

ICT ACCEPTABLE USE POLICY (Students)

Our Acceptable Use Agreement

1. The Aims of the Policy
2. The SMART Rules.
3. Policy Detail
4. Summary Quick Guide

1 The Aim

This Acceptable Use Policy, which is applicable to all schools in the Sherborne Area Schools' Trust (known as the Trust), provides teachers, students, parents and carers guidelines and instructions on how to equip young people with the knowledge and skills to identify, manage and reduce online risk, so that they can get the most from the internet and technology, whilst staying safe.

As a member of a school within the trust, students are entitled to access the school ICT Network. The Student AUP is aimed to ensure that you, as a student, can use the school network - Internet, Email, Cloud services and other technologies available such as mobile devices and tablets and ChromeBooks, both at the school and externally - in a safe and secure way, and that everyone is able to take advantage of the potential of ICT to support their learning in a responsible and safe manner. To do this students need to understand the rules and systems that are in place to protect them, to ensure that our school system is secure and that no one is subject to bullying, harassment or abuse.

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in a safe and responsible way. Schools within the Trust will take every opportunity to help parents/carers understand e-safety issues through e-safety training and awareness raising at parents' evenings, and have access to useful information via parent leaflets, letters, website and information about national and local e-safety campaigns. Parents and carers have a responsibility to monitor their child's use of technology to support the school in promoting good e-safety practice and to follow the guidelines outlined in this policy.

1.1 The Agreement

This policy forms the basis of an 'acceptable use' agreement declaration that students and parents/carers at schools within the Trust are required to sign. This policy and Acceptable Use Agreement extends to all hardware and software; both fixed and mobile internet technologies provided by the school (such as PCs, laptops, tablets, mobile devices, webcams / camera/ video recording devices, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils that have been brought onto the school premises (mobile phones and other mobile

devices), whether accessed from the school or externally, irrespective of who owns the device and how the network is accessed.

Breaches of the agreement can result in a ban from the use of the ICT facilities and can include the confiscation of mobile devices, further action can be taken under the school's Behaviour For Learning policy where necessary. Policy breaches may also lead to criminal or civil proceedings.

NB – Users of the network may be held liable for costs incurred for repair and/or replacement of equipment where the damage was caused by misuse.

1.2 Educational Purpose

The computer systems (including networks) within the Trust have been established for an educational purpose. The term "educational purpose" includes classroom 'learning' activities, purposeful communication, career development and quality research activities using the internet. Students may use the network for limited personal use, only before or after school hours and in strict adherence to the 'Acceptable Use Policy' outlined in this document.

2 SMART Rules

S	Safe	Keep safe by being careful not to give out or post personal information, such as your full name, email address, telephone number, home address, photos or school name, to people you have only had contact with online. Set strong privacy settings on social networking sites
M	Meeting	Meeting someone you have only been in touch with online can be dangerous. Do not meet anyone in person who you have met online unless you do so with your parents' or guardians' permission and even then, only when they can be with you at that meeting.
A	Accepting	Accepting emails, instant messages, or opening files, pictures or texts from people you don't know, or trust can lead to problems; they may contain viruses or inappropriate content.
R	Reliable	Information you find on the Internet may not be true, or someone online may be lying about who they are.
T	Tell	Tell your parents, guardian or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online. You can report online abuse to the police at: www.thinkyouknow.co.uk and you can report anything you are not happy about to anyone you feel you trust. This could be a teacher, guardian, parent or someone else's parent. Tell someone.

3 Policy Detail

The use of the latest technology is actively encouraged at schools within the Trust, but with this comes a responsibility to protect students, staff and the school from abuse of the system. All students, therefore, must adhere to the Policy set out below. This Policy covers all workstations, laptops, mobile telephones and other electronic devices within the school, irrespective of who is the owner. All

students are expected to behave responsibly on the ICT resources provided by the schools, as they would in classrooms and in other areas of the school.

3.1 Personal Safety

- Always be extremely cautious about revealing personal details and never reveal a home address, telephone number or email address to strangers.
- Always inform your teacher or another adult if you have received a message or have visited a website that contains inappropriate language or makes you feel uncomfortable in any way.
- Do not play with or remove any cables that are attached to a school computer.
- Always be yourself and do not pretend to be anyone or anything that you are not on the Internet.
- Do not arrange to meet anyone you have met on the Internet; people are not always who they say they are.
- If in doubt, ask a teacher or another member of staff.

3.2 System Security

- Do not attempt to go beyond your authorised access. This includes attempting to log on as another person, sending e-mails whilst masquerading as another person or accessing another person's files. Attempting to log on as staff is unacceptable and may result in the loss of access to systems and other serious sanctions. You are only permitted to log on as yourself.
- Do not give out your password to any other student; if you do and they do something wrong logged on as you, you will be held responsible. If you suspect someone else knows your password, change it immediately. This password should be changed at least once a term and be at least 6 characters long.
- Do not alter school hardware in any way.
- Do not eat or drink whilst using the computer.

3.3 Inappropriate Behaviour

- 'Inappropriate Behaviour' relates to any electronic communication whether email, blogging, tweeting, social networking, texting, journal entries or any other type of posting/uploading to the Internet.
- Do not use indecent, obscene, offensive or threatening language.
- Do not post or send information that could cause damage or disruption.
- Do not engage in personal, prejudicial or discriminatory attacks.
- Do not harass another person. 'Harassment' is persistently acting in a manner that distresses or annoys another person.
- Do not knowingly or recklessly send or post false, defamatory or malicious information about a person.
- Do not post or send private information about another person without their prior agreement.
- Bullying of another person either by email, online or via texts will be treated with the highest severity.
- Do not access, or post, material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people.

- If you mistakenly access such material, please inform your teacher or another member of staff immediately or you may be held responsible.
- Do not attempt to use proxy sites on the Internet.
- Do not take or post a photo of another student or member of staff without their permission.

3.4 Email

- You should check your school email at least once a day during term time for new messages.
- Do not reply to spam mails as this will result in more spam. Delete them and inform the IT support office.
- Do not use email (including web mail) during lessons unless your teacher has given permission.
- Do not send or forward annoying or unnecessary messages to a large number of people, e.g. spam or chainmail.
- Remember when sending an email to:
 - Be Polite - never send or encourage others to send abusive messages.
 - Use appropriate language - remember that you are a representative of the School on a global public system. What you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language.
 - Do not reveal any personal information about yourself or anyone else, especially home addresses, personal telephone numbers, usernames or passwords. Remember that electronic mail is not guaranteed to be private.
 - Consider the file size of an attachment, files exceeding 10 MByte in size are generally considered to be excessively large and you should consider using other methods to transfer such files.
 - Do not download or open file attachments unless you are certain of both their content and origin. File attachments may contain viruses that may cause loss of data or damage to the school network.

3.5 Plagiarism and Copyright

- Plagiarism is taking the ideas or writings of others and presenting them as your own. Do not plagiarise works that you find on the Internet or anywhere else.
- You should respect copyright. Breaking copyright law occurs when you reproduce a piece of work or copy someone else's designs or images and use them in your work without stating in your work where the image or source material came from.
- The best way, and most recognised way of referencing work is to produce foot notes or bibliographies in your work
- Where possible you should request permission from the copyright owner. This includes music files and the copying of CDs, downloading of films from illegal sites and other such formats.

3.6 Privacy

- All files and emails on any system provided by schools within the trust are the property of the school. As such, system administrators and staff have the right to access them if required. This includes files on physical hardware or on cloud services provided by the Trust.

- Do not assume that any email sent on the Internet is secure.
- All network access, web browsing and mails on the school system are logged, and filters are in place to reduce the impact of inappropriate web sites being accessed
- If you are suspected of breaking this Policy, your own personal laptop/device and mobile telephone can be searched by staff.
- The school reserves the right to randomly search the Internet for inappropriate material posted by students and to act upon it. This includes, but is not limited to, searching social media websites for inappropriate content posted about the schools within the trust or persons within the trust. This includes statements and comments about current or past students and staff.

3.7 Software

- Do not install any software on the school system. The only exception to this rule is students are following a course of study and are instructed to install software as part of their studies. In these circumstances special computers called 'Virtual Computers' will be used.
- Do not attempt to download programmes from the Internet onto school computers.
- Do not knowingly install spyware or any sort of hacking software or device.

3.8 Printing

- Printer accounting systems are in general operation across most of the schools within the Trust. This facility is used to monitor student use. Where students are unable to act responsibly when using the printing services, their use of these facilities will be removed.
- Students within KS2, KS3 and KS4 will be allocated an initial budget which they are expected to manage carefully, getting the students to think if the work really needs printing. Once exhausted, students will see IT Support to have an additional amount added to their account.
- Students at KS5 will be given an initial budget which they are expected to manage. The budget is based on their course combinations. Once this budget has been exhausted the students are expected to purchase additional credit. This can be purchased via the Learning Resource Centre

3.9 Sanctions

- Sanctions will vary depending on the severity of the offence; they will range from a warning or withdrawal of Internet use, to suspension or exclusion. The trust's Behaviour for Learning policy will be used to determine sanctions and the severity of them.
- A breach of the law may lead to the involvement of the police.

3.10 General and Best Practice

- Think before you print; printing is expensive and consumes resources which is bad for the environment.
- Priority must be given to students wishing to use the computers for School use.

- Always log off your computer when you have finished using it. Do not lock the computer so that others cannot use it.
- Passwords should be alpha numeric, ie. contain both letters and numbers. There will be a minimum length in force that will be publicised.
- Observe Health and Safety Guidelines; look away from the screen every 10 minutes to rest your eyes and make sure your chair is positioned correctly and that you do not 'rock' on its legs.
- Housekeep your email regularly by deleting old mail.
- If a web page is blocked that you feel you have a legitimate use for, please ask your teacher in the first instance. They may then approach the IT Support team for assistance.
- If in doubt, ask a member of the IT Support office.

3.11 Music/Video Players (eg, iPods)

- The use of such devices is banned during lessons unless the teacher has given permission.
- Do not connect such a device to the school network/school computers.
- Do not break copyright laws by swapping illegal music/video files.

3.12 Bring Your Own Devices (BYOD)

The use of your own IT equipment at school is encouraged to support your learning and educational journey/experience. To support this the Schools within the trust have created a separate WiFi network to allow students to connect personal devices to the internet without seeking prior approval. This WiFi network will be visible on your internet enabled device. If you decide to connect your device to this network you are still using school facilities and are still bound by the other items in this Acceptable Use Policy. You should also be aware of the following:

- When you connect a device to this network you should mark it as a 'public' network as this will help protect your files from other activity on this network. If you make your computer visible to others you are more at risk of having files used, altered or deleted by others.
- Under no circumstances should you attempt to access files on another users computer. Students should disable sharing of any 'media' i.e. iTunes libraries, as this is way in which you may be breaking copyright law. If you are unsure of how to disable this, please visit the IT office for assistance.
- Students should not use the BYOD network to enable collaborative gaming, this is often network intensive and may have a detrimental effect on the performance of the network, thus impacting genuine academic users.

4 Summary Quick Guide

For my own personal safety:

- I understand that the school will monitor my use of all the ICT systems
- I understand that computer storage areas will be treated like school lockers and cannot be regarded as private
- I will not share my username and password, nor will I try to use any other person's username and password

- I will immediately report any unpleasant or inappropriate material or messages that make me feel uncomfortable
- I will adopt a 'think before I click' routine when using the internet (not all websites are appropriate) and will NOT simply access a site just because someone else told me to do so
- I will be aware of "stranger danger", when I am communicating on-line, and will not share my personal details with anyone

I will act as I expect others to act toward me:

- I will respect others' work and property and will not alter any other user's files
- I will be polite and responsible when I communicate with others
- I will never, either in school or out of school, seek to harass or abuse fellow students or members of staff either on the school network itself or via external social networking sites
- I will not take, publish or distribute images of anyone without their permission
- I will only use my personal hand held devices (eg: mobile phones) in school if I have permission. If I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- I will use email appropriately and will not send emails to a large number of users, and will not use email to bully others or send inappropriate text or images

When using the internet:

- I will make sure that I have permission to use the original work of others and/or I have made reference to it. I understand that exam boards treat this as cheating and will exclude me from exams
- I will not try to download copies, or bring into school any material that is protected by copyright (including music and videos)
- I will adopt a 'think before I click' routine when using the internet (not all sites can be trusted)
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate

Respect for the system

- I will not attempt to bypass any network or Internet security systems
- I will immediately report any damage or faults involving equipment or software
- I will not open any attachments to emails, unless I know and trust the sender
- I will not install or attempt to install programmes of any type on a machine nor will I try to alter computer settings
- I will not connect any laptop or other computer hardware to the system
- I will only print what I need to do my school work. I will only print in colour when it is absolutely necessary.
- I will manage my work area to ensure it is not full.