Feltham Hill
Infant and Nursery School

Email Policy

June 2019

The use of email within the school is an essential means of communication for staff. Staff need to understand how to style an email in relation to good network etiquette.

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

Prepared by: Deputy Headteacher
Discussed with: HT & SBM (July 2019)
Agreed with: Governing Body through shared space (July 2019)
Shared with staff: Sept 2019
To be Reviewed and Updated: June 2021

This policy should be read with reference to the following policies

- Online safety
- Staff Code of Conduct
- Staff Acceptable Use of ICT

The use of email, both within the school and with the wider community is an essential means of communication. 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, staff should ensure that they are professional, maintaining a clear distinction between their personal and professional lives.

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 minimize 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 by London grid for learning (LGFL). Email histories can be traced, if necessary.

The following guidelines apply:

- It is the responsibility of each account holder to keep their password secure.
- Staff should not use any personal email addresses.
- External emails, including those to parents/carers, should be constructed in the same was as a formal letter (i.e. use of Dear Mr/Mrs/Ms).
- Emails to parents/carers will be sent via the Office email address so that parent/carers cannot address staff directly.
- If any issues/complaints are involved then staff sending emails should cc their line manager 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 appendix A). 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 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.
- Delete the ‘deleted items’ folder
- Organise emails into folders and carry out frequent house-keeping on all folders and archives.
- Respond to emails in a timely fashion.
- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school ICT, safety and email policies apply.
- Staff must immediately inform their line manager if they receive an offensive email.
- Any suspicious emails should be reported to the SBM and should not be opened.

Sending Emails

The following guidelines apply:

- When composing your message you should always use formal language, as if you were writing a letter on headed paper.
- Emails to parents should be forwarded to the office so they can be sent from the office@ email address.
- 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'.
- 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. Wherever possible, send the location path to the shared drive rather than sending attachments.

Receiving Emails

The following guidelines 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 contact office first.
- Do not use the email systems to store attachments. Detach and save business-related work to the appropriate shared drive/folder.

Emailing personal, sensitive, confidential or classified information

Assess whether the information can be transmitted by other secure means before using email. Emailing confidential data should always be password protected. Staff should ensure that they have read and are aware of the secure handling of sensitive data.

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

- Verify the details, including accurate email address, of any intended recipient of the information
- Verify 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 verify.
- Send the information as an encrypted document attached to an email. If you are unsure as how to encrypt a file please speak to the IT consultant or SBM.
- Provide the password by a separate email.
- 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 should not 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.

Monitoring and evaluation

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