



Teesside High School
Education as it should be

ICT Acceptable Use and Mobile Devices Policy

DOCUMENT CONTROL	
Date Revised/Reviewed:	November 2021
Ratified by Governors:	8 December 2021
Date of next Review:	November 2023
Committee:	Education

TEESSIDE HIGH SCHOOL

Policy Name	ICT Acceptable Use, iPads and Mobile Phone Policy
Purpose	To ensure that staff and students are aware of their obligations to ensure high standards of behaviour are set when using the School's ICT facilities. To provide clear rules and guidelines for the School, its staff and students on the acceptable use of ipads and mobile phones.
Applies to	All employees (teaching, support, casual, agency), volunteers, interns, agents, sponsors, and any other person associated with the school, including parents and pupils.
Other associated policies and documents	Student Code of Conduct, Sanctions and Rewards Policy; Safeguarding and Child Protection Policy; Data Protection Policy.

Introduction

Teesside High School seeks to ensure high and consistent standards for the acceptable use of the School's ICT facilities and any mobile devices used within the school. Technology can be used to improve the quality of learning by enhancing what is already being done at home and at school but it is imperative that this is done safely. Parents and pupils will be asked to sign a contract of agreement to the principles laid out below. Parents/carers of children using iPads, or other similar devices, must read and agree to this policy. A child-friendly version of this policy, called the 'iRules', can be found at the end of this policy. These closely follow the guidelines laid down by the Home Office and the DfES for the safe use of computers by school children.

Some older pupils in the Prep School and all pupils in the Senior School have Google accounts and access to the internet. In the interests of Child Safety they are protected by a firewall and elaborate content filtering software. The purpose of this is to block access to sites which are considered inappropriate for school children. Electronic controls alone can never be 100% effective, and the use of methods to bypass the School's security (including the use of VPNs and hotspots) are dealt with in line with the School's Sanctions Policy.

A log of children's activity is held by the School and is regularly checked. The School can gain access to any pupil's home area to check for inappropriate content. Similarly, teachers may check pupils' personal devices/memory sticks to check for inappropriate content.

It is acceptable for pupils to use the internet to access sites, at appropriate times, which are of interest to them for their learning, recreational and leisure pursuits. They may use their email account for sending emails to their friends and teachers, or to their home PC. Email can also be used in pursuit of the pupil's educational, recreational and leisure objectives.

Using ICT in School Security

Except in some junior years in the Prep School, each pupil logs on with their own unique **user name** and **password**. These **must not** be shared as to do so invites malicious tampering and access to confidential material. It is unacceptable to attempt to log on using someone else's username. Always remember to log off when you have *finished* with a computer or electronic device, but do not 'lock' the workstation. .

Copyright

Pupils should be aware of the risks of breaking the copyright of material downloaded from the internet. Work that has been copied but not referenced will be marked down and in some cases failed. The School will not condone plagiarism or intellectual theft of any kind. The illegal copying of copyright material, including music, may result in the individual facing prosecution. Downloaded material must be correctly referenced. On no account should pupils attempt to pass off downloaded coursework or answers as their own. This may result in disqualification from all public exams by the exam boards themselves.

Homework

It is acceptable for pupils to access websites to aid research for their homework. Departments will give advice to pupils about relevant sites. Some departments also compile lists of good sites for their pupils.

Personal details

Acceptable use requires pupils never to disclose personal details about themselves in emails which could be sent or forwarded to a stranger. In particular pupils must never disclose their home address, telephone number, or date of birth in an email or online.

Social Media (including chatrooms, group chats/messaging)

It is difficult for the School to supervise these adequately so access to them will not normally be permitted at school. Computers, mobile devices (including iPads/Chromebooks belonging to the school) and access to the school wi-fi are provided by the School to facilitate learning; they are not for personal use or for accessing social media (*e.g. Facebook, twitter etc.*). Abuse of this will be treated in line with the Sanctions Policy, which may include denied access from school ICT facilities for a period of time.

Online shopping

It is not expected that this should be a normal part of the use of the School's computers. It may be the case on occasion that some senior pupils may carry out online shopping under the supervision of their teachers. Where this is not the case pupils seeking to conduct online shopping must have the written permission of their parents, and the consent of their form tutor, before approaching any shopping sites with a view to purchasing goods. Normally permission would only be granted to Sixth Formers.

SPAM and Viruses

The School network is protected by Windows Defender Security Centre anti-virus software which is continually updated. In order to maintain security there are certain things which each user should avoid:

- never attempt to open unsolicited email
 - never attempt to open email from unfamiliar addresses
- never attempt to open attachments which have been blocked.

Breaches of Acceptable Use

The following are guidelines regarding breaches of Acceptable Use, and the School's Sanctions Policy will be used to deal with these breaches. It is not an exhaustive list and there are other occasions when these standards may be applied to activity which the School considers a breach. Many of these are also covered in the School's Anti Bullying (including Cyber Bullying) Policy. Do not:

- Use email to send messages which are aggressive, unfriendly, abusive, racist, offensive, pornographic, or which contain offensive language or words.
- Attempt to access websites which are offensive or pornographic
- Use the school computers to distribute material or images which may be considered indecent and inappropriate, offensive, or pornographic

- Attempt to subvert or bypass the School's firewall and content filters, or otherwise maliciously interfere with the School network *using the school computers or personal devices*.
- Download or illegally copy any copyright material
- Use the internet to access copyright material which is then passed off as your own work
- Attempt to log on using another pupil's or staff username and password

Any pupil found abusing the system will be dealt with in accordance with the Sanctions Policy, but this can include being prevented from using the school system for a lengthy time.

Bring your own device

Mobile Phones

Mobile phones are allowed in school if parents deem them necessary, but **must** be switched off during the school day and handed into form tutors every morning. The phones will be stored securely during the day and are available for collection at 4.00pm.

Procedures:

- If a mobile phone is seen or heard by staff during the school day it will be confiscated by that member of staff.
- The phone will be given to the Deputy Head (Pastoral) who will log the incident and lock the phone away safely.
- For a first offence - confiscated for the day and returned at 4.00pm.
- For a second offence - confiscated as before and parents informed by Assistant Head that if it happens again the phone will be confiscated and parents asked to come and collect it. If a pupil needs to contact parents re arrangements, this can be done at the school office.
- Phones must not be used for texting/photographing/videoing in line with the Data Protection Act.
- Pupils in Years 12-13 may hand in their phone if they wish but are trusted to act responsibly if they choose not to do so. They may be used in lesson times for educational purpose only, but should be out of sight and not used in 'free-time'. Failure to behave responsibly will result in confiscation of the phone as above.
- Any pupil who uses their device for the purposes of bullying or intimidating another child or member of staff will be dealt with rigorously in line with the School's ICT Acceptable Usage, Cyber-Bullying, and the student Code of Conduct.

Tablets and Chromebooks

We are currently in a transition period with some students using BYOD tablets (iPads and android devices) and other year groups following, significant investment, have been provided with a Chromebook to use in school and at home for educational purposes. For the purposes of this policy where the terms 'tablet' and 'devices' are used this applies to all tablets and Chromebooks used in school.

Security:

- All tablets used in school require a configuration profile to be installed. This allows internet usage to be monitored in school.
- Where possible 'Find my iPhone' (or similar location app) must be enabled on all tablets. This is a built-in App on the tablet that allows the device to be tracked and remotely locked/wiped. Because of these security features, the tablet is useless to anyone else if stolen; its location can be identified, and the information passed to the police.

- Never use the tablet on the journey to or from school if you do not travel with your parent; keep it safe within a school bag. To avoid accidents, do not use a tablet while walking around.
- Take the tablet home every night to charge it and bring it to school every day.
- Use a passcode to keep the device secure, but unlock it if asked by a member of staff.
- If using a school device always remember to sign out of the wifi and any apps you were using (e.g. Google Mail).

Using the tablet:

- Always follow the iRules
- The device is intended for use in lesson time only and may only be used during breakfast club, tea club, breaks or lunch times with permission from supervising staff.
- Stop using the tablet immediately if asked to by an adult.
- Sound should be muted at all times unless permission is given by an adult.
- School apps must not be deleted.
- Do not allow anyone else to use your device unsupervised.
- Ensure all content on the device complies with copyright laws e.g. no illegal downloads.
- Items deleted from the tablet cannot be 'undeleted' so back up your device, to iCloud or a computer, regularly. Training for parents and children will be provided to assist with this if needed.
- Print out only school work to the shared school printers, and only print when absolutely necessary.

Being Safe:

- At home, make sure that you give your parents your device at night time so that it can be charged for the following day. These should not be kept in your bedroom. This is to keep you safe.
- As the child is too young to have an account, the parent/carer will set up a new iTunes/android account for use on the device and accepts full responsibility for monitoring this.
- Never film, photograph or record audio of anyone without asking permission.
- Never upload photographs, video, audio or personal details of yourself or any other person to the public internet (eg social media). ANY form of social media is banned for pupils in the School.
- Report any form of intimidation, nastiness or bullying to your teacher.
- Unlock the device and allow staff to access its contents when asked. Do not keep 'private' information on the tablet, because it's not a private space.
- Never share your password or attempt to access anyone else's files.
- Do not tamper with the device's operating system.
- Do not attempt to circumvent the internet filtering or other restrictions, for example using VPNs or hotspots. Do not use the tablet to access inappropriate content e.g. age restricted material or images/text that are not suitable for children.
- Take regular breaks from using the tablet and avoid using headphones with the volume

too high.

- Do not remove or attempt to remove the school's configuration profile from the tablet.

Appendix 1 –

'iRules' Form

Name: _____ Form: _____

The rules below are designed to keep you safe whilst using your iPad and to make it fair to everyone. To be able to use your iPad at school and home where appropriate, you must agree to, and sign this policy. This policy will also apply to students who bring in their own personal devices, and to those who book out or loan a device during the day.

- I will bring my device to school each day (unless otherwise told), and ensure that it is fully charged before the school day.
- I will not try to bypass the school's filtering software to access blocked internet content (e.g. using personal VPN's or hotspots).
- I will not use anyone else's device without their permission.
- I will use a passcode to securely lock my device, and will keep it a secret.
- I will report any damage to my device to my parents and the school at the earliest opportunity.
- I will not take photos, or record audio or video of anyone else without their consent.
- I will setup my school email account using Gmail or the default Mail app.
- I will ensure that I keep my device backed up by using iCloud, and by saving work to my Google Drive account.
- I will enable the 'Find My iPad' feature or something similar, on iCloud.
- I will keep my device in a protective case at all times.
- I will not leave my device unattended in the school, and will keep it in a safe place when not needed.
- During lessons, I will not use my device for non-learning activities (e.g. games).
- I will not use my device to send abusive/threatening messages, photos or videos.
- I will report any abusive/threatening content that is sent to me.
- I will give my device a sensible name to help locate it, should it be misplaced within school.
- I will not remove any management profiles on a school device, and will not install my own.
- I will leave my device safely in my bag when I travel to and from the school.
- I will return loaned devices to the ICT technician's office by 4.15pm (the same day)
- I will sign out of any apps and the school wifi before returning a school owned device.
- I will print out only school work to the shared school printers, and only print when necessary.

Child to read and sign below:

I have read, understood and agree to follow the iRules. I understand it is my responsibility to make good choices when I use the tablet/device. I understand that if I break the iRules, there will be a consequence that could include confiscation of the device or having features (such as camera or internet access) disabled.

Name:

Signature:

Date:

Parent/carer to read and sign below:

As parent or legal guardian of the child above, I have read, understood and agree to comply with the iPad Acceptable Use Policy. I understand that the tablet/device is to be used for educational purposes. However, I also understand that it is impossible for the school to restrict access to all offensive and controversial materials and understand my child's responsibility for abiding by the iRules. I accept full responsibility if and when my child's use of technology is not in the school setting and understand that my child is subject to the same rules and agreements while not in school. I also understand that, in the case of repeated serious issues, the school would be forced to remove my child's use of the iPad completely.

Name:

Email:

Mobile number:

Signature:

Date: