Holywell Village First School

MOBILE COMPUTING POLICY

The purpose of this Policy is to describe the procedures and processes in place to ensure the secure use of the Council/school'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 Information Security Officer at john.devlin@northumberland.gov.uk

The Information Security Officer is the Owner of this document and has approved management responsibility for its development, review and evaluation.

1. Scope

1.1 This policy applies to all elected members, employees, and any other person with access to mobile devices owned by Northumberland County Council and to all mobile devices used within and on behalf of the Council.

1.2 Mobile devices in the context of this policy include laptop computers and other handheld devices capable of processing data, cameras, Smart Watches and mobile phones. It also includes storage media such as SD cards and USB/flash/mass storage drives.

1.3 The policy should be read in conjunction with the Transportation, Transfer and Sharing of Data Policy and the ICT & Information Security Policy.

1.4 Where appropriate, users of mobile computing equipment must also be familiar with the contents of the Acceptable Use Policy covering usage at home and other non-Council premises and public areas.

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 an office/school environment – for instance when the user is moving from one location to another – is obviously at greater risk than a desktop computer in a secure building.

2.3 In most cases the use of mobile devices takes place outside the Council/school e.g trains, planes or airports when travelling, during conferences/training and meetings, in other organisations' 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 Staff Device Acceptable Use Policy 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 Northumberland County Council or a change in roles or responsibilities which results in the user no longer requiring the mobile device, it must be returned to the school manager or the head teacher. Upon returning the device the Staff DeviceeAcceptable Use Policy agreement (at Appendix 1 of this policy) must be re-signed to release the individual from their responsibility for the device.

3.4 Any user intending to work at or from home with a mobile device must comply with the requirements of the Acceptable Use Policy, GDPR Policy and Online Safety Policy.

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

3.6 Users must ensure that no unlicensed or malicious software is installed on the mobile device. Further information is available in the school's Online Safety Policy.

3.7 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 Online Safety Officer.

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.

4.2 Mobile devices issued to employees, members and other users remain the property of Holywell Village First School with the user assuming temporary "custodianship" of the device.

4.3 Mobile devices must only be used in connection with authorised school use.

4.4 Under no circumstances must a mobile device be used in connection with any secondary business activities unless approved by the head teacher.

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

4.6 If a problem is encountered with the mobile device the Online Safety Officer 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.

4.7 Users must notify the police, the head teacher and the Online Safety Officer if a mobile device is stolen.

4.8 Non-school mobile devices must not be connected to the school network without the explicit agreement of Online Safety Officer.

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 When not in use all mobile devices must be retained in a secure environment. This may include a lockable store cupboard with controlled access, or lockable metal cabinets in larger alarmed offices, but again with controlled access.

5.3 All mobile devices must (as soon as received into department or service) be added to the appropriate inventory/asset register.

5.4 When mobile devices are taken from the school site, all users must ensure that they take adequate precautions to protect the equipment against theft or accidental damage at all times.

5.5 Records must be maintained which detail their laptops and iPads including type, serial number and software available, and include provision for signing out and return and copies of completed Mobile Computing Device User's Agreements (at Appendix 1 of this policy).

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

5.7 Mobile devices must be provided with appropriate access protection, for example, passwords and/or encryption.

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

5.9 Manufacturers' instructions for protecting equipment must be observed at all times, e.g. protection against exposure to strong electromagnetic fields.

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

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

5.12 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.

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

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

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

5.16 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 secure 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 school information potentially available to anyone who may attempt to access the mobile device.

6.2 In the case of personal data the level of security forms part of the school's notification to the Information Commissioner under the General Data Protection Regulation. This could be compromised if files are taken outside the workplace without appropriate measures being taken.

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

6.4 Staff who travel with a school mobile device must make regular backups of any data it contains. Advice on making backups can be obtained from Online safety Officer.

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

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

6.7 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.

6.8 A mobile device must never be left unattended in public places. Even in the workplace small hand-held devices must be stored out of view in a drawer or cupboard.

6.9 Where applicable, mobile devices should be set to enable a password protected screen saver to be activated following a period of inactivity of 5 minutes maximum.

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

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

Date formulated: 26th April 2019

Date adopted 16th May 2019

Chair of Committee: Signed:

Head teacher: Signed:

Date: 16th May 2019