



**BYOD Policy & Student ICT
Acceptable Use Policy**

Author: Wayne Taylor & Ben
Stout

Date Agreed by Governors: March 2018

Date of Review: November 2019

BYOD Policy:

Purpose:

Wollaston School BYOD agreement has been drawn up to protect all parties (pupils, staff and the school) where BYO ICT equipment is in use. With the increasing use of mobile phones and other hand held electronic devices to access the internet and email, this policy also covers acceptable use of these BYO devices in and out of school to the extent of how this is used.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor internet sites visited and email sent or received. Users are responsible for all emails sent and for contacts made that may result in email being received. Users need to be aware of their responsibility if they forward any email onto another party, especially if specific sensitive data is within the email (refer to the school's data protection policies for further information).

School email addresses are allocated to individual users. All emails passing through the school computer system are monitored by system administrators for malicious and/or offensive content, in addition to unsuitable text and images.

Aims:

To allow all users to safely access and use computers, internet and email for educational purposes.

Educational activities covers, but not limited to:

- individual research
- preparation of lessons
- project work
- controlled assessment tasks
- homework assignments
- private study
- communicating with other teachers and pupils

To provide a mechanism by which staff and pupils are protected from sites, information and individuals which could undermine the principles and aims of the school.

Provide rules which are consistent, and in agreement with, the Data Protection Act.

Provide rules which are consistent with the acceptable procedures commonly used on the internet, including those associated with "netiquette".

To provide a framework for a safe, non threatening ICT environment within school.

To ensure that all use of ICT in and out of school complies with the school's policies on bullying and harassment.

Acceptable Use:

- You will need to obtain the permission of your parent(s) / guardian(s) to be allowed to use the computer, internet and email facilities at Wollaston School. Users requesting ICT and internet access should read and sign a copy of this Acceptable Use agreement [Appendix 1] and return it to their form tutor.

- You must only access those services you have been given permission to use.
- You must not access any ICT service without permission from a member of staff.
- You may not use proxy servers to access any internet sites or other resources you would not otherwise have access to through the school network.
- Work or activity on the internet and/or computers must be **directly related** to your school work.
- Do not disclose any password or username you have been given, to anyone.
- Do not give out personal addresses, telephone/fax numbers or email addresses of any person at Wollaston School.
- Use of names or photographs of anybody at Wollaston School will require written permission from parent(s) / guardian(s) or staff concerned.
- Do not download, use or upload any material which is copyrighted. Always seek permission from the owner before using any material from the internet. If in doubt, or you cannot obtain permission, do not use the material. Pupils must also not plagiarize work.
- Under no circumstances should you view, upload or download any material which is likely to be unsuitable for pupils or schools. This applies to any material of a violent, dangerous, racist or inappropriate sexual nature. If you are not sure about the suitability of any material, you must ask a member of staff.
- Always respect the privacy of files of other users. Do not enter the file areas of other pupils or staff without obtaining permission from them first. All computer accounts (usernames and passwords) are for the use of a single individual, the person for whom the account was approved. All actions when an account is in use are the responsibility of the account holder.
- Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed. Do not state anything which could be interpreted as libel (untrue or misrepresents the facts).
- Use of school facilities to gain unauthorised access to any other account, at this school or any other facility, is expressly prohibited. Doing so may constitute a criminal offence.
- Whilst the school employs sophisticated web filtering software, should you inadvertently access any information or images, you are asked to inform a member of staff immediately in order that the site can be blocked.

Security and Limitations:

Wollaston School has the authority to disable users, email facilities and internet access immediately, without warning, for failure to comply with this policy.

Wollaston School takes bullying and harassment of staff and students very seriously. Where such behaviour occurs through the use of mobile technology, in or out of school, action will be taken as outlined in our climate for learning and anti-bullying policies. Where appropriate, incidents may be referred to the police.

All users have a duty to report infringements of this policy by others to a member of staff: *the school must be strict in these matters to ensure that any user breaching this agreement is prevented from bringing the school into disrepute and to ensure that the integrity of the school is maintained.*

Failure to comply with these rules will result in one or more of the following:

- A ban, temporary or permanent, on the use of computers, the internet and/or email facilities at school.
- A letter informing your parents of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on access to school facilities to be decided by the Learning Manager for your year group, Key Stage Leaders for IC, Head of Department, Headteacher or Senior Leadership Team.
- Any other action decided by the Governing Body of Wollaston School.

- Please be aware that where computer misuse gives serious cause for concern, the school may refer to the Police or Local Authorities for additional guidance.

Bring your Own Device:

Wollaston School BYOD policy has been drawn up to provide safe use and protect all parties where students' own ICT and media is in use at school. It is intended to allow all users safe access to computers, Internet and email and other devices for educational purposes.

Bring Your Own Device (BYOD) Policy applies to all students. Mobile technology has become an integral part of modern life. It offers a valuable resource for use in the classroom and has numerous educational opportunities from photographing notes for use later to browsing the internet. Wollaston School embraces new technologies and wishes to develop student skills in this arena for lifelong use, but within the safety of an agreed usage policy.

Rationale:

Throughout this policy, the word device is used to describe any mobile phone, tablet computer, laptop, MP3 player or other device capable of communicating with either the internet or mobile telephone networks and taking visual or sound recordings. Well-known examples of these that are likely to be owned by students include iPhones, iPads and laptop computers.

This policy covers the use of and liability for all devices within the School and School grounds and is for devices provided by school.

Legislative Framework:

The policy covers all students in the school and also third parties who have access to the School's electronic communication and network systems.

The use of the School's network systems and personal devices by students within school time is likely to involve the processing of personal data and is regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code, issued by the Information Commissioner. The School is also required to comply with the Regulation of the Investigatory Powers Act 2000, the Telecommunications Regulations 2000 and the principles of the European Convention on Human Rights incorporated into the United Kingdom law by the Human Rights Act 1998.

Principles for Use.

The School's Governing Body has overall responsibility for this policy, but has delegated day to-day responsibility for overseeing and implementing action to the Headteacher or his representative.

The school's students are expected to have regard to this policy at all times to protect its electronic communication systems from unauthorised access and harm.

The objective of this policy is to define the standards of conduct when employing the use of non-school owned electronic devices such as laptops, tablets, smart phones and other devices used to access the internet and school learning resources.

Guidelines and Procoesses:

- The school reserves the right to refuse to allow access to particular devices or uses where it considers there is a risk to the school network. Breaches of this policy will be taken seriously and any students found guilty may be subject to disciplinary action, in line with the school's behaviour policy.

Students should not, under any circumstances, access our network resources without completing a BYOD contract.

- Use of personal BYOD devices is at the discretion of the School and should not be seen as a right. Students' own devices can be used in the classroom at the teacher's discretion.
- Students who wish to bring their own device to school must submit a completed BYOD contract to the School and must register their MAC address to the IT department. You will then be given access to the BYOD network.
- Remote desktop is a feature that should be used internally and externally to access the school network.
- Data should not be transferred to any other person or device without using the correct equipment authorised by the school. School's internal policy does not allow the use of non-encrypted memory sticks or non-encrypted external hard drives. The external media needs to be encrypted to communicate with the devices within school (if you require further advice on this, please see the IT team). Permitted ways to transfer data are: email, secure encrypted external media or remote desktop.

Equality of Opportunity:

Any student who chooses not to bring their own device into school will not be disadvantaged. Where necessary, school will provide devices to support curriculum activities and / or examination requirements.

Acceptable Use of User Owned Devices:

The primary purpose of personal devices at school is educational or related to educational experiences. Use of personal devices during the school day is at the discretion of the staff. Pupils must use devices only as directed by their teachers.

All BYOD devices shall only contact the Internet and local area network via the school wireless network. All internet access via the network is logged.

The use of cellular data (e.g. GPRS, EDGE, 3G, 4G, etc) to access the Internet in School is strictly prohibited.

All access must be by the school wireless network which is appropriately filtered. It is a condition of BYOD use under this policy that students are responsible for disabling cellular data on their device when on the School site.

The use of device camera or microphone functions on school premises, including school events, functions and visits, is prohibited unless approved by a staff member. Pictures, video or sound recordings taken in school may only be used in school related learning and must not be posted, uploaded or shared on any website or system (e.g. social media) other than one that belongs to or is approved of by school. We would highly recommend that any school-related media is stored on the school system.

Is it prohibited to use a device to take pictures, video, sound recordings of any student or staff member without their permission. Failure to comply will be a disciplinary matter.

When on the school site and switched on, all BYODs must be set to silent. Charging devices of any kind may not be used in school. If a student is found to be using an electrical outlet for charging their device then the charging device may be removed and can be collected at the end of the school day.

It is the students' responsibility to keep their device safe while at school, on school related visits and school sponsored activities.

The school does not provide technical support for the students' own devices. Users should be competent in the use of their own device. The school does not provide direct printing from users' own devices.

Unacceptable Use:

The school does not approve any 'apps' or updates that may be downloaded onto any device whilst using the school's wireless network and such activity is undertaken at the owner's risk. The school has no liability for any consequent loss of data or damage to the individual's device.

Devices must not be used in a manner that would portray the School in an unfavourable light.

Devices should not be used to intimidate, abuse or share information that might be perceived as unfavourable against any member of staff, student or any person associated with the school.

Devices must not be used to share any information of an indiscrete or sexual nature with any other person. Students are not permitted to use any device to create a wireless hotspot.

Emails/Mobile Phone Access:

If you would like to add your emails onto your mobile and you attempt to do this, it will quarantine your actions in our system and you will require authorisation from the IT team to enable O365 on your mobile phone. Please email/contact the IT support team and arrange a convenient time where we can support you with the setup of your work emails on your mobile phone.

Please download and use the Outlook app from the android or iOS store to add your emails to your mobile phone. Please **do not** attempt to add your emails via the in-built mail applications on your android or iOS device as the mobile device management system behaves differently on these in-built applications. For example; if changes are made to the O365 platform and policies need pushing out or changes need to be completed on the mailbox, this could ultimately wipe your mobile phone if you are not using the Outlook app, (example on the iOS store - <https://apps.apple.com/us/app/microsoft-outlook/id951937596>).

Whilst every effort is made to ensure your data is safe, we cannot account for everything, please ensure you complete regular backups of your personal devices. If you leave the school and you have not come down the IT support office to disconnect your mailbox, then this will be done remotely, but we cannot be held responsible for the behaviour on each device or any data that is lost during this process.

Security of Systems and Data:

The BYOD policy and student contract will be limited to access to the internet through the school's wireless network provision.

This policy gives permission for Sixth Form to use BYODs under the provision of this policy at all times during school hours and Key Stage Three and Key Stage Four students with subject teacher permission during time.

The school requires that students have installed anti-virus software available for that device. The school does not guarantee provision of anti-virus software for BYOD.

Where students use their own device to access and store data that relates to Wollaston School, it is their responsibility to familiarise themselves with the devices sufficiently in order to keep the data secure. This includes preventing theft and loss of data, keeping information confidential and maintaining the integrity of data and information. Students should delete sensitive emails once they have finished with them and delete copies of attachments to emails on their own device as soon as they have finished with them. In the event of loss or theft a student should change the passwords to all the school's services accessed from that device and report the loss or theft within 48 hours to the data protection officer.

When a device has been registered by the school and approved, the device can be connected to the school network via access with the wireless password. Students are not permitted to share this access key or password with anybody else. If a student is found to have given this access key to anybody, their access to the system will be revoked and disciplinary action taken. The student's device will be issued with a monitored IP address. Students are not permitted to edit, adjust, disguise or share the IP address they have been given.

Monitoring of User Owned Devices:

The school will not monitor the content of user owned devices, but reserves the right to monitor any traffic over the school system to prevent threats to the school network systems.

The school does not collect or store any passwords or personal information when a BYOD is connected to the internet.

The school may require access to a student's personal device whilst investigating cases of policy breach including, but not limited to, finding or retrieving lost messages lost due to computer failure, to assist in the investigation of wrongful acts including cyber bullying, hacking of the school's computer system, virus attack or to comply with any legal obligation.

The Headteacher may require access to a student's personal device whilst investigating any behaviour or allegation relating to our School Anti-Bullying Policy. In these circumstances every effort will be made to ensure that the school does not access private information of the students which does not relate to the investigatory matter.

Controlled assessment on User Devices should only be carried out under direct instruction from a Head of Faculty. Controlled assessment procedures and policies apply to all work completed on a user device. Students must seek specific permission from subject staff to complete any controlled assessment on a personal device. OFQUAL policies, contract and guidelines apply to all coursework completed on any device.

Protection of Devices:

Users are encouraged to protect their own devices e.g. with the use of password or PIN as appropriate. Students are responsible for the use of their own device while on the school site.

Theft, Damage and Insurance:

The school takes no responsibility for any damage, loss, malware, theft, or insurance of any device that is not the property of the school, used within the school premises, including any event which causes the device not to function. We will investigate the theft, but not the loss of a device. If a device is stolen or damaged while on school premises, it is to be reported to Student Services immediately, in order that the incident can be logged.

It is the students'/parents' responsibility to ensure that they have sufficient personal insurance to adequately cover their device for any such occurrence. Any other costs, including the download of data, incurred while using devices, are not chargeable against the school and are the sole responsibility of the owner.

Incidents and Response:

Where a security incident involving students using their own devices arises at school, this matter will be dealt with very seriously. The school will act immediately to prevent, as far as reasonably possible, any further harm occurring. The Headteacher and School IT service provider will decide on the most appropriate course of action.

The School reserves the right to remove a device at any time if a student is seen to be violating this policy or any other related school policy.

Wollaston School Acceptable Media Use Policy Statement:

Wollaston School has invested significant resources to provide computers, laptops and associated network technology for students. We spend a lot of time in ensuring that our Wi-Fi and wired networks provide the best service that we can to aid student learning.

The school intends to develop opportunities for students to bring their own devices to assist their learning. This will include mobile phones for use as video and audio recording and processing devices and laptops and electronic notebooks to provide access to the Internet and word processing and other electronic documentation.

All students are expected to sign a contract agreeing a set of rules relating to behaviour covering the use of School IT or BYODs and to use of the Internet, privacy of work files, passwords and security. Students will be required to commit to this agreement prior to using IT or BYOD facilities. Any user of IT or BYOD facilities breaking the agreed rules will have their access restricted or removed for a fixed period of time.

Appendix 1.

On the next page...

ICT Acceptable Use (including email access):

Name: _____

Form: _____

Student ICT Acceptable Use:

All students are expected to sign a contract agreeing a set of rules relating to behaviour in our IT suites and to use of the Internet, privacy of work files, passwords and security. Students will be required to commit to this agreement prior to using IT facilities. **Any user of IT facilities breaking the agreed rules will have their access restricted or removed for a fixed period of time.**

I agree to the following rules in relation to use of IT in school:

- I will keep all usernames and passwords safe and secure.
- I will not use anyone else's user account.
- I will not eat or drink in any IT suite.
- I will not access any explicit or inappropriate material in school or use any game sites or websites that have been banned.
- I will follow the teacher's instructions at all times.
- I will use only computers or devices that the teacher has assigned to me or given me permission to use.
- I will not send store or publish any material on or through the school network which is bullying, threatening, abusive, indecent or offensive.
- I understand that use of unapproved sites will lead to me being barred from using the Internet and continual misuse may lead to me being barred from the school network.
- I understand that I will be expected to pay for any damage of equipment that I cause deliberately or by misuse.

I wish to use my personal device/s to access my Wollaston School emails for educational purposes. I have read and understood the ICT Acceptable Use Policy, including the "Emails/Mobile Phone Access" section for clarification on email access and using emails on a personal mobile/BYO device. I agree to abide by its conditions.

Please complete the below information regarding email access on a personal mobile/BYO device, once the IT team are in receipt of this documentation they will register your device:

Device/s: _____

Signature of agreement:

Student Signature: _____

Date: _____

'Bring your own' [BYO] Devices Contract:

- I will only use my own device when permission has been given by a member of staff.
- I will only use the school network to access the internet from my own device.
- I will not record, send on or store any pictures, video or sound of any other person without their express permission.
- I will ensure that my BYO device is always set to 'silent' when switched on.
- I will not charge my device in school.
- I will not use my device to download any materials that are not directly for school work-related purposes.
- I understand that the safety of my device and all associated passwords is my own responsibility.
- I understand that the school will investigate theft or malicious damage to my device, but I am responsible for any accidental damage or loss of my own device and any cost of repairs or replacement for it.
- I understand that the school will not provide technical support for my device and that there is no guarantee that the school's network will support my device.
- I understand that the school may require access to my own device whilst investigating cases of inappropriate behaviour such as cyber bullying, hacking the school's computer system or spreading viruses or any other action relating to the school's anti-bullying policy.
- I will only use the authorised external media and features available to me as outlined in the policy to transfer data and access the school's network.

Our full policy can be found on the website, if in agreement, please see the IT department to register your MAC address and device.

I wish to use a personal device at Wollaston School for educational purposes. I have read and understood the BYOD Policy and agree to abide by its conditions. I understand that misuse of a device may lead to the device being confiscated for return to parents and that I may lose the privilege to bring a device into school in the future.

Please complete the below information regarding your BYO device, once the IT team are in receipt of this documentation they will allow your BYO device on the network:

Device/s: _____

MAC Addresses: _____

Signature of agreement:

Student Signature: _____

Date: _____

Parental Signature: _____

Date: _____