Burnt Tree Primary School

E-mail Policy
2025

Signed by Chair of Governors	
Date	04/03/2025
Review Date	March 2027

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

- E-safety
- Staff Conduct
- Social media

Background

The use of email within a school is an essential means of communication for both staff and children. Educationally, email offers significant benefits including direct written contact between schools on different projects, be they staff-based or children-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 the children to handle email in the same way.

Introduction

The use of email, both within Burnt Tree Primary School and the wider community, is an essential means of communication for both staff and children. 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 with an external agency must be approved by the Head Teacher, to ensure that the email complies with the schools secure data handling policy.

Objective and Targets

The purpose of this policy is to outline the procedure and the 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. The 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 must not use personal email accounts to send or receive school-related information, particularly where it involves student data, safeguarding, or confidential matters. All school correspondence must be conducted via the official school email system.

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 children or parents regarding the conduct of 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 to parents (ie the use of Dear Mr/Mrs/Ms).
- If any issues/complaints are involved then staff sending emails to parents, external organisations, or, children are advised to cc their line manager/s and other relevant individuals.
- 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.
- Emails containing personal or sensitive data must be retained in line with the school's Data Retention Policy. Staff must not delete emails related to safeguarding, parental concerns, or staff communication without prior approval from the Data Protection Officer (DPO).
- Organise emails into folders and carry out frequent house-keeping all folders and archives.
- Staff should respond to emails within a reasonable timeframe during working hours (Monday-Friday, 8:00 AM - 4:30 PM). Staff are not expected to respond to emails outside of contracted hours or during weekends/holidays unless there is an emergency or safeguarding concern
- 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 suspicious emails should 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.
- Whole school emails should only be sent for urgent updates, safeguarding concerns, or school-wide initiatives approved by senior leadership. Staff should use departmental or group emails where possible to reduce inbox overload.
- Do not send or forward attachments unnecessarily.

Receiving Emails

The following rules apply:

- Check your emails regularly.
- If appropriate, activate your 'out-of-office' notification when away for extended periods.
- Never open attached from an untrusted source. If unsure, always consult the network manager first.
- Do not use the emails systems to store attachments. Detach and save business-related work to the appropriate shared drive/folder.
- The settling 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 prohibited. Staff should ensure that they have read and are aware of the secure data handling policy.

All emails containing personal, sensitive, or confidential information must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (2018). Staff must ensure that they have completed data protection training and follow school procedures for secure data handling.

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 addresses, of any intended recipient of the information.
- Verify (preferring by phoning) the details of a requestor, if unknown, before responding to email requests for information.
- Do not copy the forward the email to any more recipients that 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 ICT technician.
- Provide an encryption key or password by a *separate* contact with the recipients(s)- preferably by telephone.
- Do not identify such information in the subject line of 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 as a header in the email and any attachments to the email.

Pupils and Email

- All pupil email accounts are monitored by school staff to ensure appropriate use. Pupil-to-pupil communication via email must only take place when supervised and for educational purposes. Any misuse of email, including cyberbullying or inappropriate messaging, will be reported to the Designated Safeguarding Lead (DSL) and dealt with in line with the school's behaviour policy.
- 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 technical developments which might need a change in the policy.