

Mobile Phone Usage Policy

Version No	V1.0
Approved on	26th March 2026
Previous Version No	N/A New Policy
Approved by	Board of Trustees

Change Record

Version No	Date of Change:	Changed By:	Comments:
V1.0	11/03/2026	SR	New policy
V1.1	02/07/2026	SR	SLT

Date of next review: 15/07/27

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

Under the GDPR and Data Protection Act 2018, individuals have the right to access and receive a copy of their personal data and other supplementary information. This is known as a Subject Access Request, also known as SAR. Essex & Thames Education strictly adheres to data protection principles and this policy outlines how we meet our obligations under the right of access for data subjects.

Personal Mobile Phones

What must I do?

1. **You must not** use your personal mobile phone to access Essex & Thames (“the Charity”, “SCITT”) data;
2. **You must not** use your personal mobile phone to access Essex & Thames emails;
3. **You must not** use your personal mobile phone to use any apps required for your work, with the exception of the following which are outside the scope for Cyber Essentials: 8x8 and authenticator apps;
4. **You must use** your 8x8 app to make and receive work related calls.

Why must I do it?

Essex & Thames Education must be approved by Cyber Essentials in order to deliver the Apprenticeship route into teaching. This policy must be followed in full to ensure compliance.

1. Only SCITT provided mobile devices are approved for accessing the Charity data. This is to ensure that the risk of unauthorised access is reduced as far as possible;
2. Only SCITT provided mobile devices are approved for accessing the Charity emails. This is to ensure that the risk of unauthorised access is reduced as far as possible;
3. Only SCITT provided mobile devices are approved for access to the full set of apps required for mobile phone use. Most staff will not need to access the full set of apps in the course of their work. Those authorised to do so will be provided with a SCITT mobile device. The 8x8 and authenticator apps fall outside the scope of Cyber Essentials and are approved for use on personal devices;
4. Using the 8x8 app provides privacy to members of the team taking and receiving calls and protect personal information.

How must I do it?

1. Do not use your personal phone to access any Charity data;
2. Do not use your personal phone to access the Charity’s emails;
3. Do not use any apps other than the permitted apps to access any Charity data. The permitted apps are: 8x8 and authentication apps;
4. Ensure that you use the 8x8 to make and receive work calls. Do not provide your personal phone number in your email footer or by any other means.

SCITT Mobile Phones

What must I do?

1. **You must** only use your SCITT ("the Charity", Essex & Thames Education) issued mobile to access the Charity emails, you may not use your personal devices;
2. **You must** only use your SCITT issued mobile to access the Charity Google Workspace, you may not use your personal devices;
3. **You must** not download any documents or files to your SCITT issued mobile phone;
4. **You must not** use your SCITT mobile phone for personal use;
5. **You must** only download SCITT approved apps to your mobile phone
6. **You must** ensure that you have Malwarebytes Threatdown installed on your SCITT issued mobile phone;
7. **You must** ensure that your SCITT issued mobile phone is secured with a 6 digit lock code, this must not be your date of birth;
8. **You must** ensure that your SCITT issued mobile phone is set to a screen lock time of one minute;
9. **You must** make all possible efforts to keep your SCITT issued mobile phone secure at all times;
10. **You must** log out of all SCITT emails and systems if you will not be using your SCITT issued mobile phone for any extended period of time;
11. **You must** report the loss of your SCITT mobile phone immediately to sue@ete.org.uk;
12. **You must** return your SCITT mobile phone on leaving your employment at the Charity or as requested by the SLT team;
13. **You must not** sell, exchange or dispose your SCITT issued mobile phone without the express permission of the Charity;
14. **You must** keep the operating system up to date at all times;
15. **You must** update all apps on a regular basis.

Why must I do it?

Essex & Thames Education must be approved by Cyber Essentials in order to deliver the Apprenticeship route into teaching. This policy must be followed in full to ensure compliance.

1. You must only use your SCITT issued mobile phone to ensure the security of the Charity's data;
2. As above;
3. The Google Workspace is encrypted and accessing data only via the Workspace adds an extra layer of security to the data. Data downloaded to devices can be recovered using software available to criminals;
4. You must only use your SCITT issued mobile phone for the Charity's purposes to prevent accidental sharing of data and to prevent the risk of Malware attacks;
5. The apps approved by the Charity have been assessed for risk and are those that are essential to carry out your role. You must not install any other apps without express permission. A DPIA will need to be undertaken for all new apps, please email sue@ete.org.uk to start this process;
6. Malwarebytes provides up to date and effective protection against Malware and cyber attacks;
7. A six digit pin vastly increases the security of your device, four digit pins are not approved;
8. A short lock screen time ensures that if your device were to be stolen that there is a minimal risk to unauthorised access to your device;
9. Loss of your SCITT issued mobile phone would present a significant data risk to the Charity, all efforts should be made to keep your device safe;

10. If you will not be using your SCITT issued mobile device for an extended period, for example, a holiday, you must logout of your SCITT emails, drive and any apps installed for security purposes;
11. You must report the loss of your SCITT issued mobile device without delay in order that this can be logged on the ROPA and assistance given to securing your accounts;
12. All devices remain the property of the Charity and must be returned on request to ensure that all data is removed from the device;
13. As above
14. The Cyber Essentials certification is only valid if all operating systems are kept up to date;
15. The Cyber Essentials certification is only valid if all installed apps are kept up to date.

How must I do it?

1. You must have your own device for your personal use and keep this separate from your SCITT issued mobile device;
2. As above
3. Only access the Charity data via the installed apps;
4. Ensure that you have a separate device for your personal use;
5. A list of approved apps are shown at the end of this policy. Please email sue@ete.org.uk if you would like to use an app that is not shown on the list so that a DPIA can be arranged before approval;
6. You will be provided with a code to install Malwarebytes, please ensure that this is installed without delay. If you have any problems with installation, please email sue@ete.org.uk
7. You must set your device to a six digit pin to provide the highest level of security, please check your manufacturers instructions on how to set a new pin. This must not be your date of birth;
8. You must set your device to a lock screen time of one minute, please check your manufacturers instructions on how to set a lock screen time;
9. You must be aware of the location of your SCITT issued device at all times. Keep your device as secure as possible by keeping it out of sight when not in use;
10. If you will be away for an extended period, for example, on holiday, please secure your device by logging out of all systems and apps and keep your device in a secure place until your return;
11. If your device is lost or stolen, please email sue@ete.org.uk without delay;
12. If you leave your employment, please email sue@ete.org.uk to arrange the safe return of your device;
13. Do not exchange, sell or dispose of your device without the express permission of the Charity. If the device is at the end of its useful life, it may be possible for you to purchase the device, however, this would have to be approved by the board of Trustees;
14. You must regularly check your device for update alerts and install these as soon as they are released;
15. You must regularly open the app store and update any apps that have updates issued without delay.

Approved Apps List

Google Drive
Gmail
Zoom
MS Teams

Timetastic
Google Docs
Google Calendar
8 x 8

Google Sheets
Google Slides
Google Classroom
Doodle

Google Meet
Chrome
Canva

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Sue Rudgley (DPO - sue@ete.org.uk)

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Further Information

For further reading and information, please visit the ICO website page for Subject Access Requests by following the link below:
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/subject-access-requests/a-guide-to-subject-access/>

Key Contacts

Data Protection Officer (DPO):

Sue Rudgley

sue@ete.org.uk

01268 988580 ext 1000

Senior Information Risk Officer (SIRO)

Jo Palmer-Tweed

jo@ete.org.uk

07530184210

Information Commissioner's Office (ICO)

<https://ico.org.uk/global/contact-us/contact-us-public/>