



St. John's CE Primary School  
Wetley Rocks

## BYOD Policy

*“Shine like the star you are.”*

*“You are the light of the world. A town built on a hill cannot be hidden.*

*<sup>15</sup> Neither do people light a lamp and put it under a bowl, instead they put it on its stand, and it gives light to everyone in the house. In the same way, let your light shine before others, that they may see your good deeds and glorify your Father in heaven.”*

**Matthew 5:14-16**

### Our Values

**Strength:** have the strength to stand up for what is right. Be a courageous advocate.

**Hope:** to be people of hope. Have hope when times are dark and difficult. Keep positive and be resilient – there is light at the end of the tunnel.

**Individuality:** embrace and celebrate our differences. God made us all unique and this is a very special thing.

**Nature:** cherish, care for, encourage and protect everything in God’s world - including yourself.

**Excel:** fulfil your God given potential; be the best you can be. Shine like the star you are.

## **BYOD Policy**

St. John's Primary School recognises that mobile technology offers valuable benefits to staff from a teaching and learning perspective and to visitors.

The school endeavours to provide the necessary IT equipment for all staff to do their job as required, such as providing each class with a teaching computer and teaching staff with laptops, Ipads etc.

However, we understand the need for staff and visitors to use their own technology within school or to conduct school business out of school. Our school embraces this technology but requires that it is used in an acceptable and responsible way.

This policy is intended to address the use by staff members or visitors to the school of non-school owned electronic devices to access the internet via the school's internet connection or to access or store school information. Part of the policy also covers the student's use of personal devices. These devices include smart phones, tablets, laptops, wearable technology and any similar devices. If you are unsure whether your device is covered by this policy please check with the School's Office Managers (L. Beverley & N. Swift-Holdcroft), Computing Lead (R. Poynton) or Network Manager (LINK ICT). These devices are referred to as 'mobile devices' and/or 'portable devices' in this policy.

This policy is supported by the school's Acceptable Use Policy and online safety policy.

### Policy statements

#### **1. Use of mobile at the school**

Staff must only use mobile devices for personal use in the staff room, within the classroom (in the absence of pupils) or in the office.

Staff can use their mobile phones to take pictures of lesson activities to upload to the school One Drive or Facebook page. The staff must immediately delete the photos once uploaded to the appropriate destination.

Staff can carry their mobile phones when on site to be used in an emergency to call for staff or medical assistance.

Visitors to the school may use their own mobile devices in the following locations:

- In the classroom, with the permission of the teacher, in the absence of pupils.
- In the school environs, in the absence of pupils.

Staff and visitors to the school are responsible for their mobile device at all times. The school is not responsible for the loss, or theft of, or damage to the mobile device or storage media on the device (e.g. removable memory card) howsoever caused. The School Office must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

Mobile devices must be turned off when in a prohibited area and/or at a prohibited time and must not be taken into controlled assessments and/or examinations, unless special circumstances apply.

The school reserves the right to refuse staff and visitors permission to use their own mobile devices on school premises.

Students must not wear or bring into school portable devices such as apple watches that can record and take pictures of other members of the school community.

Pupils must not bring in their mobile phones to school unless previously agreed with the Head Teacher for reasons such as the child walks home or they are staying at another residence that day due to parental separation. If a device is to be brought into school, it must be kept in the office for safekeeping.

## **2. Access to the school's Internet connection via a mobile computing device.**

The school provides a wireless network that staff and visitors to the school may use to connect their mobile computing devices (**not mobile phones**) to the Internet. Access to the wireless network is at the discretion of the school, and the school may withdraw access from anyone it considers is using the network inappropriately. Visitors to the school will be able to use the guest wi fi. Login details will be given to them if this is deemed appropriate and necessary.

All supply teachers will be given a school managed laptop and guest login details to ensure that the device that they use is appropriate and has the relevant filtering and monitoring software installed.

The school cannot guarantee that the wireless network is 100% secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use the wireless network for online activities where your personal details may be compromised.

The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's wireless network. This activity is taken at the owner's own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's wireless network.

Visitors are encouraged to email any necessary items required for lessons/tasks to the teacher to reduce the risk of a virus compromising the system.

All network and internet traffic is monitored whilst connected to the school's Internet connection (see Section 4), the latter of which (at the time of writing) is provided by RM Safety Net. To this end, each device connected to the school's internet connection requires a one-time installation of RM's security certificate (see <https://www.rm.com/products/online-safety-tools/rm-safetynet/ssl-interception> for more information) and the appropriate RM proxy server setting being made in the Internet browser settings of the device. The school also now uses Securus Monitoring software to produce reports related to inappropriate use of the school Chrome books by pupils.

Finally, every device being connected to the school's internet connection must be protected by a suitable and up to date Anti Virus product (e.g. Windows Defender, MacAfee, Norton, Bullguard are examples of these products).

## **3. Access to school IT services**

School staff are permitted to connect to or access the following school IT services from their mobile devices:

- the school email system (where appropriate encryption technologies have been deployed);
- the school virtual learning environment (One-Drive, Office 365 and 'School Drives');
- official school apps.

Staff may use the systems listed above to view school information via their mobile devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases, it may be necessary for staff to download school information to their mobile devices in order to view it (for example, to view an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it. Where personal or sensitive data is used in this way devices or files MUST be password protected.

Staff must only use the IT services listed above (and any information accessed through them) for work purposes. School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to or distribution of confidential information should be reported to the school's Office Manager or Network Manager as soon as possible in line with the school's data protection policies.

Visitors using their own device on the school network will not have access to the school systems. They will only have access to a wireless network. This network has been set up by LINK ICT.

## **Staff must not send school information to their personal email accounts.**

If in any doubt the user should seek clarification and permission from the school Office Managers (L. Beverley & N. Swift-Holdcroft), Computing Lead (R. Poynton) or Network Manager (LINK ICT) before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the school systems.

## **4. Monitoring the use of mobile and portable devices**

St. John's has technology that detects and monitors the use of mobile and other electronic or communication devices, which are connected to or logged on to our wireless network or IT systems. By using a mobile device on the school's IT network, staff and visitors to the school agree to such detection and monitoring. The school's use of such technology is for the purpose of ensuring the security of its IT systems and for tracking school information.

The information that the school may monitor includes (but is not limited to) the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms (including passwords), information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content through school IT services or the school internet connection should report this to the school's Network Manager as soon as possible.

## **5. Security of staff mobile and portable devices**

Staff must take all sensible measures to prevent unauthorised access to their mobile and portable devices, including but not limited to the use of their password or pins required for any school apps. Staff should ensure that the device auto-locks if inactive for a period of time.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff are reminded to familiarise themselves with the school's online-safety and acceptable use of IT policies which set out in further detail the measures needed to ensure responsible behaviour online.

Staff must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up to date.

## **6. Compliance with Data Protection Policy and GDPR**

Staff compliance with this BYOD policy is an important part of the school's compliance with the Data Protection laws and GDPR. Staff must apply this BYOD policy consistently with the school's Data Protection and GDPR guidelines.

Where such devices are used to process data of a personal or sensitive nature appropriate passwords/pins of files or devices must be used. All such data should be backed up to the school's network, One Drive and/or Office 365 accounts and deleted from mobile devices as soon as work has been completed.

## **7. Support**

The school cannot support users' own devices but will offer advice to users in their use where practically possible.

The school takes no responsibility for supporting staff's own devices; nor has the school a responsibility for conducting annual PAT testing of personally owned device.

## **8. Compliance, Sanctions and Disciplinary Matters for staff**

Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs the school may discipline staff in line with the school's Disciplinary Procedure. Guidance will also be offered to staff to support them in complying with this policy. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and/or permission to use the device on school premises will be temporarily withdrawn. For persistent breach of this policy, the school will permanently withdraw permission to use user-owned devices in school.

## **9. Incidents, damage and Response**

The school takes any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of a mobile device should be reported to School Office in the first instance. Data protection incidents should be reported immediately to the school's Office Managers (L. Beverley & N. Swift-Holdcroft).

Visitors who bring their own mobile and/or portable devices into school do so at their own risk and we ask that all visitors make every reasonable effort to keep items safe within our school environment. The school is not responsible for any damage to a device which may occur on our property; e.g. collision, dropping, fluid damage, virus, power surge etc. Damage to mobile or portable devices should be reported immediately to the school's Office Managers (L. Beverley & N. Swift-Holdcroft).

**Created by R Poynton (ICT & Computing Co-ordinator) in conjunction with LINK ICT.**

**April 2023**