North Halifax

Grammar School

Student IT Acceptable Use (AUP) Policy

Approved by:	Principal
Date approved:	October 2018
Next review:	Summer Term 2021
Policy owner:	Vice Principal – Progress and Enrichment

Student ICT Acceptable Use Policy (AUP)

The computer network, equipment, subsequent systems and software are owned by the school and may be used by students to further their education. The student acceptable use policy has been drawn up to specifically protect and advise the students on ICT usage within the school.

Please be aware that we can change any element of ICT policy without notice (usually to respond to new threats to security of the network or technology changes etc), so it is important that all students ensure that they read all new communications from the ICT department.   Please read this Acceptable Use Policy thoroughly and ensure that your son/daughter fully understands it before signing to agree.

The school reserves the right to examine or delete any files that may be held on its computer systems and to monitor access to Internet sites and the use of e-mail.

It is the responsibility of students, parents or guardians as well as the school, to ensure that the security and confidentiality of the data stored on the school networks is protected, as well as protecting the rights of those that use it.

Access to Online Services

- We use an Internet filtering system which blocks sites that fall into categories such as Adult/Sexually Explicit, Intolerance and Hate, Violence, Phishing and Fraud, Weapons, Illegal Drugs, Gambling, Spyware, Chat, Proxies and Translators, Peer to Peer and Hacking. Students should be aware that any attempt to access websites that fall within these categories, or other offensive websites, will be subject to the school’s Behaviour for Learning (BfL) Policy. If the Internet Filtering system has failed to block an Internet site, then the student must report this immediately to the IT Network Manager or a member of staff.
- The Internet Filter allows the use of chat, discussion, social networking and blogging facilities that have been securely created by the school and can only be accessed by students with an active Username.
- The school will provide internal and external access to learning resources. Every student on the school network has a ‘Username’ which is unique to them and provides them with access to online resources and personal file areas. Students must be aware of the serious implications of deliberately accessing or trying to access another user’s online file area (this includes students’ and teachers’ accounts).
- The school does not permit specific files to be downloaded. These files include applications, music files and executable extensions.
- Students must never send e-mails or set up websites using someone else’s name or personal details. At best this is forgery, at worst it could place the other person in danger. Images or film of other students or staff may not be posted on the Internet or sent by e-mail without the permission of the individual concerned. Any attempt to impersonate or to make inaccurate or offensive statements about another individual in any electronic media will be dealt with through BfL.
- Students must not set up websites or groups using the school's name, initials or logo, or anything else which clearly identifies the school, without permission. If such sites are set up, then the students who operate and use them will face sanctions if they risk bringing the school's reputation into disrepute through the use of derogatory, abusive, foul or racist language or by denigrating the school or any of its members in a publicly accessible forum.
- Students should not access chat facilities via the school network, except for those that have been approved for use by the School. Public social networking sites and online photograph sharing sites should only used if specifically allowed by the teacher.
- From time to time data may be collected by the school via online forms, website or e-mail, e.g. for questionnaires, questions given for homework. If data is collected in this way, it will be kept in accordance with current Data Protection Act legislation / GDPR.
- Students should not download or upload information or files that include the following: Copyright material which you do not have permission to copy; Inappropriate content such as adult/sexually explicit; Files that could threaten the security of the network (such as executable files e.g. exe, bat, com etc); Intolerance and Hate; Violence; Weapons; Illegal drugs; Gambling; Spyware; Chat or any other information or files that is not appropriate to school work.
- North Halifax Grammar School uses the Guide for Education. This means some data will be held on secure servers outside the UK. By signing this document and/or the Home School Agreement, parents are consenting to the use of this service.
- Students who access school computers or applications via Remote Desktop facilities or other means, must use these facilities in accordance with the School Acceptable Use Policy.

‘Cyber Bullying’ / Inappropriate contact

New technologies can be used inappropriately, e.g. for bullying. This includes sending *e-mails* or *messages* containing insults or threats directly to a person, spreading hateful comments about a person or groups to others.

Any student that is found to be bullying any other member of the school community using electronic methods (cyber-bullying) such as email, blogs, chat facilities, Bluetooth, Multimedia messaging, text messages, picture messages, instant messaging will be reported to the Year Group Leader / Leadership/their parents and appropriate sanctions will be applied to the individual. If you are being bullied via electronic methods then if possible, follow the guidelines below;

- Do not respond to the communication under any circumstances
- If possible, save the message as this can be used as evidence at a later date. Don’t delete it.
- Speak to a teacher / friend / parent / carer
- Block the sender/s of the email by using the ‘Junk Email’ or ‘Spam Filter’ provided by the web mail account provider
- Report via the ‘Report-IT’ online form, available via the School website and via a link on the VLE. (http://www.nhgs.co.uk/reportit)

Students can find out more about cyber bullying on the Childline (www.childline.org.uk) website or contact them by telephone on 0800 1111.

Students should familiarise themselves with the content on the ‘Think You Know’ website (http://www.thinkuknow.co.uk) operated by The Child Exploitation and Online Protection Centre (CEOP). Students should exercise caution over whom they give their contact information to, such as email addresses and telephone numbers etc.

Email

- As a precaution against viruses, if you receive an email from somebody you do not know, then do not open it. Please email ‘stop@nhgs.co.uk’ so that it can be investigated further then delete it. If you receive an email from somebody you do know, but the content, subject or attachment of the email message is not recognised by you, then contact the person directly and query the email. It is important to do this because some viruses send email on behalf of the user to all their personal contacts if they have been infected.
- Teachers and students must use the school email system rather than personal email for contacting each other.

ICT School Network / Equipment

- If offending materials (or other breaches of acceptable use) are found (whether intentional or unintentional) on the school network, then the IT managers will locate the student responsible and liaise with pastoral teams and if appropriate the Leadership team to ensure the appropriate sanctions are enforced. This will almost certainly include contact with parents/guardians on the issue.
- All students will be allocated a username and password. It is the responsibility of each student to keep his or her password secret. This ensures that files cannot be accessed by other students. Loss or corruption of files as a result of insecure passwords is the responsibility of the individual student. From time to time the IT managers may require students to change their passwords.
- If a student forgets their username and password, they must inform the IT Department in person. No passwords will be provided over the telephone or email.
- If a student suspects another student is aware of their account password, then the student must change their password immediately and inform the IT Manager.
- The storage space allocated to each student is private. No attempt should be made to discover another user’s password or to access their files, either on the school network, or any other storage means, including online areas that the School uses.
- Students must not alter computer settings or add/remove any software (including shareware and freeware) without the written permission of the IT Manager. The illegal copying of software or the installation of unlicensed software must not take place under any circumstances.
- Any other activity which threatens the integrity of the school’s IT systems, or which attacks or corrupts other systems, is forbidden. For rules on Personal equipment, such as MP3 players,

Cameras, Mobile phones, (Including camera phones) and Game devices see the School's Year Group Handbook.

- Students may bring in their own mobile devices to school. Such devices are to be used in line with the Year Group Handbook. A member of staff may ask students to use their devices in a lesson or in another setting; if students are asked to use their devices, students do so at the discretion of the members of staff in school. Parents and/or students must ensure they have the necessary insurance to cover the device against any accidental damage or theft. Parents and/or students have the responsibility to maintain the device. Should the student use their device in school, or connect their device to the school network, via wifi or any other means, they need to abide by the school's Acceptable Use Policy and Year Group Handbook. Parents should note that access to the Internet via the school's wireless Internet (wifi) connection uses filtered access. Should the student access the Internet via their mobile network provider's network (e.g. 3G / 4G network) then the school does not have any way to control or filter any content that is delivered or sent to or via the device. Parents have the responsibility to provide adequate filtering and parental controls for such devices, for instances when students are not connected to the school's network.
- Any file storage devices/media such as Memory Cards, USB Sticks, external hard drives, CD's and DVD's should be scanned for viruses before they are used on the NHGS network.
- The school takes vandalism to computers very seriously. Vandalism includes the following;

    - Graffiti
    - Moving computer desktops / monitors away from their installed position without the permission of the IT Network Manager
    - Altering the display properties of the monitors without permission e.g. changing the colour settings using the monitor buttons etc.
    - Unplugging / Removing devices such as the keyboard, mouse, network cable and monitor cable.
    - Damaging equipment such as cutting cables, removing keys from keyboards (or swapping them around) breaking equipment due to unnecessary force.

If any student is found to have vandalised a computer, then this will be reported to the Year Group Leader/Leadership and the necessary sanctions will be applied. The IT Manager may disable the account and even delete the student's account from the network, therefore disallowing any further network access.

- Eating and drinking is strictly prohibited within the vicinity of computers.
- Any student that has been found to have taken equipment without consent will be reported to the Year Group Leader / Leadership for appropriate sanctions.
- Storing certain file types such as music files, video files, applications (including shareware, freeware or peer to peer software) or other non-educational data on the NHGS network is forbidden. All students have been provided with a file storage quota. Students must stay within this quota as they will be unable to save any further information to their personal file area if they exceed this. In addition to this, students must ensure that they regularly delete files that are no longer required as this is the usual cause of students being unable to save, although in special circumstances a student's quota can be temporarily increased.

Website

The North Halifax Grammar School website http://www.nhgs.co.uk provides information for members of the public, those affiliated with the school, visitors to the school, parents, existing students, members of our alumni, potential students and their parents and other people who have an interest in the school. The aim of the website is to provide information to such groups about our activities and to support teaching, as well as to promote the work that goes on in school (this may include students' work, photographs, sound and video).

All sites hosted by or for The North Halifax Grammar School belong to the school and should not be replicated on any other site. All content on the website, unless otherwise stated, is not to be downloaded (apart from viewing or printing off information) onto any external media or distributed in electronic form. Any attempt to copy files from the site, without prior consent, constitutes a breach of Copyright Law.

This section of this policy and the term 'school website' refer to any pages or files on our sites that have unrestricted access. It does not refer to pages that sit in a password protected (restricted) area. Any information on any of our sites, which is not restricted for certain users, constitutes part of our website.

Images of students on the school website help to promote the positive work that happens in the school and helps to motivate students involved. However, images of students may be downloaded and used for inappropriate means. To avoid this, the school takes into account the following statement when considering whether photographs and moving images of students should be included on the school's website:

> *A photograph of an individual (which is not considered a group photograph) will not normally be used. However, if such a photograph is needed, then the school will require that a separate permission form to be completed. In the event that a photograph does appear on the website in error, please inform the school at the earliest opportunity in order to get it removed. A group photograph is considered to be at least 3 students. If a group photograph is shown, first names may be given but not necessarily in the order that the students are shown. Students, who appear in photographs, must be in suitable dress and in a non-compromising pose in order to reduce the risk of inappropriate use.*

By accepting this Acceptable Use Policy, you are agreeing to allow group photographs of your son/daughter being published on our website. If you do not wish for photographs of your son/daughter to be included on the website, then please inform the school in writing.

Student Signature

I agree to abide by the above Acceptable Usage Policy.

Signature …….……………………..………… Date ……………………

Full Name ………………………………..(printed)

Authorised Signature (Parent / Guardian)

I have read this Acceptable Use Policy and explained the terms of this agreement to my son/daughter.

Signature …….………………………………..... Date …………………

Full Name ……………………………......……………………………(printed)