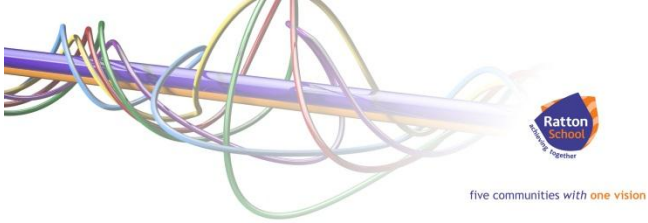


ACCEPTABLE USE	
DOCUMENT	

This policy is in addition to the e-safety data policy and should be read alongside it. The use of the phrase 'Mobile Devices / Laptops' includes:

- Student Owned Laptops
- Netbooks
- Tablet computers
- Smart Phones
- Mobile Phones
- or any other 'Internet Device' used by students.

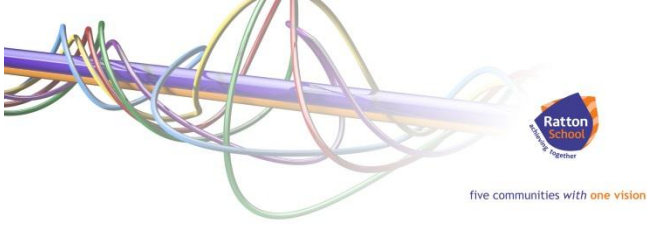
## Wireless Access

**Students should only connect personal devices to Ratton**

It should be noted that traffic travelling through the school Internet connection will be intercepted and logged. This may also apply to data sent securely (via HTTPS).

## Use of the devices

- Devices must be used solely for school based learning
- Devices can only be used to film, take photos or record sound when agreement has been sought by all parties involved including the supervising teacher / adult. Outside of lesson times permission must be sought by a member of staff and a note recorded in the student's planner. Students are reminded that all content captured must be used for educational reasons only.
- Students must first gain staff permission to avoid recording images of any students who cannot be photographed or videotaped
- The owner of the device is solely responsible for the physical security and the network security of the device.
- The owner is solely responsible and capable of setting up the device on the network and provides all necessary equipment such as battery, power supply, and connections.
- With permission of a teacher, students may charge their device in classrooms only.
- School staff will NOT provide technical support and peripheral equipment.
- Students who are not doing academic work or are creating a disruption will be asked to put the device away.
- Students should report any e-safety incidents to school staff.

ACCEPTABLE USE	
DOCUMENT	

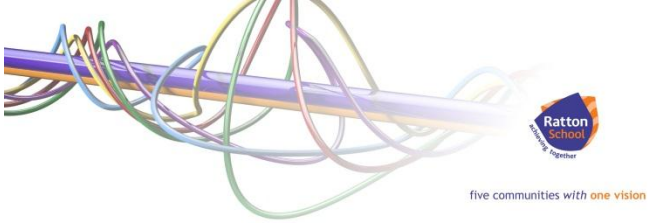
- Students should make sure they have adequate insurance for their devices including accidental damage cover that protects them in school. The school cannot be held responsible for any damage or loss of devices.
- Use of devices should be for lawful purposes only including, but not limited to: Computer Misuse Act, UK Copyright Law.
- Use of these devices for voice, video or text messaging is not allowed unless under teacher direction, as per school policy.
- Students are reminded of the schools e-safety policy which applies to the use of personal devices.
- No device is to be brought on site that contains any content forbidden in the e-safety policy. This includes illegal material of any sought, pornographic or offensive material, illegal software etc.
- Whilst school systems are filtered many devices allow students to connect to 3G (or equivalent) networks that allow unfiltered internet access, students at all times must adhere to the e-safety policy.
- Students should not attempt to bypass school filtering or access any system they are not authorised to access.
- Students should not use phones as calculators in school.

## Security

- Current Antivirus must be installed and running on the students machine.
- Any appropriate software / operating system updates must be applied.
- To ensure there are no viruses on any piece of equipment brought into school - we keep the DYOD wireless network entirely separate from the schools network. Equipment owned by the school is managed by us. Updates/antivirus is monitored and kept up to date automatically by central servers here. Equipment not owned by the school and managed by us should only connect to the DYOD network. To further fortify things, there is a piece of work being undertaken to establish a 'white list' of devices for the schools network which will mean only devices we specify can connect.

## Sanctions

- Students infringing on the rules noted above will have their Mobile Devices / Laptops confiscated. It will be taken to a secure place within the school/college and the parent(s) of the students informed. Parent(s) of the student may collect the Mobile Devices / Laptops at their convenience.

ACCEPTABLE USE	
DOCUMENT	

## Educational Visits

- We recognise that Mobile Devices / Laptops can be useful, but the same rules apply. If you are on a trip and the teacher is giving instructions to the travel party or you are being shown around a site, then this is as a 'classroom or its equivalent'.
- The school/college accepts no responsibility for replacing Mobile Devices / Laptops that are lost, stolen or damaged whilst on school/college premises or on school/college sponsored functions.
- It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and/or passwords must not be shared.

## Inappropriate Conduct

- For external exams, Mobile Devices / Laptops must be switched off and handed to the invigilator, locked away or left at home. Any student/s caught using a mobile phone / student owned device to cheat in exams or assessments will face disciplinary actions as sanctioned by the Headteacher.
- Any student who uses vulgar, derogatory, or obscene language while using a Mobile Devices / Laptops will face disciplinary actions as sanctioned by the Headteacher.
- Students using Mobile Devices / Laptops to bully other students will face disciplinary actions as sanctioned by the Headteacher.

## Theft or Damage

- In order to reduce the risk of theft during school/college hours, students who carry Mobile Devices / Laptops are advised to keep them well concealed and not 'advertise' they have them.
- Mobile Devices / Laptops which are found in the school/college and whose owner cannot be located should be handed to front office/reception
- The school/college accepts no responsibility for students who lose or have their Mobile Devices / Laptops stolen while in school or while travelling to and from school/college