THE CHARTER SCHOOLS
EDUCATIONAL TRUST

Email usage policy

The Charter Schools Educational Trust

Author	**S Varcoe DPO**	**Date: November 2021**	
Approved by:	**C Buchanan CEO**		
Last reviewed on:	**09/12/22**	**Next review Date:**	**09/12/25**
VERSION: 1			

Contents

Introduction

The Charter Schools Educational Trust (referred to as "The Trust) and its schools, understand that computer technology is an essential resource for supporting teaching and learning, and the general operation of the schools and the Trust. Whilst the Trust recognises the importance of promoting the use of computer technology throughout the curriculum and wider operational management, we also understand the need for safe internet access and appropriate use.

FACTS:

- **Email use is the greatest risk in terms of data breaches across the education system including emailing personal data to the incorrect recipient or failure to BCC**
- **Cyber attacks, including ransomware and phishing attacks via email come second**
- **Email inboxes used as data storage create issues around data protection especially when subject access requests are raised**

The Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff, and should be read alongside the following policies:

- TCSET Data Protection Policy
- TCSET Mobile Device and Remote working Policy
- School Acceptable use of internet and e-safety policies
- TCSET Records management policy
- TCSET Staff Code of Conduct

The Trust is committed to providing a safe learning and teaching environment for all pupils and staff and has implemented controls to reduce any harmful risks.

This policy will be reviewed every 12 months or as necessary to reflect best practice, or amendments made to legislation.

1. Email usage and retention policy

Email is a universal electronic communication system. Email is about person to person communications, but the outcome of an email exchange can have a much wider significance. Of all data breached reported to the ICO last year, breaches from the education system were second only to those from healthcare, and breaches from the incorrect use of email were the biggest single category of reported breach from the education sector.

All emails held at The Trust and all/any of its schools are legally discoverable following a request under the General Data Protection Regulation (GDPR) or the Freedom of Information Act (FOI) and may be cited as evidence in legal proceedings.

Recent legislation such as the Data Protection Act 2018 and Freedom of Information Act has highlighted that it is timely to adopt more formal policies for email retention.

There are key situations where an obligation to retain emails arises: Under Freedom of Information law – The Freedom of Information Act, section 77, contains an offence of altering, defacing, blocking, erasing, destroying and concealing any records held by a public authority with the intention of preventing the disclosure of records in compliance with a FOI access request or a GDPR access request. If emails are kept for longer than is required this causes potential problems in the amount of data that can must be shared in some subject access requests or Fredom of Information requests.

The Trust will retain only personal data that is appropriate for the function of the organisation. This will ensure The Trust meets its Data Protection Act obligations set out in law.

This document sets out policy that The Trust and all its schools will follow to ensure email data is not kept longer than needed, ensuring The Trust meets its legal obligations and endeavours to safeguard business critical information.

It will also set out best practice guidelines for all employees for the use of email.

2. Email usage

The use of the Trust and its schools email facilities shall indicate acceptance of this Email Policy.

Each Trust school provides email to assist employees in the performance of their jobs, and pupils with their learning objectives. Staff will only use the approved email accounts that have been provided to them for school/Trust business and will not use personal email accounts to send and receive personal data or information related to their work in school.

Whilst its use should be primarily for official Trust or school business, incidental and occasional personal use of email shall be permitted, on the understanding that:

- Personal messages shall be treated the same as any other message
- Personal use of the email system shall never impact on the normal traffic flow of business related email
- The Trust and its schools shall reserve the right to purge identifiable personal email to preserve the integrity of the email systems.

No employee or pupil shall send, forward or receive emails that in any way may be interpreted as insulting, disruptive or offensive by any other person, or company. Examples of prohibited material include but are not limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files
- Unwelcome propositions
- Profanity, obscenity, slander or libel
- Ethnic, religious or racial slurs
- Political beliefs or commentary

- Any message which could be viewed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs.

The Trust owns the e-mail systems used by the schools which means that all email traffic, both sent and received, including attachments, shall be monitored and reviewed and any action deemed appropriate shall be taken. This means that nothing should be taken to be private, even if marked as “private” and/or “confidential” or with any similar wording.

This monitoring will make sure that this policy is effective and that users of the email system are abiding by its content. The monitoring is also to ensure that the Trust school email systems are working properly.

All teaching staff, administrative staff and pupils shall ensure compliance with relevant legislation.

- Internal email and other internal information shall not be forwarded to destinations outside of the Trust’s schools domains without the authority of the appropriate individual.
- Where any member of staff has given access to a mailbox to another member of staff (for example to their PA or administrator or a group of staff members), this will be clearly communicated to those who may wish to send communications to that mailbox via the school/trust website. This will include details of what the mailbox’s primary use is and which staff members will be monitoring it.
- Email users shall not forward chain letters either internally or externally.This includes those purporting to be for charity or other good causes as well as those promising wealth or other personal gain. Virus warnings shall come under the same exclusion, as the majority of these are false.
- Email users will not open any emails or links within that email or attachments if there is any doubt as to its source or concerns that it may be a scam email. The message might be from a company you don’t normally receive communications from, or someone you do not know. You may just have a hunch. If you are suspicious, you should report it. You should refer to your ICT support team to check the validity of such messages but shall not forward these messages to anyone inside or outside the Trust or any of its schools under any circumstances.
- Emails of any kind shall not be sent to multiple external organisations without the appropriate approval of a senior staff member or teacher. This may be considered as ‘spamming’ which is an illegal activity in some countries.
- The individual logged in at a computer shall be considered to be the author of any messages sent from that computer. It is therefore important that all ICT users shall log off or lock their computers when away from their desks; under no circumstances should a user send a message from somebody else’s account.
- Email addresses should not be disclosed unnecessarily. Information provided in surveys or other questionnaires may lead to risks such as receiving unwanted junk messages.
- Email shall not be used to send large attached files, unless very urgent and authorised by ICT. Many email systems will not accept large files. Other media shall be used, such as shared drives, when sending large amounts of data.
- Emails and attachments shall not be opened unless they are from a known source. Caution shall also be exercised even if attachments are received from a known source but are unexpected.
- The facility to automatically forward emails shall not be used to forward messages to personal email accounts. The school ICT support will be able to provide solutions for securely accessing the Trust/school email system when working away from the office. Advice shall be sought from ICT support if remote access is required.

- All users are reminded to think before sending and email. Email is effectively a database and it may be more appropriate to phone or meet someone before sending an email. Please see APPENDIX 1 for our guidance on good email useage.

3. Email Storage

Please note, mailbox owners are responsible for managing their own mailbox and the data held within. If you have concerns regarding the storage or deletion of an email, please contact your local Data Protection Champion (DPC) or the Trust Data Protection Officer (DPO) for guidance.

- Emails must be deleted no later than 12 months after being received unless required for business-critical needs or for other operational purposes.
- Emails content MUST be assessed and stored in line with the Trust Data Protection Policy and Records Management Policy.
- Deleted emails. Where a “Recycle Bin” is in use email held within the Recycle bin will be stored for a maximum of 10 calendar days before being automatically and permanently deleted.
- Devices used to store emails MUST meet the TCSET Mobile Device and Remote working Policy. These devices MUST not be shared in a manner that allows unauthorised access to Trust and school emails. Please see E-Security for more information.
- When sending emails only include users that are required and where the content is appropriate for those users. Emails must NOT be sent to recipients where the content is not appropriate or where the is no beneficial need or business requirement.
- When forwarding emails, you MUST ensure that the recipients are correct, and the content is appropriate for the recipient including any historical content contained within the mail. If in doubt historical content in the email chain should be deleted or a new email should be created to share the required information, thereby breaking the chain.
- If you believe you receive an email in error, you MUST contact the sender only immediately to confirm. Under no circumstances should this email be shown or forwarded to any recipient until confirmation has been provided from the original sender. In the event of the email being sent in error the recipient MUST delete the email immediately from all devices and the DPO must be notified.
- If you believe you have sent an email to an incorrect recipient they you must if possible recall the offending email, then contact the appropriate recipients informing them of the error and requesting that it be removed immediately. You MUST also contact the DPO and inform them of the error.

APPENDIX 1 – Effective use of email

1. Think before you send that email? Can you walk down the corridor and speak to someone or pick up the phone instead? If it's possible to have the conversation over the phone rather than emailing it, It would be better if there is work where you need to hit a deadline or explain something in more detail that requires an explanation in more detail which can be more effective than going back and forth on an email chain.
2. If you do need to send an email, please ensure careful use of autofill for email recipients – this is one of the most common causes of accidental data breaches when sensitive information is sent to the wrong person. Check the recipients before pressing send. You can use settings in Outlook or GMail to delay and if necessary undo the sending of any email as a final failsafe. Speak your IT team about how to change these settings if you need help.
3. Always use BCC if emailing multiple recipients outside the organisation – for example groups of parents. Sharing an individual's email address without their permission is a data breach. If you need to email a group of parents, it is advisable to always use the school communications system (e.g BROMCOM) rather than your individual school email account.
4. Avoid 'Reply All' unless every recipient on the email needs to see your reply – if you have a question for the sender just email the sender – or better still phone them! By replying to people who don't need to be copied, it'll only clog up their inbox – and potentially yours if they reply to something you don't need them to.
5. Include a signature block: The school should have a standard signature template that all staff should adopt. Generally, this would state your full name, job title, the school/Trust name, and your contact information, including a phone number. Ideally it should also include the school/trust branding and a link to the school/Trust website. See example email signature below:

Shalene Varcoe
Head of Trust Governance and Compliance
The Charter Schools Educational Trust
E: SVarcoe@tcset.org.uk
T: 020 3873 2290 ext: 3061
www.tcset.org.uk

The Charter Schools Educational Trust respects the work life balance of its staff. If this email has been sent outside of normal working hours there is no expectation for you to provide an immediate response.

THE CHARTER SCHOOLS EDUCATIONAL TRUST

The Charter Schools Educational Trust is a company limited by guarantee and registered in England and Wales. Company No 07338707 Registered Office: Jarvis Road, London SE22 8RB

6. Include a Clear Subject Matter: A short title with the key subject matter will likely be more effective than a full sentence. If it's for review/action, put that at the beginning of the subject line to make it more eye-catching. E.g. "Please respond" "For review" or "Action requested". People often decide whether to open an email based on the subject line.
7. Think about where your email could end up: Never use inappropriate language in a work email. The reality is that your email will remain on the server long after you have deleted it. Only use shorthand if you know your recipients: If you're writing to your own team about a matter that you've been discussing, then you can write short emails with a list of bullet points.
8. Be wary of using humour or colloquialism as this may be understood differently by different cultures. Be aware of funny sayings or colloquialisms. Instead, keep your emails to the point and as clear as possible. Humor can easily get lost in translation without the right tone or facial expressions. In a professional exchange, it's better to leave humor out of emails unless you know the recipient well. Also, something that you think is funny might not be funny to someone else. This is especially important when communicating with and about colleagues, parents or pupils
"Something perceived as funny when spoken may come across very differently when written. When in doubt, leave it out."
9. Keeping emails you don't need, 'just in case' - The more personal data you hold, the more storage space and security measures you need to keep it safe – which will cost time, as well as money. Your mailbox is a database. For example, it'll take you longer to deal with a request for information if you need to search through thousands of old emails, rather than a few hundred current ones. In addition, data protection legislation says that personal information shouldn't be kept for longer than needed.
10. Save any emails or attachments that may need to be retained to your school drive. Ideally you should not have anything in your inbox unless it still requires follow up or action.
11. Do not use email chains to carry out conversations – Think about where your email could end up. This is particularly important when it come to discussing sensitive issues involving individuals. Mailboxes are databases that can be searched if any individual submits a subject access request to the Trust/School or we receive a Freedom of Information request. If in doubt have a face-to-face or phone conversation. Any agreed actions can be confirmed in an email or in a meeting report.
12. Try to minimise the time you spend on emails to distinct parts of the day – for example first thing in the morning, lunchtime or at the end of the day. Use this time to respond, action, save or delete emails so that your inbox does not get out of control!
13. **FINALLY - Never open links or attachments in any suspicious looking email – if in doubt report to your line manager and IT support team immediately.**

    42% of reported cyber breaches in education reported to the ICO in Q2 2021 were as a result of email Phishing attacks.

    Top tips for spotting a suspicious email:

    - Is the email addressed to you by name, or does it refer to 'valued customer', or 'friend' or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
    - Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?
    - Check the domain name on the sender's email address – no legitimate company will send emails that end in @gmail.com. The best way to check an organisation's domain name is to type the company's name into a search engine.

- Your bank or any other official source should never ask you to supply personal information in an email. If you need to check, call them directly.
- If it sounds too good to be true, it probably is. It's most unlikely that someone will offer you designer trainers for £10, or codes to access films for free.