Mobile Device Policy

Governors Meeting:	**18 July 2022**
Safeguarding Governor:	**Jane Owens**
Chair of Governors:	**Gail Webb**
Review:	**17 July 2023**

Contents

1. Overview

Huxley CE School embraces the positive impact and educational benefits that can be achieved through appropriate use of the internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, the s chool aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world. Employee-owned Mobile Devices (or BYOD - bring your own device) are an increasing trend within a business and school. Smartphones are the most common example, but employees also take their own tablets and laptops into the workplace. Securing mobile devices is an essential part of guarding the organisation against a variety of threats, many of which herald from the internet.

2. Scope

This policy applies to all staff. The purpose of this policy is to establish the criteria of using a personally owned or school owned smartphone, mobile computer and/or tablet device where the user has established access to the school network in order to gain access to the internet or to access school resources.

School staff may use approved personally owned and school owned mobile devices to access school resources, providing such access is compliant with the terms of this policy, and any other relevant policies.

3. User Responsibility

Staff agree to a general code of conduct that recognises the need to protect confidential data that is stored on, or accessed using, a mobile device. This code of conduct includes but is not limited to:

- Doing what is necessary to ensure the adequate physical security of the device
- Maintaining the software configuration of the device – both the operating system and the applications installed
- Preventing the storage of sensitive company data in unapproved applications on the device
- Ensuring the devices security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes
- Reporting a lost or stolen device immediately

4. Personally Owned Devices

Your personal smartphone, tablet and computer devices are not centrally managed by the school. For this reason, a support need or issue related to a personally owned device is the responsibility of the device owner. Specifically, the user is responsible for:

- Settling any service or billing disputes with the carrier
- Purchasing any required software not provided by the manufacturer or wireless carrier
- Device registration with the vendor and/or service provider
- Maintaining any necessary warranty information
- Battery replacement due to failure or loss of ability to hold a charge
- Back up all data, settings, media and applications, noting that any ‘business data’ remains the property of the school
- Installation of software updates/patches

5. Device Access Requirements

Devices provided with internet access, access to ‘business data’, and/or access to the school network, must adhere to a strong mobile device settings policy. If this is not the case, the system will reject access to the school data on the device, and/or access to the relevant resources and using the device will be in breach of this policy.

6. Security Policy Requirements

The user is responsible for securing their device to prevent sensitive data from being lost or compromised and to prevent viruses and malware from being spread. Removal of security controls is prohibited. Users are forbidden from copying sensitive data; including from email, calendar and contact applications to other applications on the device or to an unregistered personally owned device. A failure to do so could be in breach of UK GDPR regulations and any loss could result in reporting incidents to the ICO.

7. Wi-Fi Access

Users who connect to the school provided Wi-Fi networks with a personally owned device will be allowed access to the school systems and resources available via the internet only.

8. Loss, Theft or Compromise

If a device is lost or stolen, or if it is believed to have been compromised in some way, and the device contains company information (such as email, contacts etc.) the incident must be reported immediately to the Headteacher.

9. Enforcement

Any user found to have violated this policy may be subject to disciplinary action, including but not limited to:

- Account suspension
- Revocation of device access to the school network
- Data removal from the device
- Employee termination

10. Policy Review

The working of this policy will be reviewed by the school annually. As well as examining the specific review data, the policy statement will be checked for continuing relevance against any changed statutory requirements.