



## St. Martin's School - Wireless Infrastructure Policy

### 1. Introduction

#### 1.1. Statement

The decision to improve the wireless infrastructure has been agreed at school level by the Headteacher and Senior Leadership Team. This policy should be used to ensure best practice implementation. This includes school mobile devices and Sixth Form 'Bring Your Own Device (BYOD)'.

#### 1.2. Aim and purpose

This policy is designed to implement the school's new wireless infrastructure, the management of school mobile devices, and allow the use of personal devices by Sixth Form Students in a way that enhances and supports teaching and learning. It also aims to protect children from harm, minimise risk to the school network and explain what constitutes acceptable use or misuse of the policy.

#### 1.3. Who it applies too

This policy applies to all staff, pupils, students and young people at the school and their parents, guardians and carers.

### 2. Policy

#### 2.1. Description

The wireless infrastructure will include the following technologies:

- All school mobile devices
- Sixth Form Laptops, netbooks, iPads and Tablets.
- All smart phones

Staff and students using mobile devices in lessons should be aware of the need to:

- Protect themselves and other students from harm online
- Understand what constitutes misuse
- Report suspected misuse immediately
- Be responsible for their own behavior (Sixth Form Students)
- Minimise risk of theft of school mobile devices (Staff)

School mobile devices

- The school takes full responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices.
- Heads of Faculty manages sets of faculty mobile devices.
- Staff are responsible for individual mobile devices
- IT Technician and Wireless Infrastructure Team will oversee these mobile devices and their management.
- Mobile devices must be counted, collected and returned by a member of staff only. No student should be responsible for collecting or returning devices.
- Devices must be locked when not in use at all times and keys returned to appropriate member of staff responsible.
- When staff are returning mobile devices they should plug them back in for charging and ensure that any work undertaken on them is cleared ready for other staff to use them.
- Mobile devices must be returned in the condition they were at the start of the session.
- Please avoid booking if they are in use the lesson before, to ensure there is sufficient charge for you to use with your class.

## Sixth Form Bring Your Own Device (BYOD)

- The school takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. Please check with your homeowner's policy regarding coverage of personal electronic devices, as many insurance policies can cover loss or damage.
- The school is not responsible for any possible device charges to your account that might be incurred during approved school-related use.

### 2.2. Permissive/non permissive

- Students and Parents/Guardians participating in BYOD must adhere to the Home School Agreement.
- The school's network filters will be applied to any device connected to the school's internet connection and any attempt to bypass the network filters is prohibited. Filtering requests should be reported to IT Technician.
- Mobile devices will be set up by IT Technician to protect the wireless infrastructure. All passwords will be kept secure with the IT Technician and not issued to users. Wireless infrastructure passwords will be changed once a term for security purposes.
- Visitor access can be obtained on request, access will be set up by IT Technician, password will not be issued to users.
- Whilst passwords will be changed routinely, they may also be changed if the security of the network is thought to be at risk
- All devices connected to the wireless network must have up to date firewall and anti virus software.
- Sixth form students wishing to connect to the BYOD wireless infrastructure must report to IT Technician. Students will not be issued with the password.
- Students may not use devices to record, transmit, or post photographic images or video of a person or persons on school site during school hours or during school activities, unless otherwise allowed by a teacher.
- Sixth Form personal devices must be charged prior to school and run on battery power while at school. Charging of devices is not permitted.
- In compliance with GDPR, all users are reminded not store personal, sensitive information on portable devices that could be accessed by others.
- Mobile devices linked to our google platform must accept / grant us the required permissions to delete / protect the account if the device is ever lost or stolen
- Mobile devices linked to our google platform must have a device password / key lock enforced

### 2.3. Compliance

Students who infringe the rules set out in this document whilst using school devices could face having their device confiscated by teachers. If the device is being used inappropriately the student must give it to a teacher if requested. Teacher reserves the right to report any infringements to an appropriate member of staff.

## 3. Key steps in the process

### 3.1. Roles and responsibilities

It is the responsibility of all students to adhere to this policy and to monitor this policy against fellow students. It is the role of all staff members to enforce this policy and to highlight any misuse to the appropriate staff members.

### 3.2. Procedures

If any student or staff does not adhere to this policy, this misuse should be reported to IT Technician and/or Senior Leadership Team where appropriate actions taken.