Sherburn High School

Achievement for all

Acceptable Computer and Internet Usage Policy

Adopted/Reviewed: December 2018

Date of Next Review: December 2020

Signed: .... Date: ....
(Head Teacher)

Signed: .... Date: ....
(Author of Policy)

Acceptable Computer and Internet Usage Policy

Outline / Overview

All Staff and Students of Sherburn High School who abide by these policy guidelines are entitled to use the computing facilities at Sherburn High School.

The school has taken and will continue to take all reasonable precautions to ensure that students access appropriate material only. However, it is not possible to guarantee that a student will never come across unsuitable material while using a school networked computer. The school cannot accept liability if such material is accessed nor for any consequences resulting from Internet Access.

All Key Stage 3 & 4 (KS3 & 4) students will be actively supervised at all times when using computers. Post 16 students have unsupervised access to computers for independent research and study. All reasonable precautions to ensure that students only access appropriate material have been taken. If they encounter such material they will know that they should report the incident to the nearest teacher or a member of IT Support.

The school's Internet access incorporates a software filtering system to block certain chat rooms, newsgroups, and inappropriate websites.

- Access to inappropriate sites is blocked
- Access will be allowed only to a listed range of approved sites
- The content of web pages or web searches is dynamically filtered by keyword checking
- Records of Internet sites visited by students and teachers are logged
- Accessing a site denied by the filtering system will result in a blocked webpage

If an appropriate webpage is blocked, 'allowed' access can be made of certain banned sites and provide the educational reasons behind the request, which will be carried out by ICT Support.

The school's ICT Support regularly assesses the effectiveness of the filtering system.

All school internet access must be via the school's wired or wireless network and on a device that has been configured by ICT Support. The school is not responsible for any content / information accessed via a 3G / 4G data connection i.e. a data connection via a cellular network provider as this connection cannot be monitored. Tethering is not permitted at any time. The use of personal laptops on the network is not permitted on the domain without authorisation from the network manager. However, users will be able to access the BYOD (Bring Your Own Device) wireless networks.

Under no circumstances should personal data be stored on local hard disk drives of computers to which multiple users have access.

Antivirus software is installed on all school machines and is updated when the device is either connected to the network or connected to the internet. If any user suspects that their machine has been infected with a virus or malware, they are to connect ICT Support immediately.

All Users

- Must make sure passwords must be complex, not contain any words which are part of your username, be at least 8 characters long and fill at least 3 of the 4 follow criteria:

  ✓ at least 1 Capital Letter
  ✓ at least 1 Lower Case letter
  ✓ at least 1 Number
  ✓ at least 1 Special Character (e.g.: !"£$%^&*()@~?><)

  and are forced to change their passwords every 53 days. Users are asked to make sure the password is not easily guessable by not using words such as "password"

- Must ensure network username and passwords are not shared between users
- Should make sure they log off any session once they have finished using a computer or laptop
- Are not to move / disassemble ICT equipment
- Must not install any software or hardware without permission from ICT Support
- Must not consume food and drink in ICT suites
- Must not use password cracking, VPN Apps or software, key logging, IP Scanners, BIOS cracking, port scanners, network sniffers or any other hacking or cracking software of any description should be installed, stored or ran on the network via any device.
- Are not permitted to use anonymous proxy sites or software to bypass the school's filtering system
- Are not permitted to install and / or use file sharing or bit torrent programs on laptops or desktops purchased by the school or use any device which can gain access to the internet via the network
- Must not plug in mobile devices to the school's equipment which would allow tethering (gain access to the internet)
- Must make sure printed documents are deemed necessary and must not misuse printing
- Are responsible for emails they send and for contacts made. Emails should be written carefully and politely
- Are not permitted to use public chat rooms or instant messaging services
- Must ensure copyright and intellectual property rights are respected
- Must be aware that the school has various systems in place to monitor computer use, internet access, file stores and emails. These systems will be used to ensure that this Acceptable Use Policy is followed at all times.
- Must ensure that they save their work every 10 minutes in case of error / power cuts

Staff

Staff must ensure that all KS3 and KS4 students are actively supervised at all times when using computer equipment, which can include using the appropriate classroom monitoring software (Impero). Failure to do so may result in that member of staff being unable to book and / or access ICT resources such as computer rooms.

The email system and internet access facilities are provided by the school as a business tool to enable authorised users to carry out their job role efficiently. The school regards any emails sent or received via the school email system as impersonal and access to emails may be granted by the Line Manager or Senior Leadership Team if the need arises, such as staff absence or leaving the employment of the school.

Staff must ensure that they regularly check for new emails. Each email address has a limited storage space and therefore staff must delete old emails regularly. Once the storage limit has been reached, no further emails will be sent or received. If staff require more storage, they should contact ICT Support.

Members of Staff:

- Must only use the school's technologies for professional purposes or for uses deemed "responsible" by the Head or Governing Body. Using a school email address for personal reasons or personal gain is demeaned irresponsible and will not be permitted

- Shall not use their school email address to sign in / sign up to sites that are not school related unless these sites are under the "Everybody Benefits" scheme provided by the Local Authority

- Must only use approved, secure school email systems for any school business

- Have access to view / control students' screens / network sessions

- Must not browse, download or send material that could be considered offensive and should report any accidental access of inappropriate materials to their line manager

- Have a duty to protect their passwords, SIMS logon details and personal network & Learning Platform logins and should log off / lock a logged in network session when leaving a workstation unattended. Any attempts to access, corrupt or destroy other users' data or compromise the privacy of others in any way, using any technology, will not be tolerated

- Must contact ICT Support, if a member of staff leaves their workstation locked and another member of staff needs to use to the machine to register a class. Any unsaved work will be lost during this process

- If you are downloading a blocked file such as a .ZIP file, please contact ICT Support

- Are permitted to use Personal Digital Equipment, such as mobile phones and cameras to record images of students including when on external trips / visits only if they are removed / deleted from the device(s) at the earliest opportunity. With the written consent of parents (on behalf of parents) and staff, the school permits the appropriate taking of images by staff and students with school equipment. Digital images are easy to capture, reproduce and publish and therefore, misused.

- Never store / send sensitive / personal data on Laptops, Removable storage / media or email without this being encrypted beforehand. ICT Support can advise and help staff if they have a requirement to take sensitive data off site be it via laptop, removable storage or email. ICT Support can even set up encryption on your devices. Recommended programs to use to encrypt data are: WinZip, 7Zip and Microsoft's BitLocker. You can purchase encrypted memory sticks but these must be encrypted to at least 256bit AES

  It is up to the individual member of staff who has responsibility to inform ICT Support that their laptop, removable device or email requires encrypting for sensitive personal data

- Should ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off school premises or accessed remotely. Personal data can only be taken out of school when authorised by the Headteacher or Governing Body.

- Should be aware that any USB storage device (memory stick / external hard drive) used in school needs to be encrypted if staff would like to write back / save back to the USB storage device otherwise the USB Storage device will remain a read only device

  Photos of students are dealt with when a student is enrolled at Sherburn High School via an opt-out form which is returned to Sherburn High School signed by a parent or guardian and stored in the General Office

- Members of staff should ensure that their use of web technologies, including social networking sites, such as Facebook, Twitter, Bebo and MySpace does not question or bring their professional role into disrepute

  - Staff are advised to consider and set out appropriately, their privacy settings on such sites

  - Should consider the appropriateness of images and material posted. Once posted online, as message, photo or video they can be freely copied, manipulated and circulated and will potentially exist forever

  - Should not communicate with students, in relation to either school or non-school business, via web technologies. Members of staff should only communicate with students using the appropriate School systems or systems approved by the Headteacher

  - Are not permitted to contact or communicate with students, parents or conduct school business using personal email address or telephones, without specific permission from the Headteacher

  - Should not give out their own personal details, such as telephone / mobile number or personal email addresses to students

  - Must ensure that all electronic communication with students and staff is compatible with their professional role

  - Must respect and comply with copyright and intellectual property rights

  - Are to have a responsibility to report any misuses of technology, including the unacceptable conduct of others, to ICT Support or Headteacher

By signing below, I have read and understood the Acceptable Computer and Internet Use Policy.

Name: ____
(Please print)

Signature: ____ Date: ______ / ______ / ______

ALTHOUGH NOT PART OF THE ACCEPTABLE COMPUTER AND INTERNET USE POLICY I.E. POLICY IN ITS OWN RIGHT, REFERENCE SHOULD ALSO BE MADE TO THE CHILD PROTECTION POLICY WHICH COMPLEMENTS ACCEPTABLE COMPUTER AND INTERNET USE IN THE SCHOOL, THIS IS AVAILIBLE ON THE Q DRIVE IN THE POLICIES FOLDER

Students

This Acceptable Use Policy will be displayed in appropriate places where students have access to computers.

Post 16 Students must sign this agreement before access to the school's network is allowed.

If a student breaches this Acceptable Use Policy then severe penalties will be enforced to protect the school, student and computer systems. The penalties will be decided by ICT Staff depending on the severity of the incident. In serious cases the School Management Team will be consulted and the pupl may have to appear before a sub-committee of the governing body. Sherburn High School may also report concerns to other appropriate bodies.

Students may find it difficult or impossible to continue with their studies depending on the penalty imposed.

This Acceptable Computer and Internet Policy will help protect students and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user's authorised account and password. Students must never reveal their password to other students even to those whom they trust. If students believe that security of their password has been compromised, they must inform an ICT Teacher or ICT Support
- Students must not pose as someone else when asking to change their password
- Uploading / downloading software is not permitted
- Students are not allowed to store executables and system utilities in user areas or bring in / run these files from removable storage devices
- Viewing of any offensive or pornographic materials is not allowed. Accidental access should be reported at once to the appropriate member of staff or ICT Support
- Playing non-educational games / quizzes is prohibited at all times unless authorised by a member of staff
- Students must log out after every network session and not lock their workstations. Failure to log out will result in any unsaved work being lost. You will be responsible for any work lost / edited if you leave your machine unattended.
- Users are not to physically tamper with ICT equipment, attach unauthorised hardware or install software
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals
- Students must not upload / send personal addresses, telephone / fax numbers / email addresses of anyone
- Students will not intentionally visit sites that attempt to bypass the school filtering system.
- Irresponsible use of ICT facilities will result in the loss of Network and / or Internet access. Depending on the severity of the abuse further action may be taken by the school or the appropriate authorities.

By signing below, I have read and understood the Acceptable Computer and Internet Use Policy. I understand that breaching the code will result in penalties and these will have a serious effect on my ability to continue with my studies. Any breach will also affect any references provided by Sherburn High School.

Name: ____
(Please print)

Signature: ____ Date: ______ / ______ / ______

Student Year Group: _________________________ School: Sherburn High / Tadcaster Grammar **

Post 16 students:
If you are attending Post16 from Year 11, please write Year 12.
If you are doing your 2nd year of Post 16, please write Year 13.
If you are stopping for a 3rd year of Post16, please write Year 14.

** Please delete / highlight as appropriate.