Mobile Technologies Policy

Our Vision

Bells Farm Primary 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, Bells Farm Primary School 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.

Scope

This policy applies to all Bells Farm staff. The purpose of this policy is to establish the criteria of using personal owned smartphone and tablet (mobile) devices where the owner has established access to the school's network.

Policy Statement

Bells Farm staff may use approved personally owned and school owned mobile devices to access the school network as necessary in the course of their normal work.

Overview

BYOD (bring your own device) is the increasing trend toward employee-owned devices within a business. Smartphones are the most common example but employees also take their own tablets, laptops and USB drives into the workplace.

User Responsibility

General

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 device's security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes
- Reporting a lost or stolen device immediately

Personally Owned Devices
The personal smartphone and tablet devices are not centrally managed by Bells Farm. 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
- Backing up all data, settings, media, and applications
- Installation of software updates/patches

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	Yes	Yes
No network access	N/A	N/A	N/A	No	N/A	No

1 Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

Emails on personal devices
Staff are allowed school email access on their personal devices however the device must adhere to a strong password policy. If this is not in place, the email system will automatically reject installation of school emails on the device.

Security Policy Requirements
The user is responsible for securing their device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread. Removal of security controls is prohibited.

Users are forbidden from copying sensitive data from email, calendar and contact applications to other applications on the device or to an unregistered personally owned device.

Wi-Fi Access to school network
Users who connect to Bells Farm Wi-Fi network with a personally owned device will be allowed access to the school systems and resources available via the Internet.

Loss, Theft or Compromise
If the device is lost or stolen, or if it is believed to have been compromised in some way, the incident must be reported immediately to Mr Baddhan or the Head Teacher.

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

Date of review June 2018

Next review July 2019