STAFF EMAIL POLICY

Reviewed and updated: March 2022
Next review: March 2025
Status: non-statutory

This policy should be read with reference to the following policies:

- E-safety.
- Staff discipline.
- Internal data security.
- ICT and use of the internet and intranet by staff.
- Staff professional identity protection.
- Social media.
- Use of personally owned ICT devices by staff.

Background

The use of email within a school is an essential means of communication for both staff and students. Educationally, email offers significant benefits including direct written contact between schools on different projects, be they staff-based or student-based, within school or in an international context.

Members of staff need to understand how to style an email in relation to good network etiquette (netiquette) and need to teach students to handle email in the same way.

STAFF EMAIL POLICY

Introduction

The use of email within **Elthorne Park High school** is an essential means of communication for both staff and students. In the context of school, emails should *not* be considered private and staff should assume that anything they write or email could become public. Therefore, they should ensure that they are professional, maintaining a clear distinction between their personal and professional lives.

Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff-based or student-based, within school or in an international context.

We recognise that staff and students need to understand how to style an email in relation to good network etiquette (netiquette*)*.

If data is to be sent with an email then reference must be made to the school internal data security policy and if it is personal data then the Data Protection Act and the General Data Protection Regulation (GDPR) 2018 must be followed.

Objectives and targets

The purpose of this policy is to outline the procedure and protocols to be used when staff use email.

Action plan

Managing emails
The school gives all staff their own email account as a work-based tool. This school email account should be the account that is used for *all* school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal contact information being revealed.

For the safety and security of users and recipients, all mail is filtered and logged. If necessary, email histories can be traced.

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.
- All external emails, including those to parents, should be constructed in the same way as a formal letter written on school headed paper (i.e. use of Dear Mr/Mrs/Ms and ‘Yours sincerely’).
- If any issues/complaints are involved, then staff sending emails to parents, external organisations or students are advised to cc their line manager/s.
- The school requires a standard disclaimer to be attached to all email correspondence, clarifying that any views expressed are not necessarily those of the school – see the appendix.
- ICT technical support will set up all school staff email accounts so that the disclaimer is added to all emails.

- All emails should be written and checked carefully before sending.
- 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.
- Staff are expected to manage their staff email account in an effective way as follows:
  - Delete all emails of short-term value.
  - Organise email into folders and carry out frequent house-keeping on all folders and archives.
  - However you access your school email, (whether directly, through webmail when away from the office or on non-school hardware) all the school ICT, e-safety and email policies apply.
  - Only school-approved email clients can be used for school-related email.
  - Staff must immediately inform their line manager/network manager and as appropriate the DSL if they receive an offensive email, e.g. forms of harassment, bullying or unacceptable digital images.

Sending emails
The following rules apply:

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, please see the section below 'Emailing personal, sensitive, confidential or classified information' and be aware of the Data Protection Act and the GDPR.
- Use your own school email account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- School email is not to be used for personal advertising (e.g. advertising/promoting a personal business, either your own or others).
- Staff must not send any emails which could be considered to be harassing, bullying or contain unacceptable digital images.

Receiving emails
The following rules apply:

- Check your email regularly. We ask that staff check and respond or confirm receipt to emails within 24 hours.
- If appropriate, activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source. If unsure, always consult the network manager first.

- Do not use the email systems to store attachments. Detach and save business-related work to the appropriate shared drive/folder.

- The setting to automatically forward and/or delete emails is not allowed. Individuals are required to 'manage' their accounts.

Emailing personal, sensitive, confidential or classified information
Whenever handling personal information, at all times be aware of, and abide by, the Data Protection Act and the GDPR.

Assess whether the information can be transmitted by other secure means before using email. Emailing confidential data is not recommended and should be avoided wherever possible. Staff should ensure that they have read and are aware of the internal data security policy. Only school-approved email clients can be used for school-related email.

Where the conclusion is that your school email must be used to transmit such data, then exercise caution when sending the email and *always* follow these checks *before* releasing the email:

- Verify the details, including accurate email address, of any intended recipient of the information.

- Verify (by phoning) the details of a requestor, if unknown, before responding to email requests for information.

- Do not copy or forward the email to any more recipients than is absolutely necessary.

- Do not send the information to any person whose details you have been unable to separately verify.

- Send the information as an encrypted document *attached* to an email.

  - Provide the encryption key or password by a *separate* contact with the recipient(s) – preferably by telephone.

  - Do not identify such information in the subject line of any email.

  - Request confirmation of safe receipt.

- When sending an email containing personal or sensitive data, the name of the individual is not to be included in the subject line and the document containing the information must be encrypted.

- To provide additional security you need to put 'CONFIDENTIAL' in the subject line and as a header in the email and any attachments to the email.

Students and email
Those working with children need to be on the lookout for cyber bullying and other activities in emails which might affect the mental health of pupils.

Students are introduced to email as part of the ICT scheme of work. Staff should make students aware of the following when using email:

- All student email users are expected to adhere to the generally accepted rules of netiquette, particularly in relation to the use of appropriate language.
- Students should not reveal any personal details about themselves or others in email communication.
- Students should not use email to arrange to meet anyone without specific permission.
- Students must ensure that any email attachments they receive are checked for viruses before opening.
- Students must immediately inform a teacher/trusted adult if they receive an offensive email.
- The forwarding of chain letters is not permitted in school. The school has a dummy account to allow students to forward any chain letters causing them anxiety. This account will be monitored by ICT technical support.

Staff should inform other relevant staff if they become aware of *any* student misuse of emails. Staff have a duty of care and a statutory duty to report signs of potential radicalisation so staff should report to the headteacher any student who gives rise to fears that s/he may be being radicalised.

Monitoring and evaluation

This policy will be monitored by the senior management team in consultation with the network manager on a regular basis for changes or developments in current practice in email procedures and protocols. An evaluation will be made and the policy adapted or changed as necessary.

Reviewing

The headteacher will present a report to governors on an annual basis. The policy will be reviewed and altered in the light of any concerns brought to the governors and where changes in legislation make it necessary.

Next school review due March 2025

-

APPENDIX

Email disclaimer text

This email and any attachment is intended to be read by the above named recipients only and the contents may be confidential, personal and/or privileged. It is for the exclusive use of the intended recipients. Therefore, if you are not the intended recipient(s), please note that any distribution, forwarding, copying or use of this communication or the information in it is strictly prohibited. If you have received it in error, please contact the sender immediately by return email. Please then delete the email and any copies of it and do not use or disclose its contents to any person. Any personal views or opinions expressed in this email are those of the individual sender and Elthorne Park High school does not endorse or accept responsibility for them. No contractual arrangement is intended to arise from this communication. Before taking any action based upon this email message, you should seek appropriate confirmation of its authenticity.

If you have any complaints about the content of this message please reply to:

Elthorne Park High school

School telephone number: 0208 5661166

Main school email: elthorne@ephs.ealing.sch.uk