The Trust is committed to providing a safe learning and teaching environment for all pupils and staff 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.

A member of staff could inadvertently create an issue for the Trust by sending an email message. For example, he or she 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 UK General Data Protection Regulation (UK GDPR) or the Freedom of Information Act (FOI) and may be cited as evidence in legal proceedings.

In recognition of the principles that underpin The Data Protection Act 2018 and Freedom of Information Act 2000 the Trust maintains 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.

The Trust 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 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.

Should you need more information or have any questions about anything outlined in this policy, then direct them to your Data Protection Lead (DPL) or the Trust's Data Protection Officer (DPO) (dpo@aet.cheshire.sch.uk)

3. Email Storage

Please note, 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 local Data Protection Lead (DPL) for guidance.

Emails must be automatically deleted **6 months** after being received. The exception to this rule is any finance related emails that must be kept **for 6 years FOLLOWING** the **current year** we are in.

Please see the exemplar email data processing actions below.

Email content **MUST** be assessed and stored in line with the AET Records Management Policy.

Deleted emails: Where a "Recycle Bin" is in use, emails held within the Recycle bin will be stored for a maximum of 10 calendar days before being automatically and permanently deleted.

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 the is no beneficial need or business requirement.

Where possible the sender should consider using 'bcc' to avoid breaches of GDPR.

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.

If you believe you receive an email in error, you **MUST** contact the sender 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. If the sender has confirmed that the email has been sent in error the recipient **MUST** delete the email immediately from all devices and the local DPL 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 the DPO and inform them of the error.

4. Exemplar email data processing actions

Email Processing Question:	Action:
The email is informal correspondence between staff or external bodies, confirming a meeting, or agreeing something that is not related to documents detailed in the AET document retention policy	The email must be deleted once processed or automatically deleted after 6 months.
I am only wanting to retain the email due to the attachment?	Save the attachment to the academy document storage system. Once stored, the email can be deleted. Ensure that the attachment is stored in line with the AET Records Management Policy.
The email contains information that is required for audit trail purposes such as correspondence on contracts or purchases, correspondence pertinent to quality assurance processes or delivery of projects etc?	Review data type and file email in line with the AET Records Management Policy.
I have received an email that I want to keep but am not sure if I am allowed.	Review the AET Records Management Policy for guidance. If you are still unsure, please contact your local DPL.
Emails can act as evidence of the school's activities, i.e. in business and fulfilling statutory duties, so all relevant emails.	To be retained for at least 6 months.
I need to retain an email longer than the required retention period as it may be required for litigation.	If data is required for longer than the period stated in the AET Records Management Policy then you must clearly document why this data is being kept for longer. Data can be retained for as long as necessary, but we need to have a legitimate reason for doing so. Your mailbox is not to be used to store staff performance data or pupil data such as SEN and Safeguarding information. Emails that contain information about pupils that form part of a pupil record must also be stored elsewhere. Please ensure this data is kept in the appropriate system such as SIMS or CPOMS. If in doubt contact the Trust's DPO.
Is there a way to manage my mailbox more efficiently?	Keep on top of monitoring your mailbox. Letting emails build up will make it more difficult to manage. Local IT can set up Folders to ensure data that is required for longer than 6 months is not deleted. For example, a folder that retains emails for 1 year, 3 or 6 years. These folders should be used in accordance with the retention periods stated in AET Records Management Policy.

	You should also ensure data is stored in the appropriate place/system. This may not always be your mailbox.
Why can I not keep all my emails?	The UK General Data Protection Regulation and Data Protection Act 2018 requires organisations to have definite retention periods and to not retain personal data for periods that are longer than necessary. Retaining data for longer than is necessary or legally required means we are non-compliant and opens the Trust to a number of risks such as reputational and financial risks. Storing excessive data can also make handling a Subject Access Request very time consuming and difficult.