

Roding Primary - Email Policy 2020

The use of e-mail within schools is an essential means of communication. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact within the school and to external organisations i.e. other schools, the borough, outside agencies and individuals, i.e. parents within school or international.

1. Staff Accounts

- a) Via the Borough, the school requests an individual e-mail account for all staff to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- b) Staff should use their school email for all professional communication.
- c) It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- d) Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- e) All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- f) E-mails 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. You must therefore actively manage your e-mail account as follows:
 - Delete all e-mails of short-term value
 - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- g) A signature should be included on all e-mails sent:
 - Internal e-mails – Name.
 - External e-mails – Name, position and contact details.
- h) The school requires a standard disclaimer to be attached to all e-mail correspondence. The responsibility for adding this disclaimer lies with the account holder:

E-mail confidentiality notice. This message is intended for the addressees only. It may be private, confidential and may be covered by legal professional privilege or other confidentiality requirements. The views expressed are not necessarily those of the school or the LA. If you are not one of the intended recipients, please notify the sender immediately on (+44) 020 8270 4010 and delete the message from all locations in your computer network. Do not copy this email or use it for any purpose or disclose its contents to any person: to do so maybe unlawful. Roding Primary School, Cannington Road, Dagenham, Essex, RM9 4BL, United Kingdom. (to be amended by staff for Hewett Road)
- i) The forwarding of chain emails is not permitted in school. If a chain email is received please advise Technical support via the helpdesk.
- j) Staff must inform the eSafety co-ordinator or Assistant Head if they receive an offensive e-mail.
- k) Staff must not leave their mailbox open and unattended and shared areas (i.e. classrooms, PPA room).

2. Children's Accounts

- a) Children may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- b) Only children in Years 2-6 will have their own individual school issued accounts. All other children use a class/ group e-mail address.
- c) Children are introduced to e-mail as part of the Computing Programme of Study.
- d) All children e-mail users are expected to adhere to the rules of responsible online behavior, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission. These rules will be reviewed at the start of each e-mail unit.
- e) Children must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail.

3. Sending e-mails

- a) Do not send e-mails to parents/carers from your own school e-mail account. All electronic communication with parents/carers should go via the school office e-mail account with you

Roding Primary - Email Policy 2020

identified clearly as the originator of the message.

- b) Staff sending e-mails to external organisations or parents are advised to cc. the appropriate Assistant Head, Site Head, ECM, or other appropriate person.
 - c) Confidential information should be sent by post or via a secure transfer system. However, if this is not possible and an e-mail needs to be sent containing personal, confidential, classified or financially sensitive data to external third parties or agencies, please refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information.
 - d) When sending an e-mail, address it only to the person who is required to reply or action it. If additional people are to be made aware of the contents of the email, use the cc function. Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
 - e) The school does not promote the use of bcc.
 - f) When replying to an email, ensure that 'reply' is selected from the drop down list. Do not click on the reply button as this will default to 'reply all' unless you change the global settings in your account.
 - g) Only ever use your own school e-mail account for school business purposes. This ensures that you are clearly identified as the originator of a message.
 - h) Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
 - i) School e-mail is not to be used for personal advertising.
 - j) Downloading and sending of copyright material is not allowed.
 - k) Emails should not be sent while teaching.
-

4. Receiving e-mails

- a) Check your e-mail regularly.
 - b) Activate your 'out-of-office' notification when away for extended periods.
 - c) Never open attachments from an untrusted source; consult your network manager first.
 - d) Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
 - e) The automatic forwarding and deletion of e-mails is not allowed.
 - f) Save external attachments into your my documents before opening to ensure that the school's antivirus software scans the attachment before opening.
 - g) Do not open attachments sent from an email account you do not know. If you are expecting contact from an external organization follow point **f**) above before opening.
-

5. Personal e-mail accounts

- a) Staff can access personal e-mail accounts outside of lessons or directed time (i.e. break time and lunch time [if not on duty]).
 - b) Personal e-mail accounts should not be used for any school business.
-

6. Security and safety

- a) School e-mail addresses should only be registered with reputable organisation for the business of the school.
 - b) Personal information should never be given out over the internet unless the procedures identified under section e-mailing Personal, Sensitive, Confidential or Classified Information are followed.
 - c) Never open, reply to or forward spam (junk e-mail). Inform technical support if this occurs via the helpdesk.
 - d) Report any problems with your e-mail account to technical support via the helpdesk.
 - e) However school e-mail accounts are accessed (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.
-

7. Monitoring of e-mail accounts

- a) There may be occasions when an e-mail account requires monitoring. This will only be performed under the direct request of the Executive Headteacher.
- b) If this is required, it will be performed confidentially by the Network Manager, with the results passed directly to the Executive Head.

8. e-mailing Personal, Sensitive, Confidential or Classified Information

- a) Where your conclusion is that e-mail must be used to transmit such data:
Obtain express consent from your manager to provide the information by e-mail. Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
 - Encrypt and password protect the document
 - Verify the details, including accurate e-mail address, of any intended recipient of the information
 - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
 - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- b) Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- c) Send the information as an encrypted document **attached** to an e-mail
- d) Provide the encryption key or password by a **separate** contact with the recipient(s)
- e) Do not identify such information in the subject line of any e-mail
- f) Request confirmation of safe receipt
- g) Do not refer to any children specifically by name in the contents or subject header of the email, use initials if required.