

Ormiston Academies Trust

Cowes Enterprise College, an Ormiston Academy Email Retention policy

Policy version control

Policy type	Statutory, template is mandatory
Author	Alex Coughlan Data Protection Officer
In consultation with	Data Strategy and Information Governance Board
Approved by	James Miller, Director of Estates and Technology, October 2021
Release date	February 2022
Next release date	February 2023
Description of changes	<p>February 2022 changes (Version 5)</p> <ul style="list-style-type: none"> ▪ GDPR updated to UK GDPR ▪ Data Retention Policy updated to Records Retention Policy ▪ Author changed to Alex Coughlan <p>October 2021 changes (Version 4)</p> <ul style="list-style-type: none"> ▪ Author Changed from Sonia Pressure to Laurence Boulter ▪ Amended references to statutory framework to reflect the ongoing context. ▪ Various adjustment in grammar (possessive apostrophes, definitive articles etc.) ▪ Addition to exemplars to contain a direct reference to the management of pupil files. ▪ Adjustment to paragraph numbering for suggested audit questions.

Contents

1. Introduction	3
2. Email Storage.....	3
3. Signature.....	4
4. Exemplar email data processing actions.....	5
5. Email Retention Audit.....	6

1. Introduction

Ormiston Academies Trust (referred to as “the Trust” and any or all of its Academies), 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.

This policy will be reviewed every 12 months 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 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@ormistonacademies.co.uk).

2. 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.

- 2.2. Emails must be automatically deleted 6 months after being received unless required for business-critical needs or for other operational purposes.
- 2.3. Email content **MUST** be assessed and stored in line with the OAT Records Retention Policy.
- 2.4. 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.
- 2.5. 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 OAT emails. Please see eSafety and eSecurity Policy for more information.
- 2.6. 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.
- 2.7. 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.
- 2.8. 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.
- 2.9. 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 local DPL and inform them of the error.

3. Signature

- 3.1. It is very important that a format for email signatures is shared across all Trust academies. Naturally, differences in ICT platforms, email applications etc. will exist, and therefore guaranteeing an identical format is a challenge. Despite this, staff are requested to adopt a format that is consistent, smart and as close to the example below as possible.
- 3.2. The example below can be copied and pasted, but parts may need re-formatting.
- 3.3. Please Note: Information located within **[]** and highlighted in yellow are to be changed to meet the local user and site. If this is not required, then **MUST** be removed. Yellow highlighting must also be removed.
- 3.4. The quality of the logo image is paramount, and images already in circulation that appear blurred and pixelated must be replaced.

[First Name] [Last Name] | [Job Title] | [Site Name]
DD: +44 (0)##### | M: +44 (0)##### | E: [Email Address]



[Site Name.]
[Site Address]
☎ [Main Phone Number #####]
✉ [Main Email Address]



IMPORTANT NOTICE: This message contains confidential information and is intended only for the recipient. If you are not the recipient you should not disseminate, distribute or copy this email. Please notify [Appropriate Email Address] immediately if you have received this email by mistake and delete this email from your system. Email transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. Ormiston Academies Trust does not accept liability for any errors or omissions in the content of this message, which arise as a result of email transmission. Ormiston Academies Trust is a limited registered company in England and Wales, registration number 06982127. The registered office for Ormiston Academies Trust is Ormiston Academies Trust, 1, Victoria Square, Birmingham, B1 1BD.

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 OAT document retention policy	The email <i>must</i> be deleted once processed or automatically deleted after 6months
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 OAT Records Retention 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 OAT Records Retention Policy.
I have received an email that I want to keep but am not sure if I am allowed.	Review the OAT Records Retention 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 12 months.

<p>I need to retain an email longer than the required retention period as it may be required for litigation.</p>	<p>If data is required for longer than the period stated in the OAT Records Retention Policy than 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 your DPL or the Trust's DPO.</p>
<p>Is there a way to manage my mailbox more efficiently?</p>	<p>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 OAT Records Retention Policy. You should also ensure data is stored in the appropriate place/system. This may not always be your mailbox.</p>
<p>My Academy needs to amend the automatic deletion period, is this possible?</p>	<p>Yes, if you have a legitimate reason for amending the automatic deletion period. For example, Covid 19 has delayed responses to emails, so they are required for longer than the 06 months. Your Academy must document this change, so it is reflected in your retention policy.</p>
<p>Why can I not keep all my emails?</p>	<p>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.</p>

5. Email Retention Audit

5.1 It is the responsibility of the Data Protection Lead (DPL) and local IT to ensure retention audits are conducted at regular intervals. This can be done on a termly basis, half termly or any other interval the academy deems appropriate.

5.2 The email retention Audit findings need to be documented and sent to OAT Data Protection Officer: dpo@ormistonacademies.co.uk

5.3 It is recommended that all staff at your academy have reviewed the Record Retention Policy and Email Retention policy, so that any questions about these policies can be raised and addressed before conducting a retention audit.

5.4 The email retention audit should be conducted on a random sample of staff and if possible, avoid staff doing the same job role. For example, if you conducted your audit on 10 members of staff, and they were all teaching staff, this would not include a variety of job roles.

5.5 The questionnaire in 5.6 should be completed by the staff member included in the audit and where possible, the information provided verified by the DPL and/local IT member. For example, if the staff member states they delete emails within the required retention period then a check of the staff email account should show this is the case. The questionnaire can be amended to reflect the needs of the Academy.

5.6 Sample Record Retention Audit Questionnaire for Staff:

Staff job title: _____
Date of Audit: _____
Name of Auditor: _____
Auditor's job title: _____

Please ensure you answer all the questions below independently.

1. I can locate policies relating to records retention and know who in my academy can assist with questions?
2. Routine emails not relating to pupils, safeguarding or another legitimate reason should be retained for no longer than?
3. Do you have emails older than this period? If yes, approximately how many emails?
4. Do you know your academies policy/procedure on deleting confidential data?
5. Can you please outline what the process is?
6. How often do you review the documents you manage?
7. **[Insert a question regarding retention that is specific to the staff members role.]** For example, a teaching staff member could be asked, 'how long we are required to keep Pupil's work?'