Berwick Academy Mobile Computing Policy

The purpose of this Policy is to describe the procedures and processes in place to ensure the secure use of Berwick Academy's mobile computing devices and to protect devices and the data they may contain from unauthorised access or disclosure.

Any queries arising from this Policy or its implementation can be taken up directly with the ICT Manager.

The ICT Manager is the Owner of this document and has approved management responsibility for its development, review and evaluation.

Summary of Contents:

1. Scope

1.1 This policy applies to all staff and any other person with access to mobile devices owned by Berwick Academy.

1.2 Mobile devices in the context of this policy include laptop computers, tablets, palmtops, personal digital assistants and other handheld devices capable of processing data.

1.3 The policy should be read in conjunction with the Berwick Academy ICT Network Security Policy.

Commented [EJ1]: Change made to remove the mention of USB flash drives and external storage hard drives. This is to coincide with the change made to the Network Security Policy.

2. Introduction

2.1 This policy provides guidance and instruction on the use of mobile computing devices and all users of such equipment must read, understand and comply with its requirements.

2.2 Any mobile device being used outside the school environment – for instance when the user is moving from one location to another – is obviously at greater risk than a desktop computer in an office in a secure building.

2.3 In most cases the use of mobile devices also takes place outside the school e.g. trains, when travelling, during conferences and meetings, in other buildings or in private homes.

2.4 There are many additional risks to mobile devices that result from this way of working and users must be aware of these risks and adapt their behaviour accordingly.

3. Responsibilities

3.1 Anyone allocated a mobile device must assume an appropriate level of responsibility for the device itself and the information stored on it, in accordance with the requirements of this policy.

3.2 Upon receiving a mobile device the user must complete a Mobile Computing Device User's Agreement (at Appendix 1 of this policy) confirming compliance with all applicable paragraphs of this Mobile Computing Policy.

3.3 Upon leaving the employ of Berwick Academy or a change in roles or responsibilities which results in the user no longer requiring the mobile device, it must be returned to the ICT Support Department. Upon returning the device the Mobile Computing Device User's Agreement (at Appendix 1 of this policy) must be re-signed to release the individual from their responsibility for the device.

3.4 Users must take all reasonable steps to ensure no unauthorised persons have access to the mobile device or the data stored on it.

3.5 Users must ensure that no unlicensed or malicious software is installed on the mobile device. Programs such as MSN Messenger, Yahoo Messenger, LImewire or any other files sharing software are not permitted to be installed on the device. If any of these programs are detected ownership of the school device may be revoked**.**

3.6 Where any of the requirements of this policy are impractical or inappropriate the user is responsible for taking all reasonable steps to minimise any risks to the mobile device or the data stored on it. Advice should be sought from the ICT Manager.

3.7 The ICT Support Department will take no responsibility for data that is lost from mobile device hard drives**.**

4. Use of Mobile Devices

4.1 Users of mobile devices must be set up as users on the network and a network username and password must be required to login to and access the device in school. A separate username and password must be required to login and access the device at home.

4.2 Berwick Academy provides computer equipment such as laptops for business use, which are built for compatibility with the school's network and internet connection.

4.3 Non-Berwick Academy devices must not be used to access school network resources unless authorised by the ICT Manager.

4.4 Mobile devices issued to staff, students and other users remain the property of Berwick Academy with the user assuming temporary “custodianship” of the device.

4.5 Mobile devices must only be used in connection with authorised business use.

4.6 Under no circumstances must a mobile device be used in connection with any secondary business activities unless approved as part of any formal school scheme.

4.7 When transporting a mobile device it should always be turned off and placed securely in its carry case.

4.8 If a problem is encountered with the mobile device the ICT Support Department must be informed. If the problem compromises the security of the device it must not be used until either the problem is resolved or authorisation is provided for resumed use.

4.9 Users must notify the police, appropriate line managers and the ICT Support Department if a mobile device is stolen.

4.10 Non – school mobile devices must not be connected to the school network without the explicit agreement of the ICT Manager.

4.11 Any school owned mobile device can be recalled at any time for maintenance work.

4.12 All school mobile devices shall have web monitoring software installed (SECURUS). This software can flag up E-Safety incidents inside and outside school. The software does not monitor real time, but will only flag up categorised events.

5. Physical Security of Mobile Devices

5.1 All mobile devices must be maintained in an environment with an appropriate level of security to prevent unauthorised access to information stored on the device.

5.2 All mobile devices must be security marked (etched, UV pen, etc.) as soon as received into department or service, and then added to the appropriate inventory. The devices are also added to the asset register and an asset tag applied.

5.3 All users must ensure that they take adequate precautions to protect the equipment against theft or accidental damage at all times.

5.4 Mobile devices must be carried as hand luggage and where possible disguised when travelling.

5.5 Mobile devices must be provided with appropriate access protection, for example, passwords and/or encryption (BitLocker).

5.6 Mobile devices must not be left in an unattended vehicle at any time.

5.7 Care must be taken not to bump or drop the device and it should not be carried with objects that could damage it.

5.8 Items should not be placed on top of the device as it may not be able to support the weight.

5.9 A mobile device must not be exposed to extreme temperature changes. Cold temperatures can make components brittle and warm temperatures can cause them to melt or warp.

5.10 Care must be taken to keep liquids away from mobile devices.

.

5.11 Users should avoid touching a device's screen whenever possible.

5.12 Where appropriate only the supplied stylus should be used with touch screen devices.

5.13 Users should always ensure that peripherals such as USB devices, stylus, cables etc are kept with the mobile device.

6. Data Security When Using Mobile Devices

6.1 All data saved to the mobile device must be transferred to a network drive as soon as possible. The data must then be removed from the device as soon as practicable in order to minimise the amount of personal/confidential or corporate information potentially available to anyone who may attempt to access the mobile device. All school owned mobile devices shall be encrypted using BitLocker.

6.2 Equipment carrying important, sensitive and/or critical business information must not be left unattended.

6.3 The mobile device must not be used to store passwords, safe/door combinations, or classified, sensitive or proprietary information

6.4 Care must be taken when using mobile devices in public places, meeting rooms and other unprotected areas outside of the school's premises.

6.5 It is important when such devices are used in public places that care is taken to avoid the risk of being overlooked by unauthorised persons.

6.6 Where applicable, mobile devices should be set to enable a password protected screen saver to be activated following a period of inactivity of 15 minutes maximum.

6.7 A mobile device must not be left unattended while it is connected to a computer.

6.8 Effective and frequently updated virus protection software must be used and backup of data must be carried out regularly.

6.9 Students are not permitted to access staff laptops.

6.10 Use of school owned mobile devices must be vigilant when accessing school email at home. It is prohibited for any family member or for any person other than the authorised owner to use the device. When Email tasks are complete the owner must log out of the email application. When local device tasks are complete the user must always log out of the device and shut down in the correct manner.

6.11 A separate folder should be created within email applications and clients. All sensitive or personal identifiable data should be moved into this folder so there is separation between work related and personal information.

Appendix 1

Mobile Computing Device User's Agreement

I agree to take responsibility for the Mobile Computing Device/s and associated peripherals detailed below. I have read the Berwick Academy Mobile Computing Policy and agree to comply with its requirements.

The agreement will start when I sign this document below date of issue and will terminate when I return the device and all associated peripherals and sign the Agreement below date of return.

User Information	
Name:	Job Title:
Department:	Phone No:
E-mail:	
Equipment Information	
Make & Model:	Tag Number:
Peripherals: (List any peripherals issued with the device)	

General Data Protection Regulations 2018 The school is registered under the General Data Protection Regulations 2018 for holding personal data. The school has a duty to protect this information and to keep it up to date. The school is required to share some of the data with the Education Authority and with DfE.

Sign-off Information	
Date of issue:	Date of return:
User Signature:	User Signature:
Authorising Signature:	Authorising Signature:

Record of issued versions				
Author	**Approved date**	**Committee**	**Version**	**Status**
Eddie Jefferson	25/06/2014 25/05/2018	Full Governing Body	1.0 1.1	Final GDPR 2018 reference added
Eddie Jefferson	25/05/2019	FGP	2.0	No changes
Eddie Jefferson	12/02/2020	Full Trustee Board	2.1	No changes