Hatfield Peverel St Andrew's Junior School

Personal Mobile Technologies Policy

Approved by:	B. Black	**Date:**	25/01/2021
Last reviewed on:			
Next review due by:	January 2022		

Our Vision

St Andrew's Junior 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, St Andrew's Junior 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.

Policy Statement

St Andrew's staff may use approved personally owned 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 the workplace. Smartphones are the most common example but employees may also use their own tablets, laptops and computers in the process of their work.

User Responsibility

General

Staff agree to the GDPR policies and ICT and internet acceptable use agreement 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 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

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. All sensitive data must be stored on an encrypted USB drive or on a secure school owned device.

Personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, while children are present. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staff room).

There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time. For instance:

For emergency contact by their child, or their child's school

In the case of acutely ill dependents or family members

The headteacher will decide on a case-by-basis whether to allow for special arrangements.

If special arrangements are not deemed necessary, school staff can use the school office number 01245 380131 as a point of emergency contact.

Safeguarding

Staff must refrain from giving their personal contact details to parents or pupils, including connecting through social media and messaging apps (see ICT & Internet Acceptable Use and Online Safety Policies).

Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil without consent from the Headteacher. If mobile phone cameras are used to photograph a pupil

or their work, the photos should be saved onto the school's own secure servers and then deleted from the device.

Using personal mobiles for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:

Emergency evacuations

Supervising off-site trips

Supervising residential visits

In these circumstances, staff will:

Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct

Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil without express permission from the headteacher

Block their personal number if making phone calls to parents, by dialling 141 before the phone number.

Wi-Fi Access to school network

Users who connect to St Andrew's 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 your personal device is lost or stolen, or if it is believed to have been compromised in some way, and has been used to access sensitive school data, the incident must be reported immediately to the Head Teacher and School Business Manager (GDPR lead).

Visitors

Visitors to the school site, whether governors, parents, volunteers or contractors, are expected to follow the guidance on mobile phone use as set out in the Mobile phone information slip for visitors (see Appendix 1 below).

Pupils

Pupils are not permitted to bring mobile phones into school.

Enforcement

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

- Confiscation of a mobile device from a child
- Account suspension
- Revocation of device access to the school network
- Data removal from the device
- Employee Termination

Monitoring and review

The school is committed to ensuring that this policy has a positive impact on pupils' education, behaviour and welfare. When reviewing the policy, the school will take into account:

Feedback from parents and pupils

Feedback from teachers

Records of behaviour and safeguarding incidents

Relevant advice from the Department for Education, the local authority or other relevant organisations

The policy will be reviewed and approved by the Headteacher, on an annual basis.

Appendix 1;

Mobile phone information slip for visitors

Use of mobile phones in our school

- Please keep your mobile phone on silent/vibrate while on the school grounds
- Please do not use phones where pupils are present. If you must use your phone, you may go to the staff room
- Do not take photos or recordings of pupils (unless it is your own child), or staff
- Do not use your phone in lessons, or when working with pupils

The school accepts no responsibility for phones that are lost, damaged or stolen while you are on the school grounds.

A full copy of our mobile phone policy is available from the school office.