'Let all that you do be done in Love'
1 Corinthians 16:14
The example of Jesus Christ and the Good news
that He brings inspire St George's to be a place of
hope and a caring and inclusive community in which we all
Love to learn and Learn to Love.

# St George's CE Primary and Nursery School

# Mobile and Remote Working Policy

**Approved Summer term 2020**

| | |
|---|---|
| **Date Agreed:** | January 2023 |
| **Review Date:** | January 2024 |

**School's Christian values**

**Love, Compassion, Friendship, Thankfulness, Truthfulness, Forgiveness, Hope**

## 1. Introduction

1.1 The school has a duty to safeguard personal and sensitive data and equipment purchased with public funds. In addition, the technology and mobility that make portable devices so useful to employees can also make them valuable prizes for thieves.

1.2 The purpose of this protocol is to recognise the risks associated with mobile and remote working and provide employees with protocols to minimise those risks.

1.3 This protocol applies to any access or use outside school premises of:

- all school issued static and portable ICT equipment (see definitions later) and
- any information held by the school to which an employee has access because of his or her role within the school.

1.4 All ICT equipment provided to employees by the school remains the property of the school and must be returned promptly upon request for audit and inspection, to enable maintenance work to be undertaken, or for removal or disposal.

## 2. Definitions

2.1 The following terms are referenced throughout this document and are defined as follows;

**Outside school premises**: includes locations such as; an employee's home, premises of another organisation and public venues.

**Mobile Working**: Employees who sometimes have the need to work from multiple locations. Usually accompanied by portable computing equipment, employees can utilise any workspace at any given time (including home, office, other school or agency premises, etc.).

**Remote Working**: Employees who are able to access information or resources from a remote location. This usually applies to workers who perform their work from home or from an alternative office on a regular or an ad-hoc basis.

**Home Working**: Employees who are based at home or work from home for part of the working week on a regular basis. This would be an agreed arrangement and would necessitate the provision of appropriate equipment, which may be static or portable.

**Personal information**: is any information about any living individual, who could be identified from the information or any other information that is in the possession of the school. The school is legally responsible for the storage, protection and use of such information as governed by the Data Protection Act 1998.

**Special Category information**: (similar to the concept of sensitive personal data under the Data
Protection Act 1998). This data is covered by Articles 6 and 9 of the General Data Protection
Regulations. As it is more sensitive it needs more protection and consists of:-

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health;
- sex life; or
- sexual orientation.

**Protected Information** is any information which is;

(a) personal/special category (sensitive personal data); or

(b) Confidential to the school and which could have adverse consequences for the school if it was released in an uncontrolled way.

**VPN (Virtual Private Network):** refers to a secure network connection that uses the internet to transmit data. It allows employee's access to the school network out of the office from a school issued PC/laptop.

**Personal (Wi-Fi) Hotspot**: a wireless internet access point provided by a smartphone.

2.2 In this protocol the term 'portable devices' includes but is not restricted to the following:

- Laptop/slate computers;
- Personal Digital Assistants (PDA's);
- BlackBerrys/Smartphones;
- Mobile phones;
- Text pagers;
- Wireless technologies;
- Digital Cameras; and
- Storage devices including flash memory cards/USB memory sticks.

## 3. Roles and Responsibilities

3.1 All employees are responsible for the safety and security of portable devices issued to or used by them. Particular care must be taken when moving equipment between sites and storing when not in use.

3.2 Where the school provides a laptop computer to an employee, it is the responsibility of the employee to ensure that the anti-virus updates are maintained by regularly connecting the device directly to the school network. This can be done by connecting via from their classroom or office within the school building and any automatic update should be downloaded. If employees are not clear on how to check if their anti-virus files are up to date they must check with the IT support services

3.3 Employees must not install any software or connect any hardware to a school owned portable device without the prior permission of the school. However connection to the following is permitted:

- an external monitor or projector;
- equipment supplied, owned or configured by the school;
- internet connection via a home router or home broadband modem (wired or wirelessly connected)

- A printer.

3.4 Employees must not update or change the security configuration of any school ICT equipment unless advised by school ICT support services. This is to prevent potential loss of protected information or damage to a portable device.

3.5 All employees with a school issued portable device are responsible for the information held on the device. Employees must be aware of their surroundings and take appropriate measures when viewing information on a portable device to ensure it is not within view of others.

3.6 It is the responsibility of individuals to immediately report any actual or suspected breach in information security by informing their line manager and/or the Risk and Insurance Manager. Any incident where protected information is lost, leaked or put at risk must be reported as a potential security incident. Failure to do this could not only result in reputational damage, but fines could also be imposed by the ICO. The ICO can also fine individuals.

3.7 To reduce the risk of unauthorised access whilst working out of the school, protected information must only be stored on school issued portable devices if they are encrypted (e.g. laptops). Some items like digital cameras cannot be encrypted, however if the contents would be considered to be protected information, the camera (or other storage medium) must be kept securely until it can be transferred to a more secure storage format.

## 4. School ICT Equipment and Wi-Fi

4.1 To facilitate mobile working and working differently the school will, by default, issue one laptop or other alternative mobile device to those that need access to the school's systems. All equipment used to store or access any protected information must be supplied, configured and installed by the school.

4.2 Equipment supplied by the school may only be used by authorised persons. Employees must therefore ensure that the supplied equipment is not used by anyone outside the school.

4.3 ICT equipment may be used for personal purposes by employees so long as it is in accordance with Information Governance Conduct Policy and appropriate supporting policies, protocols, procedures and guidance documents. However, the school owned equipment must not be used to undertake any private business enterprise.

4.4 All faults or requests for upgrades must be made via the school office who will contact the ICT support service.

## 5. Non-School Equipment

5.1 Personal or any other non school equipment should not be used to conduct school business. This would include employees own smartphones (including iPhones), laptops, iPads/slate PCs, personal desktop computers or internet cafes. Under no circumstances should school data be stored or downloaded onto any non-school equipment, as it then becomes insecure.

5.2 School emails must not be forwarded on to a personal email account. Emails sent in these ways exit the school's network and are transmitted over an untrusted network. If an email or attachment containing protected information is sent to a personal device/email account, the contents are open to misdirection, interception and corruption and therefore this would be in breach of this protocol.

5.3 Employees must not install any school owned/licensed software onto personal equipment, unless this has been authorised. Any software purchased by the school is licensed to the school and any unauthorised use outside of the licence is likely to be a breach of copyright and could result in a prosecution.

5.4 Non-school owned portable devices including mp3 players, iPods/iPhones, cameras and USB memory sticks must not be physically connected to school owned equipment unless authorised by the school.

## 6. Physical Security and Insurance

6.1 Portable devices issued by the school are usually insured when they are inside the United Kingdom, although misuse or inadequate protection may invalidate that insurance cover. Employees must seek advice from the school before taking any school owned portable device outside the United Kingdom as the device may not be covered by the school's normal insurance against loss or theft. There is also the possibility that the device may be confiscated by Airport Security staff, which could result in having to leave them behind, or they may request to see the contents, which could result in a breach of this policy and possibly the law if the device contains protected information.

6.2 Employees should be aware of the physical security risks associated with working from a remote office or mobile working location. All protected information (including information stored on portable devices and in paper files) must not be left where it would attract the interest of an opportunist thief. Protected information must be located securely and out of sight so that visitors or family members do not have access. Unauthorised disclosure of protected information is a breach of this protocol and the law.

6.3 Council equipment and protected information must be kept safely and securely at all times. When equipment/protected information are at home, employees must:

- ensure that only the employee has access to the equipment/information;

- ensure that the equipment/information is safely and securely locked away when not being used;
- prevent access to the school equipment and protected information, by family members and visitors; and
- ensure that any telephone conversations discussing protected information cannot be overheard.

These precautions are necessary to reduce the risk of unauthorised persons listening to or viewing school information.

6.4 Employees who regularly work at home must have a suitable workstation where these issues have been considered. In order to prevent a potential breach, documents should be collected from printers as soon as they are produced and not left where they can be casually read.

## 7. Use of Information Out of the Office

7.1 All school supplied laptops (and all USB memory sticks) are encrypted and so provide a secure method in which to save information when necessary. However, whilst this is likely to prevent unauthorised access to the information, it does not protect the information against loss. Therefore, documents and files should be saved on shared drives to prevent any loss of information. Master copies of information must never be held on a portable device on anything other than a temporary basis. Once the temporary information is no longer required on the portable device it must be deleted.

7.2 It is also possible to setup folders so that they can be worked on off-line, which means there is a local copy of the data. This will allow a user to work out of the office without access to the school network. However only a limited number of folders should be made available off-line in order to avoid performance issues on the laptop. In addition, folders that contain personal data should only ever be made available off-line on a temporary basis.

7.3 All school supplied laptops are provided with software to connect to a Virtual Private Network (VPN) to allow secure access to the school Network. VPN software will NOT be installed on non-school equipment as this is a security risk.

7.4 When working out of school, employees should avoid using Wi-Fi Hotspots or free Wi-Fi connections provided by retail outlets, coffee shops and the like. Even when connected via the school's VPN, hackers could still intercept transmissions potentially revealing protected information or password and login details. Individuals are required to assess the risks based on the data they work with. Those that work with personal and sensitive data should not use such facilities. Others are permitted to use these facilities but must never give any information about their school email account or passwords. The only exception to this would be a private network that requires a password to access, for example Wi-Fi at a Local Authority building, or at a business or academic premise. Purchased connectivity at a hotel, where you are given a unique password would also be acceptable.

7.5 Some work may require physical documentation (e.g. paper files) to be removed from the school to assist with mobile and remote working. If this is the case, a booking out system should be in place. This is to ensure that your line manager or Head teacher is aware of the movement of information, as if a loss occurs they will need to provide assurance they were controlling their information adequately.

7.6 Arrangements must be made to properly dispose of any protected information used out of the school in order to prevent unauthorised access. To do this any information that would qualify as being personal or sensitive must be returned to the school office and disposed of securely or shredded.