RIVERSIDE SCHOOL

Email Protocol and Retention Policy

APPROVED BY GOVERNORS

RESPONSIBLE PERSON – HEADTEACHER

February 2023

Contents

Email Protocol

Email Retention

Email Protocol

1. Objectives

The primary objectives of this protocol is:

- to set the expectations for email etiquette and establish email management standards and retention guidelines;
- to help comply with the legal requirements for email management and protect the school against litigation; and
- to support the school's Cyber Security Policy.

This policy applies to the use of the school's email facilities to send, receive and manage email messages (and attachments) whether accessed through a PC, laptop, personal device or any other hardware device. It is applicable to all school staff, teaching and non-teaching, whether working from the school, at home or from any other location. This policy should be read in conjunction with the Cyber Security Policy.

Staff found to be in breach of this policy may be disciplined in accordance with the school's disciplinary procedures. In certain circumstances, breach of this policy may be considered gross misconduct.

This policy aims to enhance the use of email as part of the portfolio of communication media and develop good practice in the use of email as a medium of communication.

2. Email Etiquette

Email is a key communication tool but we need to ensure that it is used as effectively as possible and maintains the highest professional standards which are in line with the school's values, ethos, Staff Code of Conduct, Data Protection Policy and Staff Handbook.

Email correspondence should only be used to answer factual questions or to arrange a face-to-face meeting. Sensitive or complex issues should always be dealt with in person to ensure clarity of understanding and help prevent misinterpretation. Before sending an email consider whether it is the correct medium for communication.

Where possible, emails should normally be answered within 48 hours of receipt (not including weekends or holidays). If more time is required for a response, reply with an email saying that you have received it and will get back to the sender is good practice. Parents will be informed that teachers will normally not be able to respond during the working day and that urgent emails should be directed to reception.

Emails should be given the same level of attention as drafting a formal letter. Emails could potentially commit the school to an agreement with parents, suppliers and other third parties, or provide evidence of harassment, defamation, libel and discrimination if worded incorrectly. Use a concise, professional standard of communication and write in

accurate, plain English. Use short paragraphs and blank lines between each paragraph.

Managers need to have an awareness of staff needs as some may require support interpreting and acting on the information contained within an email. For example, staff who may have a disability such as dyslexia, could need the email to be printed, read to them slowly or more time to complete actions.

The school's preferred font for email is Verdana or Calibri, font size 10 and black. Do not use all capitals as this is regarded as shouting. Avoid using exclamation marks or emoticons. Email accounts will be set up to include the school's signature.

Emails should target the recipient(s) appropriately by sending it only to those people who really need to read it or to take action as a result of its content. Only distribute emails to colleagues who need to receive the message. It may sometimes be appropriate to blind copy (bcc) other staff in to the email depending on the nature of the email.

Emails should always have a subject and be meaningful so that people immediately know what the message is about. Be careful with the Reply All function. Do all the recipients of the original message really need to read your response?

It is appropriate to re-read your email before you send it and check details of recipients in the address bar are correct. This helps to ensure that your message is effective and may avoid potential misunderstandings later. In addition, it helps to prevent data breaches.

If you are uncertain about the content or tone of an email, it is appropriate to ask your line manager or a member of the senior leadership team to check what you have written before sending.

The vast majority of emails do not need delivery and read receipts. If you want to know whether an email was received, it is better to ask the recipient to let you know if it was received in the body of the email.

3. General Use of Email

Staff must not:

- Use a personal or non-work email account to send or receive school business emails.
- Use a false identity in emails nor use email for the creation or transmission of anonymous messages.
- Create emails, or alter a message and then forward it, with the intention of deceiving the recipient.
- Create, transmit, or forward any illegal, offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images.

- Create, transmit, or forward material that is designed or likely to cause annoyance, inconvenience or needless anxiety.
- Create, transmit or forward material that is designed to or would conflict with the school business, or undermine the school in any way.
- Create, transmit or forward emails containing staff, pupil or family personal information, or information that is sensitive, to a personal or non-work email account or to a work email account where the recipient does not require it for legitimate use. Please also refer to guidance regarding protecting documents.
- Attempt to gain access to the email mailbox of any other member of staff without their permission.
- Send an email message to pupils of the school unless you have been authorised by the headteacher to do so.
- Include sensitive personal data within emails.
- Forward emails containing anyone's personal messages without their permission.
- Forward material via email in breach of copyright.
- Send emails referring to the recipient colloquially or with terms of endearment not appropriate to the workplace i.e., "Hi Darling", "Hey Babes" etc. In the same regard, emails should not be signed off with a kiss or similar gesture.
- Use their work email address when posting comments on public bulletin boards or chat rooms unless directly related to your work.
- Never participate in chain emails where you are asked to forward an email to a number of others.
- In legal terms, under the Telecommunications Regulations 2000, sending an email is as binding as sending a signed letter. Therefore, do not express personal views or information by email, because as an employer, Riverside School can be held vicariously liable for the opinions and views expressed.

This also applies to comments posted on public discussion boards if you use the school email address or state the opinions in a work capacity.

Staff should:

- Be 'responsible communicators' i.e., they should check their emails at the start of each day as they currently would their pigeon holes.
- 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 (electronic or paper based), in line with UK GDPR guidance and the school's Retention Schedule.
- If they require response, consider carefully the use of the "reply all" button.
- Delete unwanted emails promptly.
- Protect yourself from viruses when emailing from home.
- 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 the school or LA, as the email address contains the name of both.
- If an urgent email is sent, you may want to follow this with a phone call.

4. Security

Staff are responsible for the security of their computer, and for protecting any information or data used and/ or stored on it. Staff must log out from or lock their computer when temporarily away from their desk to prevent unauthorised use of email accounts. This applies wherever you are located at the time of use. Mailboxes should not be left open and unattended and the computer must always be locked. Staff need to strive to keep their passwords confidential to prevent other users from accessing and sending emails from their account. Users may need to make their passwords known in the event of absence.

Staff must not open any email from an unrecognised source or emails that have dubious or missing subject lines.

Staff should not open unsolicited email attachments or suspect links unless they are sure of the source. To check suspicious links, hover over sender to see the source address before making a judgement. Also look for spelling errors or control characters being used. Report all problems with unwanted emails or any suspicious activity to ICT. Never send or forward chain email messages or virus warnings, as the vast majority are bogus and a waste of time.

When prompted, staff are responsible for changing passwords on an agreed schedule to maintain security. Passwords should ideally contain a mix of uppercase and lowercase letters, a number and a symbol.

5. Sensitive Information

Emails are the electronic equivalent of a postcard. Anyone can read the content along the delivery path. Sensitive information should be sent by post or via a secure transfer system. The school uses Egress, plus password protection on documents to protect sensitive electronic documents.

In general, emails containing sensitive information should be limited to identifiers i.e., pupil initials and date of birth as opposed to using a pupil's full name and DOB.

Child protection issues should not be reported via email. There is a secure reporting system in place named CPOMS. Staff must use CPOMS to log any concerns or issues.

6. Personal Email Use

Limited personal email use by staff in their own time at work is permitted, but this must

comply with the Cyber-Security Policy. Clearly title personal email and email folders as "personal" to reduce the risk of ICT administrators inadvertently viewing private non-work emails. Delete personal mail from email systems as soon as possible.

Staff must not use the school's email system to send:

- personal adverts;
- personal sponsorship requests;
- personal appeals; or
- details of events that are not supported by the school.

Do not use the school's email system to send or receive multimedia attachments that are not related to school work e.g., containing images, video or sound clips. Do not use your school email account as the registration email address when registering with any organisation or web-site for personal use.

7. When to Use Other Methods of Communication

Never discuss performance appraisal or review issues by email, always do it face-to-face. It may however, be appropriate to summarise some of the content of discussions via email.

HR issues (salary, job, career progression) should not be discussed by email. This is dependent on the context and appropriateness.

Private or privileged client materials may not be appropriate to send by email. If unsure please discuss with your line manager.

Complex issues should be discussed at meetings. This helps to prevent possible miscommunication or incorrect interpretations.

Topics that require interactive dialogue or robust discussion on certain issues may not be best conducted via email.

When needing to vent frustrations about a workplace situation, particularly if you are angry may not be appropriate by email. Wait to calm down so your response is more measured and professional.

8. Inspection of Email Records

Emails will only be monitored by the headteacher in very exceptional circumstances. Staff must comply with a request from the headteacher, or delegated member of staff, to inspect email records and/ or to printout items relevant to a particular individual, case or subject. This will only be requested when required under the Data Protection Act 2018; under a Freedom of Information request; as part of a disciplinary investigation; or for

other legitimate school business reasons.

The email accounts of absent staff may be opened by another member of staff.

Email will be checked:

- if there is a reasonable cause to believe the member of staff has violated or is violating this policy, and guidelines or procedures established to implement this policy;
- if an email account appears to be engaged in unusual or unusually excessive activity;
- if it is necessary to do so to protect the integrity, security or functionality of ICT resources or to protect the school from liability;
- to establish existence of facts relevant to school business;
- to prevent or detect crime;
- to investigate or detect unauthorised use of email facilities;
- to ensure effective operation of email facilities;
- to determine if communications are relevant to school business (for example, in the last resort where a member of staff is off sick or on holiday and business continuity is threatened);
- if a member of staff is absent; and
- if it is otherwise permitted or required by law.

Where an individual has reasonable cause to believe that a member of staff has violated, or is violating this policy, or any guidelines, or procedures established to implement this protocol then they shall, in the first instance, inform the headteacher who may refer the matter for investigation under the school's Disciplinary Policy and Procedure for Staff. In these circumstances, the checks may necessitate the immediate suspension of the member of staff's access to the school network, ICT resources, ICT systems and applications in order that any potential evidence is not compromised.

The school's email provider will apply automatic message monitoring, filtering and rejection systems as appropriate and deny transmission or receipt of messages with content that represents a threat to the ICT network or is unacceptable in the terms of this and other school policies. An ICT administrator may examine messages placed in quarantine, and forward or delete them as appropriate.

Email Retention

9. Introduction

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 school to an action by an

email message; they can cause illegal material to be transmitted through the school's systems for which the school may be liable; all emails held at the school are legally discoverable following a request under the UK General Data Protection Regulation (UK GDPR) or the Freedom of Information Act 2000 (FOI), and may be cited as evidence in legal proceedings.

The Data Protection Act 2018 and Freedom of Information Act 2000 have 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 FOI 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 the FOI access request or a UK GDPR access request.

The school will retain only personal data that is appropriate for the function of the organisation. This will ensure the school meets its data protection obligations set out in law.

This document sets out the guidelines that the school will follow to ensure data is not kept longer than needed, ensuring the school 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 the school business manager or the administration and data manager.

10. Emails and Retention

The retention period of emails is up to the school to decide. Having a retention period in place can ensure schools do not keep data longer than necessary and can greatly assist the school to reduce the content of a search, should we receive any subject access requests; as you are expected to search emails (unless otherwise stated), having a retention period can significantly reduce the workload.

Judicium (the school's DPO) recommends a retention period of 2 or 3 years provided that emails/ attachments that require retaining for longer are kept separately (for example in a personnel file/ SIMS).

The emails and documents contained in school mailboxes will be retained for a maximum of 3 years (36 months).

This policy will be reviewed every 3 years, or as necessary to reflect best practice, or amendments to legislation.

Email accounts are not a case management tool in itself. Generally, emails may need to

fall under different retention periods (for example, an email regarding a health and safety report will be subject to a different time frame to an email which forms part of a pupil record). It is important to note that the retention period will depend on the content of the email and it is important that staff file those emails in the relevant areas to avoid the data becoming lost.

The school's data protection leads (DPLs) are:

- Tracy De Freitas – Administration and Data Manager
- Naomi Walters – School Business Manager

11. Email Storage

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 one of the DPLs for guidance.

Emails will be automatically deleted at the end of the third academic year of receipt, unless required for business-critical needs, or for other operational purposes.

Email content must be assessed and stored in line with the school's Data Protection Policy.

Where a "recycle bin" is in use, emails held within the recycle bin will be stored for a maximum of three academic years before being automatically and 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 school emails. Please see the E-Safety Policy for more information.

When sending emails only includes 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 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 immediately contact the sender only 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.

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.

12. Exemplar Email Data Processing Actions

Email Processing Scenario	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 this policy.	The email must be deleted once processed or automatically deleted at the end of the third academic year.
I am only wanting to retain the email due to the attachment.	Save the attachment to the school's electronic storage system. Once stored, the email can be deleted. Ensure that the attachment is stored in line with the school's Data Protection Policy.
The email contains information that is required for audit trail purposes such as correspondence on contracts or purchases or purchases, correspondence pertinent to quality assurance processes or delivery of projects etc.	Review data type and file email in line with the school's Data Protection Policy.
I have received an email that I want to keep but am not sure if I am allowed.	Review the school's Data Protection Policy for guidance. If you are still unsure, please contact your local DPL.
I need to retain an email longer than the required retention period as it may be required for litigation.	If the data is required for longer than the period stated in the school's Data Protection 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. Please ensure this data is kept in the appropriate system such as SIMS or CPOMS. If in doubt contact your DPL or the school's DPL.
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 to be kept is stored appropriately. For example, a folder that retains emails for 1 year, 2 or 3 years. These folders should be used in accordance with the retention periods stated in the Data Protection Policy. You should also ensure data is stored in the appropriate place/ system. This may not always be your mailbox.

Is it possible for the school amend the automatic deletion period?	Yes, but only on a whole school basis. There may be legitimate reasons for amending the automatic deletion period. For example, Covid 19 has delayed responses to emails, so they may be required for longer. However, the expectation is that staff are storing emails and their attachments in line with the school's retention guidelines.
Why can I not keep all my emails?	The UK General Data Protection Regulation and the Data Protection Act 2018 require organisations to have definite retention period, and not to retain personal data for longer than necessary. Retaining data for longer than is necessary or legally required means we are non-compliant and opens the school to a number of potential risks such as reputation or financial. Storing excessive data can also make handling a subject access request very time consuming and difficult.

13. Email Retention Audit

It is the responsibility of the DPLs and local IT to ensure retention audits are conducted at regular intervals. This can be done on an annual basis or any other interval the school deems appropriate.

The email retention audit findings should be documented and saved in the GDPR folder located in Personnel\GDPR\Audit Findings.

It is recommended that all staff in the school have reviewed the Data Protection Policy and Email Retention Guidelines, so that any questions about these policies can be raised and addressed before conducting a retention audit.

The email retention audit should be conducted on a random sample of staff and if possible, avoiding 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 role.

The below questionnaire should be completed by staff members included in the audit and where possible, the information provided verified by the DPL and/ or 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 school.

14. 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 data retention and know who in my school 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 the school's policy/ procedures 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 that is specific to the staff member's role). For example, a teaching staff member could be asked 'how long are we required to keep a pupil's work?'