Policy:	Email
Person(s) responsible for updating the policy:	Chief Executive
Date Approved:	Board of Directors on 7 July 2016
Date of Review:	Every 3 years
Status:	Non Statutory

Tudor Park Education Trust oversees this policy but the local governing body of each academy or school within the Trust is responsible for the implementation of the policy.

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

- E-safety.
- Staff discipline.
- Secure data handling.
- ICT and use of the internet and intranet by staff.
- Social media.
- Use of personally owned 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 and need to teach students to handle email in the same way.

Introduction

The use of email, both within Tudor Park Education Trust and with the wider community, 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.

Any data exchanged with an external agency must be approved by the Principal, to ensure that the email complies with the schools secure data handling policy.

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. Staff will also be issued with a Google email account to which this policy will apply equally.

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 (ie use of Dear Mr/Mrs/Ms
- If any issues /complaints are involved then staff sending emails to parents, external organisations, or students are advised to cc their line manager/s and other relevant individuals.
- 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. Please note that this disclaimer is automatically added to emails sent externally
- 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.
- Respond to emails in a timely fashion, it is courteous to respond to emails within 24 hours.
- 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.

- Staff must immediately inform their line manager/network manager if they receive an offensive email.
- Any suspiciaous emails shoud be reported to the network manager and should not be opened

Sending emails

The following rules apply:

- When composing your message to a parent or non staff member you should always use formal language, as if you were writing a letter on headed paper.
- 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'.
- 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 whole school emails unless essential for school business
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

Receiving emails

The following rules apply:

- Check your email regularly.
- 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 of emails is not allowed. Individuals are required to 'manage' their accounts.

Emailing personal, sensitive, confidential or classified information

Assess whether the information can be transmitted by other secure means before using email. Emailing confidential data without the use of encryption is strictly prohibitied. Staff should ensure that they have read and are aware of the secure data handling policy.

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 (preferably 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. If you are unsure as to how to encrypt a file please speak to the network manager/ ICT technician.
- 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

- If students are issued with a gmail account when joining the school that is active for the time they are studying with us, staff should make students aware of the following when using email:
- Student email users are required to use the appropriate formal language in their messages.
- Students should not reveal any personal details about themselves or others in email communication.
- Students should not use email to arrange to meet anyone.
- 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.
- Staff should inform other relevant staff if they become aware of *any* student misuse of emails.

Monitoring and evaluation

The policy will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

Appendix

Email disclaimer text

The information in the e-mail is confidential and intended solely for the person to whom it is addressed. If this message is not addressed to you, please be aware that you have no authorisation to read the rest of this e-mail, to copy it or furnish it to any person other than the addressee. If you are not the intended recipient of this e-mail, please bring this to the attention of the sender and destroy the original message. Tudor Park Education Trust does not guarantee that the e-mail is free of viruses, interceptions or interference.