Email Retention Policy

THIS POLICY WAS AGREED BY TRUSTEES ON (Date):	March 2026
REVIEW DATE:	March 2028
CHAIR OF TRUSTEES:	
CEO:	

Introduction

EPA Trust (referred to as "The Trust" and any or all of its Academies), 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 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.

This policy will be reviewed every 2 years or as necessary to reflect best practice, or amendments made to legislation.

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; 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 General Data Protection Regulation (GDPR) or the Freedom of Information Act (FOI) and may be cited as evidence in legal proceedings. Recent legislation such as the Data Protection Act 2018 and Freedom of Information Act 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. 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 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 safe guard business critical information.

Email Storage

2.1. 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. (Each school has a DPL, the Trust CEO is the DPO)

2.2. Emails should be deleted as soon as possible to avoid the storage of large amounts of potential data some of which is being retained beyond any necessary business purpose. Therefore, best practice is to regularly, perhaps weekly, to delete emails. They must be automatically deleted 6 months after being received unless required for business-critical needs or for other operational purposes.

2.3. Where a “Recycle Bin” is in use, email held within the Recycle bin will be stored for a maximum of 10 calendar days before being automatically and permanently deleted.

2.4. 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 EPA emails. Please see E-Security for more information

2.5. When sending emails only include users that are required and where the content is appropriate for the uses. Emails must NOT be sent to recipients where the content is not appropriate or where there is no beneficial need or business requirement.

2.6. 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.

2.7. If you believe you receive 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 the local DPL must be notified.

2.8. 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 recipients informing them of the error and requesting that it be removed immediately. You MUST also contact your local DPL and inform them of the error.