The Charter Schools Educational Trust
Transforming lives through the power of inclusive education

The Charter Schools Educational Trust

Mobile and Remote Working Policy

Author: Shalene Varcoe - DPO

Date: March 13, 2020

Approved: C Buchanan CEO **Review date**: March 2022

Contents

1. Introduction

This Mobile and Remote Working Policy is a sub-policy of the Data Protection Policy and sets out the additional principles, expectations and requirements relating to the use of mobile computing devices and other computing devices which are not located on school premises when these devices are used to access school information assets with a classification of confidential or above.

While recognising the benefits to the Schools and their staff of permitting the use of mobile devices and working away from the main school sites, the Trust also needs to consider the unique information security challenges and risks which will necessarily result from adopting these permissive approaches. In particular, the Trust must ensure that any processing of personal data remains compliant with the Data Protection Act.

Under the Data Protection Act, personal data can only be processed off school site if all of the following conditions are met:

- the personal data is used or processed to carry out the duties of the member of staff and for no other purpose;
- the processing is carried out only for legitimate purposes related to school business;
- the data protection principles are followed strictly;
- adequate security is maintained to protect against the loss or theft of the personal data.

Any breach of these responsibilities could lead to disciplinary action and the School/Trust receiving a fine of up to £500,000 from the Information Commissioner.

2. Definition

A mobile computing device is defined to be a portable computing or telecommunications device which can be used to store or process information.

Examples include laptops, netbooks, smartphones, tablets, USB sticks, external or removable disc drives, flash/memory cards and wearable devices.

3. Scope

This policy applies to all staff at each of the Trust schools (including permanent and temporary staff, and those employed to work at the schools via third party suppliers) and covers all mobile computing devices whether personally owned, supplied by the schools or provided by a third party.

Personally owned, school owned or third party provided non-mobile computers (for example desktops) which are used outside of school premises are also within scope.

4. General guidance for remote working.

Agile working and the use of personal devices increases the security risks around personal data. The Trust and its schools remains responsible for ensuring that any personal data that is handled away from school is processed in accordance with GDPR. In particular, Principle 6 of the GDPR requires the Trust to take appropriate technical and organisational measures to protect personal data.

If you are working remotely, staff remain responsible for handling personal data securely even when working away from school. The ICO would expect any device used to process personal data (whether school issued or personal) to be encrypted with a strong password. Family members and friends should not be able to see or access any personal data held electronically or manually.

Non-school owned computing equipment must only be used in accordance with this policy to ensure that appropriate security measures are in place for such devices. Accessing the School's assets remotely from a personally owned computer/device is acceptable as this is simply accessing the School's network remotely and no information should be retained on your computer/device.

The Trust uses cloud based systems and it is very important when using remote access, to ensure that no personal information or data is copied or saved locally to any end user computer/device.

Do not send documents including personal data to a private, non-school email address to access these documents remotely – storing personal data with an unauthorised third party (without consent) is likely to be a breach of the Data Protection Act. Similarly, storing personal data with third party cloud storage providers that do not meet security standards acceptable to the School is not permitted.

Also ensure any backup devices used to store personal data are fully encrypted and physically secure at all times.

Alternatives
Always consider how necessary it is to take personal data off School premises, taking the following into account:

- Rather than storing personal data on a mobile storage device, could you use the School's remote access provision to access the information remotely? This would remove the need for any personal data to be carried off premises and reduce the risk to the School. If you have trouble accessing Staff Desktop remotely, please speak to IT Support.
- If you need to use hard copy documents containing personal data, do you need a whole file or could you limit the personal data you take off premises?
- Could the personal data be anonymised before being taken off premises?
- Can you ensure that no sensitive personal data is taken off premises? A breach of the Data Protection Act will be deemed more serious if it involves sensitive personal data.

Security measures
If taking personal data off School premises, it is the responsibility of individual members of staff to ensure that they have adequate security measures in place to protect against loss or theft.

For hard copy personal data, you should consider -

Security of information when in transit:

- Are you using public transport? If so, there is a greater risk of loss or theft
- If working on bus/train, do other passengers have sight of your work?
- If driving, is the information safe if your car were to be stolen or broken in to?
- If you are hand delivering personal data, ensure it is handed to the recipient or put through the letterbox - do not leave a package in a porch or similar.

Security of information at home:

- Where are you working at home?
- Have you taken precautions against burglary and unauthorised access by family members?
- Do you have a "safe space" for storing personal data?
- Can you lock personal data away?

We advise that hard copy personal data is not taken off school premises unless completely necessary.

5. Personally owned devices

Whilst the Trust does not require its staff to use their own personal devices for work purposes, it is recognised that this is often convenient and such use is permitted subject to the following requirements and guidelines.

Users must at all times give due consideration to the risks of using personal devices to access school information and in particular, information classified as confidential or sensitive:

- The device must run a current version of its operating system. A current version is defined to be one for which security updates continue to be produced and made available to the device.
- Mobile devices must be encrypted.
- An appropriate passcode/password must be set for all accounts, which give access to the device.
- A password protected screen saver/screen lock must be configured.
- The device must be configured to "auto lock" after a period of inactivity (no more than 5 minutes).
- Devices must remain up to date with security patches both for the device's operating system and its applications.
- Devices which are at risk of malware infection must run anti-virus software.
- All devices must be disposed of securely.
- The loss or theft of a device that has been used to access school information must be reported to IT Support and the Data Protection Officer.
- Any use of personal devices by others (family or friends) must be controlled in such a way as to ensure that these others do not have access to school information assets.

In addition to the above requirements, the following recommendations will help further reduce risk:

- Consider configuring the device to "auto-wipe" to protect against brute force password attacks where this facility is available.
- Consider implementing remote lock/erase/locate features where these facilities are available.
- Do not undermine the security of the device (e.g. by "jail breaking" or "rooting" a smartphone).

- Do not leave mobile devices unattended where there is a significant risk of theft.
- Be aware of your surroundings and protect yourself against "shoulder surfing".
- Minimise the amount of restricted data stored on the device and avoid storing any data classified as strictly confidential.
- Access restricted information assets via the School's specific remote access services wherever possible rather than transferring the information directly to a device.
- Be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device **not to connect** automatically to unknown networks.
- If a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.
- Reduce the risk of inadvertently breaching the Data Protection Act by ensuring that all data subject to the Act which is stored on the device is removed before taking the device to a country outside of the European Economic Area (or the few other countries deemed to have adequate levels of protection).

6. School owned devices

The Schools may at times provide computing devices to some of their staff. When they do, it will supply devices which are appropriately configured so as to ensure that they are as effectively managed as devices which remain within the office environment. Devices supplied by the Schools must meet the minimum security requirements listed above for personally owned devices.

In addition, the following are required:

- Non- staff members of the School (including family and friends) must not make any use of the supplied devices.
- No unauthorised changes may be made to the supplied devices.
- All devices supplied must be returned to the School when they are no longer required or prior to the recipient leaving the School.

Staff should also follow the additional recommendations listed above for personally owned devices.

7. Third party devices

In general, staff should not use third party devices to access restricted school information assets. This includes devices in public libraries, hotels and cyber cafes etc.

8. Reporting losses

All staff members of the Trust's Schools have a duty to report the loss, suspected loss, unauthorised disclosure or suspected unauthorised disclosure of any school information asset to the Data Protection Officer, svarcoe@tcset.org.uk

Further guidance on the Trust Data protection policies can be found at:

https://www.tcset.org.uk/page/?title=Policies&pid=12