Burdett-Coutts & Townshend CE Primary School

Email Security & Etiquette Guidance

Date: September 2019
Review date and frequency: July 2021
Lead Person(s): E. Camplin, Data Protection Lead
Ratification by: FGB (@ meeting 19th September 2019)
Statutory Policy: No
Policy Author: *Adapted from London Diocesan Board Model Policy March 2018*

Table of Contents

1. Aims

This policy aims to provide guidance to staff and governors around email use within our school, including how to ensure a level of email security and data protection, as well as having good manners in its day to day use a communications tool.

Email as a tool allows us not only to communicate with people, organisations, public bodies and service providers easier than ever before, but it also allows us to pass information further and easier as well.

This use of email is defined as processing under GDPR 2018 and as such all email communication needs to be created, secured, transmitted and handled in accordance with those regulations.

This guidance applies to all communication by school employees, governors, and third-party staff using email to conduct business on behalf of the school, whether with school employees, other governors, and/or third-party staff; as well as governors who have access to a school email account.

2. Email Security Measures

School employees, governors, and third-party staff using email to conduct business on behalf of the school, or who have access to a school email account should abide by the following guidance on email security. By doing so, this ensures that the technical IT security measures the school has in place remain robust and are less likely to be compromised.

1. Passwords /log ins to the email and IT system should be changed regularly and must include capital letters, numbers and symbols. 'Password', 'P@55word', 'letmein' are not to be used or included in a password and are examples of insecure passwords.
2. Emails should be regularly reviewed, and either filed, archived or deleted if not required anymore.
3. Sensitive or Special Data, which might include SEND, EHCP, medical or health information, criminal record data or financial information, should not be sent without appropriate protection and/or encryption.
4. Carefully check the recipients of the emails they are sending, especially if the auto-complete function is operating giving suggested recipient email addresses.
5. Carefully check the recipients listed in the CC box and BCC box to ensure email confidentiality of recipients where necessary.
6. Ensure email contacts are up to date, especially those that are dated or pre-set.
7. Ensure all anti-virus software and malware software is up to date on your machines
8. Do not open an attachment unless you know who the sender is, or what the attachment is about.
9. Do not enable Macros unless you have checked with IT Manager first.
10. Do not click on links to web pages without first hover the cursor over them to see if the page looks legitimate. Consider opening a blank browser and typing the address
11. Users must report unsolicited mail ("spamming") to the school administrators and/or the school IT Manager. Do not click the "Unsubscribe" link in a spam email. It would only let the spammer know your address is legitimate, which could lead to you and other users receiving more spam.
12. Email will in a user's absence be monitored or forwarded to another account for processing where necessary in the interests of business continuity.
13. When you have finished with your terminal/machine or need to leave it for some reason either ensure you have a timed lock out in place OR be sure to log out.
14. If using a shared machine in school or a public place, always log out at the end of the day.

3. Email Etiquette

The proliferation of email traffic over the last few years has allowed us to communicate more efficiently and effectively. We are entering an even greater period of email use and to ensure that

email use continues to be effective and not too burdensome there are some simple guidelines listed below that users are expected to adhere to:

1. **Understand the difference between "To", "CC" and "BCC"**. The people you include in the "To" field should be the people you expect to read and respond to the message. The "CC" field should be used sparingly. You should only "CC" people who have a need to stay in the know. "BCC" should be used for distribution lists and mail groups where there is no need to share contact information or a need to keep recipients contact data safe.

2. **Keep messages brief and to the point.** Make your most important point first, then provide detail if necessary. Make it clear at the beginning of the message why you are writing.

3. **Don't discuss multiple subjects in a single message.** If you need to discuss more than one subject, send multiple e-mails. This makes it easy to scan subject lines later to find the message you need.

4. **Reply in a timely manner.** All email should be replied to in an appropriate timeline, but normally with 24 hours of recipient during the working week. Do acknowledge received email, even if it is not possible to respond to the query immediately.

5. **Be mindful of your tone**. Unlike face-to-face meetings or even phone calls, those who read your e-mail messages don't have the benefit of your pitch, tone, inflection, or other non-verbal cues. As a result, you need to be careful about your tone. Sarcasm is especially dangerous. Choose your words carefully in email to avoid ambiguity and misinterpretation. The more precise you are upfront, the less likely you'll see subsequent emails generating confusion and asking follow-up questions seeking additional clarity.

6. **Don't use e-mail to criticize others**. E-mail is a terrific way to commend someone or praise them. It is not an appropriate medium for criticism. It almost never serves your purpose or long-term interests.

7. **Don't reply in anger**. If you find yourself in the throes of what is clearly becoming an antagonistic email discussion: **STOP!**
   Either pick up the phone or head over to the person's office to have the discussion in person. Face-to-face interaction will reintroduce all of the important sub-text that can be completely lost in email and help prevent unnecessary arguments.

8. **Don't overuse "reply to all."** If you do it just adds more clutter to everyone's already unwieldy inbox. Your default response should be to reply only to the sender. Before you reply to everyone, make sure that everyone needs to know.

9. **Don't forward chain letters.** They can be used to infiltrate the IT system and at the very least clog up mail boxes.

10. **Don't "copy up" as a means of coercion.**

11. **Don't overuse the "high priority" flag.**

12. **Don't write in ALL CAPS**. This is the digital equivalent of shouting.

13. **Don't send or forward emails containing libellous, defamatory, offensive, racist or obscene remarks.** This could mean disciplinary measures being instigated.

14. **Remember that company e-mail isn't private.** Email can be requested and included in Data Subject Access Requests. Remember that people can request what you have written about them.

15. **Use a signature with your contact information**. The school has a standard email signature that should be used and can be obtained from the school office.

16. **Provide "if-then" options.**

17. **Use your spell-checker**. Also check for punctuation and grammar.

18. **Re-read your e-mail before you send it**.

19. **Email should not be printed unnecessarily**. Printing email reduces the benefit to the environment email allows, can clog printers, and be a waste of resources if unnecessary. Create and use email files and an E-Filing System where necessary.

20. **Do not send email after 7pm**. The school promotes a work life balance which can only be obtained by staff not working late into the night or checking their emails at home.

4. Monitoring arrangements

The School DPO will monitor the guidance as part of their ongoing compliance and auditing work, and policy review schedule. As previously stated this policy will be reviewed after one year, and then after that point it will be reviewed every two years.

5. Links with other policies

This guidance is linked to our:

- Freedom of information publication scheme
- Online and E-Safety Policy
- ICT User Agreements
- GDPR/Data Protection Policy
- Document Retention Policy
- Breach Management Policy
- Asset Management Recording Policy
- Disaster Recovery/Business Continuity Planning and Risk Register.
- Safeguarding and Child Protection Policy

6. Agreement Form

- I agree to abide by all the points contained in this guidance
- I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible ICT user'.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

Signature

Date

Full Name (printed)

Position / Role