Sherburn High School

Acceptable Computer and Internet Usage Policy

Adopted/Reviewed: July 2020

Date of Next Review: July 2021

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. Sixth Form 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 students encounter such material, students are to report the incident to the nearest teacher or a member of IT Support.

The school's Internet access incorporates a dedicated hardware filtering and firewall system that all users pass through to access the internet.

- 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 and logged by keyword checking
- Records of Internet sites visited by users are logged and are kept for a maximum of 12 months
- Accessing a site denied by the filtering system will result in a blocked webpage

If an appropriate webpage / category is blocked, 'allowed' access can be configured to allow the requested blocked site(s) and the requestor should 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 Making sure the updates and policies from the management host are applied in a timely maner, testing accounts against the appropriate filtering groups and viewing the filtering and firewall logs, acting when necessary.

All School internet access must be via the school's wired or wireless network. The school is not responsible for any content / information accessed via a personal data connection i.e. a data connection via a cellular network provider as this connection cannot be monitored. Tethering (connecting a device to a mobile data connection) 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 internet via the BYOD (Bring Your Own Device) wireless networks where a certificate will need to be installed on to the device(s) to access the internet. This certificate poses no threat to the device, it is there to keep the user safe and compliant whilst on the BYOD networks.

Under no circumstances should personal data be stored on local hard disk drives of computers that are attached to the domain or that multiple users have access to.

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 contact ICT Support immediately.

All Users

- Must make sure passwords are 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.: !"£$%^&*()@~?><)

  Users are forced to change their passwords every 53 days and must make sure the chosen password is not easily guessable by not using words such as "password". Using Phrased such as "Sw33t-Home-Alabama" would be classed as a very strong 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 software / hardware, IP Scanners, BIOS cracking software, port scanners, network sniffers or any other hacking or cracking software of any description. These applications must not be installed, stored or ran on the networks 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 regularly in case of error / power cuts
- Users are not permitted to use the internet to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

Personal Use of the internet

Whilst the internet should primarily be used for business functions, incidental and occasional use of the internet in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the School
- Employees understand that School management may have access to their internet browsers and browsing history contained within,
- Employees understand that the School reserves the right to suspend internet access at any time,
- Use of the internet for personal use does not infringe on business functions.

Inappropriate Use of Internet Usage

The School does not permit individuals use the internet in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic images, cartoons, jokes or movie files,
- Images, cartoons, jokes or movie files containing ethnic, religious, or racial slurs,
- Any content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Email Use

This Email Acceptable Use Policy (AUP) applies to all Sherburn High School users.

General Principles

- Use of email by Sherburn High School staff and students using the @shs.starmat.uk (and the old @sherburnhigh.co.uk and @students.sherburnhigh.co.uk) domain, is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of the School and its business units. Email is to be used in a manner that is consistent with the School's standards of business conduct.

- School email accounts are to be used for School business.

- The School will directly access staff email accounts in the pursuit of an appropriately authorised legal or disciplinary investigation.

- Use of email may be subject to monitoring for security and / or network management reasons. Users may also be subject to limitations on their use of such resources.

- The distribution of any information through the School's network is subject to the scrutiny of the School. The School reserves the right to determine the suitability of this information.

- The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately. For example, the Police can have a right of access to recorded data in pursuit of a crime.

- Email messages are treated as potential corporate messages of the organisation.

- The School reserves the right to either redirect the email of staff that have left or delete the mailbox for legitimate business purposes. Users are responsible for ensuring personal emails are stopped.

- Individuals may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of an individual's email rights. The IT Manager at Sherburn High School will have overall responsibility for allowing access to group email accounts but this responsibility may be devolved to other individuals.

Unacceptable Use or behavior

It is unacceptable to;

- Solicit emails that are unrelated to business activities or for personal gain.

- Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.

- Represent personal opinions as those of the School.

- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the School or the School itself.

- Reveal or publicise confidential or proprietary information which includes, but is not limited to financial information, databases and the information contained therein, computer network access codes, staff and student information and business relationships.

- Waste time on non-School business.

- Use School email for personal business – please keep personal matters to your personal email address.

- Not send excessively large email attachments without authorisation from School management and the School's IT provider.

- sign up to marketing material that could jeopardise the School's IT network.

- click on links in emails from un-trusted or unverified sources.

Users should

- Keep emails brief and use meaningful subject lines – Using the subject line of the email for the message is not considered as correct email etiquette.

- Proof read messages before sending to check for clarity and to make sure that they contain nothing which will embarrass the organisation or make it liable. Emails are a form of corporate communication and therefore should be drafted with the same care as letters.

- Understand how to use - and don't mismanage - CC and BCC: only CC in people that really need to receive the email.

- Archive effectively - use folders and delete any messages you no longer need – this includes messages in the sent and deleted items.

- Don't overuse the "URGENT" or "High Priority" flag as it will lose its value.

- Never reply to spam.

- Avoid using email for sensitive or emotional messages or offensive content.

- Take care in drafting emails, considering any form of discrimination, harassment, School representation and defamation of Data Protection issues.

- Users should be careful when replying to emails previously sent to a group or pressing the Reply All button.

- Ensure your terminal is locked or logged out when you leave your desk, a malicious user could send messages in your name.

- Avoid 'Mail Storms' - long discussions sent to a distribution list - consider verbal communication or use a bulletin board.

  Report any suspicious emails to IT Support – they will recommend the next steps to take – users are not to click on any pictures, links, buttons or attachments that the email may contain if the user suspects the email is suspicious

- Users are to look out for:
  - The sender's email address doesn't tally with the trusted organisation's web address
  - The email is sent from a completely different address
  - A suspicious display name that doesn't match the email address
  - The email contains spelling and grammatical errors
  - The email uses unspecific greeting like "dear customer" as opposed to recipient's name
  - The entire text of the email is contained within an image rather than plain text
  - Indicates "urgent" action is required
  - Asks for personal credentials via email – legitimate businesses always provide contact details and never ask for personal details

- Hover the mouse over the link but NOT click it, usually the link is different to the written text. Links could also lead to malicious software allowing it to run on the device – if in doubt, contact the company to check it is legitimate.

- Unsubscribe from any marketing / advertisement emails that they may claim as junk.

- Encrypt emails using the email's Message Encryption System if the email contains ANY personal information be it in an attachment or the body of an email. Speaking to IT Support can advise on best practice.

- Staff should be able to identify what data is safe to send off site via email without being encrypted. Anything that can identify a student or adult is classed as sensitive / personal data, so just a name would not need encrypting.

- List of items to encrypt:
    - ✓ A name with any personal information such as: Address, Date of Birth, email address and / or SEN Information
- List of items not to encrypt:
    - × Tracking data, registers, lesson plans; anything that cannot be used to identify a student.

Monitoring

The School accepts that the use of email is an extremely valuable business, research and learning tool. However, misuse of such a facility can have a detrimental effect on other users and potentially the School's public profile. As a result;

- The School maintains the right to access user email accounts in the pursuit of an appropriately authorised investigation.
- The specific content of any transactions will not be monitored unless there is a suspicion of improper use.
- The School may monitor and review all email traffic that comes to and from individual and group email accounts.

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) to achieve this. 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. When emailing parents and / or students, only school email or approved parental communication systems are to be used, staff must not user their personal email when communicating with parents / students.

- 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, MIS (school database) logon details and personal network & Learning Platform logins and should log off / lock a logged in network session when leaving a workstation unattended. This can be done by pressing the "Windows Key" & the "L" key together or press "Ctrl", "Alt", "Del" together and select "Lock". 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

- Are to contact ICT Support if they are required to download known compressed files such as ZIP files from unknown sources as these could potentially contain malicious software

- Are permitted to use Personal Digital Equipment, such as mobile phones and cameras to record images and/or videos 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 and videos are easy to capture, reproduce and publish and therefore, misused.

- Are to 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.

- Video Conferencing / Webinar sessions – See the appropriate policy

- 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

- Should ensure that their use of web technologies, including social networking sites, such as Facebook, Twitter, Instagram and SnapChat does not question or bring their professional role into disrepute and must adhere the Social Media policy at all times.

  - 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.

Sixth Form 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 and/or Achievement Leaders depending on the severity of the incident. In serious cases the School Management Team will be consulted and the student 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. Students will be responsible for any work lost / edited if you leave your machine unattended.
- Students 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 or Personal Information 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.
- Students are to only communicate with staff via approved systems and platforms, the use of personal email will not be used to communicate with a member of staff

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: _____

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.**

School: Sherburn High / Tadcaster Grammar **

** Please delete / highlight as appropriate.