FRIARS MULTI ACADEMY TRUST

Mobile Device Policy

NON-STATUTORY POLICY

Reviewed:	October 2019
Reviewed by Chair of LGB:	December 2019
Presented to Local Governing Body:	March 2020
Next review date by LGB:	Autumn 2022
Policy Created by:	Network Manager/Operations Manager

Glossary

The term **'School'** is used as standard to mean the educational establishment that is adopting this policy.

The term '**Headteacher'** is used to refer to the person with overall day-to-day responsibility of the **School.**

Directors are the Trustees of the Board.

The term **LGB** is the Local Governing Body**.**

Mobile devices such as laptops, mobile phones, iPads and external storage and compute devices pose a particularly high security risk, primarily because they are vulnerable to theft and loss. Their material value is of secondary concern when compared to the potential cost of losing or compromising confidential, personal and/or sensitive data (student data for example).

School mobile devices (those owned by the Trust) are purchased with the full consultation of IT Support and so technical measures can be taken to ensure that the data on those devices is secured. Devices purchased by individual end users and brought into the School have not had the same input and therefore implementation of security on those devices is made much more difficult – not least due to the diversity of devices that exist and are used on a daily basis. Most end users fail to implement adequate security on their devices without specialist help.

Security controls should be appropriate for the level of information the device will carry.

Physical security – all mobile devices

1. Mobile devices should not be left unattended and, where possible, must be physically locked away or secured.
2. Mobile devices should be transported using the proper carry holders, cases, and/or in hand luggage at all times.
3. Mobile devices should be marked with an asset tag and serial numbers recorded.
4. A password/pin should be enabled on all devices.

General – all mobile devices

1. Mobile devices, in order to access the network, must comply with network access policies and at the least show the installation of a recognised and updated anti-virus package and any relevant operating system patches.
2. All mobile devices used to store and transmit personal or Trust data, the loss of which could cause damage or personal distress to individuals and loss of data to the School/school, must be encrypted using AES 256-bit encryption methods (the IT Support department use Bitlocker encryption as standard).
3. Passwords must not be stored within email clients, browsers, login scripts or cloud accounts used to hold data of any kind.
4. Mobile devices that contain or access personal/sensitive information, or have been used to access personal or sensitive information in the past, must be processed to ensure all data is permanently removed in a manner that prevents recovery before their disposal or transfer to another user. Deleting files and/or reformatting a device is insufficient to prevent recovery of data by a third party.
5. In the event that a mobile device is lost or stolen, users should refer to the *Trust Data Loss Procedure* and make a formal notification as quickly as possible.

6. Appropriate backup of mobile devices should be undertaken on encrypted backup medium using no less than AES 256-bit encryption.

Laptops

The following steps should be taken to secure data, in increasing order of effectiveness and depending on the sensitivity of data stored on the laptop:

1. Access to the BIOS of the device should be protected using an adequately strong password set by the IT Support department. This prevents casual access to data stored on the device, but data can still be read from the hard disk if it is removed and installed on another system.
2. Individual documents can be secured with document-level encryption (saving them with a password protection option).
3. Individual folders can and should be protected using NTFS folder-level encryption (Windows only). The Windows Encrypted File System (EFS) has provision for creating a recovery key for use in corporate environments.
4. Sensitive data can be stored within a container file that can be mounted as a virtual disk drive.
5. Whole disk encryption (AES 256 recommended) must be implemented for laptops that personal and/or sensitive data are stored on. All Trust laptops should have whole disk encryption enabled as standard. With this mechanism, the operating system and data are encrypted so that the disk is inaccessible even if removed from the device.
6. All staff handling medical data for staff and students should not export data except where clear information sharing protocols have been set and appropriate permissions secured.
7. Security cables such as Kensington Locks should be used to secure laptops when they are used in open access areas and offices.

Smartphones

1. All Trust owned smartphones should be password protected.
2. Android devices owned by the Trust should be encrypted using system-level encryption offered through the operating system.
3. Smartphones not owned by the Trust should not be used to store, transmit or otherwise offload data owned by the Trust in any way.

Portable Storage devices (USB memory sticks and hard disks)

Sensitive and identifiable personal data must always be encrypted. Many devices are supplied with proprietary encryption mechanisms that are easy to configure and use. The recommended encryption standard should meat FIPS 140-2 compliancy at the least and AES 256 bit encryption is recommended. Devices that do not carry their own encryption software offering 256-bit AES encryption can be secured using Bitlocker drive encryption services built into Windows 10.

Cloud Services (Office 365)

All Trust staff have access to Office 365 and associated services, including and not limited to:

1. Exchange email services
2. Cloud storage (OneDrive Business)
3. Sharepoint Online
4. Office for web

Risks

As more staff use cloud storage services access to work becomes more convenient and flexible: it is possible to use many different devices to work from, but when employed within a work context such services introduce risk to the security, privacy, copyright and retention of data.

Main risks when using cloud services are:

- The Trust cannot guarantee the quality of access to data stored, the access controls or security of the storage facility.
- The location where data is stored cannot be guaranteed – even though in general Microsoft aim to keep all EEA data local to that region. Storing data outside the EEA may mean that privacy laws are different.
- There is a risk of loss of data if a member of staff that the data belongs to becomes ill or for other reasons leaves employment of the Trust and access to the account is required.
- There is no liability on the part of Microsoft for any loss of data should their servers suffer breakdown or other damage.
- Using cloud storage clients to synchronise files between work and personal devices could result in sensitive information being held inappropriately on personal – *and unsecured* – equipment.
- If cloud providers suffer financial loss or need to scale down or close their cloud provision, staff will lose access to their files.
- Staff may encounter difficulties accessing their online account if the provider, ISP or School networks, suffer outages affecting the internet and its use.

Policy

1. Trust staff must not use cloud storage to store files containing information about individuals or other sensitive information. There are exceptions to this policy: for example, where collaboration is required with other agencies or internally and no other secure mechanism can be utilised. Exceptions should be approved by the DPO and Senior Leadership and recorded. All information in Microsoft OneDrive for Business and all communications across email using TLS 1.2 transport security are encrypted. However, additional file level encryption must be used if collaborating internally and externally using the cloud technologies available.
2. Cloud storage should not be used for *long-term* retention of School documents or files – even if those files are used for non-sensitive information. SharePoint and shared network drives should be used in those cases.
3. Trust staff using cloud storage for collaboration with others, from either within School or elsewhere, should only grant access to files and folders that are required for collaboration to take place. Access to personal data should be given on a strictly need to know basis and comply with the GDPR. If staff are unsure, they should seek the advice of the DPO.
4. The Trust does not support and will not advocate the use of cloud storage applications such as Dropbox or Google Drive; IT Staff at the Trust will only offer support for Microsoft OneDrive for Business Client if it installed internally and secured with Bitlocker Drive Encryption.
5. The Trust uses a long retention policy in Office 365 for both emails and storage, but even so, staff should not store data in these locations for extended periods of time without storing another copy on the local network (backups are regularly made of local files and folders).
6. Trust cloud accounts are secured using a local Active Directory username and password, email address, and a centralised synchronisation policy. If staff believe that any one of these is compromised, the DPO should be informed in the first instance so that remedial actions can be taken to secure the account and its data.

7. Downloading data from a cloud account to a personal device carries the potential for data loss and abuse. Staff should only download data to work with locally (on personal devices) if they have device encryption enabled, have a password on the device itself, and if the data holds no personally identifiable information.
8. Attachments sent from Office 365, or received from external sources, are scanned for malicious content. Any content deemed malicious will be moved to a quarantine area in Office 365 and the administrator will receive an alert.
9. If a member of staff will be off work for an extended period and/or other staff will require access to some of their data, they should seek help sharing the data so that only the access required is given. If a member of staff leaves the Trust, with the permission of the DPO and Senior Leadership, the IT Support Department are able to gain access to the data stored in the account for up to seven years.

This cloud policy applies to all staff, data processors, partners, suppliers and contractors and other authorised users. Any exceptions to this policy must be documented and approved.