



The North
Halifax
Grammar
School

[NHGS ICT POLICY FRAMEWORK]

This document includes all the relevant ICT Acceptable Use Policies (AUP) that have been drawn up to specifically protect and advise all people involved with The North Halifax Grammar School on ICT usage. In addition to this policy, we have created a 'Glossary of terms' document that is available on request.

Contents

Contents.....	2
Student ICT Acceptable Use Policy (AUP).....	3
Internet / VLE (Virtual Learning Environment) usage.....	3
‘Cyber Bullying’ / Inappropriate contact.....	5
Webmail.....	5
ICT School Network / Equipment.....	6
Website.....	8

Student ICT Acceptable Use Policy (AUP)

The computer network, equipment and subsequent systems 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 for ICT usage thoroughly and ensure that your son/daughter fully understands it before signing to agree.

A glossary of terms document is attached to this Acceptable Use Policy.

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 the 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.

Internet / VLE (Virtual Learning Environment) usage

- At the North Halifax Grammar School we ensure that students that use the Internet are supervised at all times, as far as is reasonable. For sixth form students of the school we provide Internet facilities to them without direct supervision, but all Internet activity is recorded and monitored remotely per individual.
- 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. In order to maintain an accurate Internet filtering system, we consistently review the websites that we block to ensure the students are getting the most from what the Internet has to offer in terms of educational development. Students should be aware that any attempt to access websites that fall within the categories listed in the latter statement, or other offensive websites, will themselves become subject to the school's sanction policy (School detention / Isolation / Exclusion / depending on seriousness of the offence and students behavioural record) and this will result in temporary disabled account or if necessary permanently.
- If the Internet Filtering system has failed to block an Internet site, then the student must report this immediately to the ICT Network manager or a member of staff.

- The Internet Filter allows the use of chat, discussion and blogging facilities that have been securely created within the school VLE (Virtual Learning Environment) and can only be accessed by students with an active network ID. These facilities are also closely moderated by staff that create them.
- The Virtual Learning Environment provides internal and external access over the Internet to learning resources that are held by subjects to enhance learning. Every user on the school network has a 'User ID' which is unique to them and provides them with access to online information and personal file areas. Students must be aware of the serious implications (School detention / Isolation / Exclusion / depending on seriousness of the offence and students behavioural record) 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 over the Internet. These files include applications, music files and executable extensions.
- Users of e-mail in years 7 to 11 must not give their home address or telephone number, or arrange to meet someone unless their parent or guardian has given permission. Older students should be aware of the dangers of making such arrangements with strangers.
- Users must not give out personal information about themselves or other people (telephone numbers, home address) on the VLE or the Internet.
- Users must never send e-mail or set up web sites 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 in e-mails 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 as a serious breach of the school's code of conduct.
- Students should not access Chat rooms, MSN chat facilities, Instant Messaging either via application program or via website. Public social networking sites such as Myspace, Bebo and online photograph sharing sites should only be used if specifically asked for by the teacher.
- Students should report all accidental access to sites that have been blocked by the Internet filtering system immediately to the teacher or the ICT network manager. This should include the site URL and the time you accessed the site.
- From time to time data may be collected via online forms via the VLE, e.g. for questionnaires, questions given for homework. If data is collected in this way it will be kept in accordance with the Data Protection Act (1998).
- Students should not download or upload information or files to the VLE, which 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.

‘Cyber Bullying’ / Inappropriate contact

There are several ways that student and young people can bully one another using new technologies. For example they can send *e-mails* or *text messages* containing insults or threats directly to a person. They may also spread hateful comments about a person to others through e-mail, or postings on *Websites* and *online diaries* (blogs). There is a plethora of information available on the Internet that provides advice for everyone in relation to cyber bullying.

- Any student that is found to be bullying other students 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 Head of Year / Leadership, their parents and appropriate sanctions will be applied to the individual. If the student is 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 online form on the VLE
- Students should also exercise caution over whom they give their contact information to, such as email addresses and telephone numbers etc.

Student can find out more about cyber bullying on the Studentline (www.studentline.org) website or contact them by telephone on 0800 1111.

Webmail

- If a student uses a web mail account (or is considering creating one) with a particular Internet site, then they should ensure that they thoroughly read and understand their privacy statements before signing up. This is very important as their personal information (including contact information) could be passed onto other organisations that could exploit that information for their own purposes, such as sending large amounts of spam to their email account or even using contact information to send them junk mail through the post.
- Most, if not all email accounts suffer from spam emails that can contain inappropriate content and also fill up the mailbox very quickly. Nearly every web mail account provider on the Internet provides a utility for controlling spam. These are called 'Spam Filters' or 'Junk Email Filters' and they are designed to allow the account holder to set controls on what email they want

to allow and disallow to be delivered into their mailbox. If a student receives an inappropriate or offensive email they should either close it or delete it and immediately seek advice from the teacher, but never reply to it. If you are still receiving spam emails, even though you have applied filters to your account, then create a new account with a fresh email name and notify only people you trust of the new contact details.

- All E-mail communication should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers. Also be aware that using capital letters is seen as 'Flaming', which is usually interpreted as shouting your message to the recipient.
- Although our anti-virus protection system will detect viruses before you try to open them you should still be aware of how email attachments can contain viruses. If you receive an email from somebody you do not know, then the basic rule is not to open it and just 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 your friend 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.

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 ICT Network Manager will locate the responsible user and liaise with pastoral teams and even the Leadership team (dependent upon severity) to ensure the appropriate sanction actions are enforced on the matter. This will almost certainly include contact with the parents/guardians on the issue.
- All users will be allocated an account name ('user ID') and password. It is the responsibility of each user to keep his or her password secret. This ensures that files cannot be accessed by other users. Loss or corruption of files as a result of insecure passwords is the responsibility of the individual user. From time to time the ICT System Manager may require users to change their passwords.
- If a student forgets their user ID and password they must inform the ICT technicians in person. No passwords will be provided over the telephone or email.
- If a user suspects another student is aware of their account password, then the user must change their password immediately and inform the ICT Network Manager.
- The storage space allocated to each user is private. No attempt should be made to discover another user's password or to access their files.
- Users must not alter computer settings or add/remove any software (including shareware and freeware) without the written permission of the ICT System Manager. The copying of software or the installation of unlicensed software is illegal and must not take place under any circumstances.

- Any other activity which threatens the integrity of the school's ICT systems, or which attacks or corrupts other systems, is forbidden.
- Personal equipment, such as MP3 players, Cameras, Mobile phones, (Including camera phones) PDA's (Personal Digital Assistant) and Game devices should not be switched on during school hours. Further information on this can be found in the School Code of Conduct.
- Any file storage devices/media such as USB disks, external hard drives, CD's and DVD's should be scanned for viruses before they are used on the NHGS network. Please use up to date Anti-virus software to scan all files on your home computer before bringing them into school. If you are having difficulty doing this / or DO NOT have any Anti-virus software installed, then the student should contact the ICT network manager BEFORE they insert the storage device into any NHGS computer.
- 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 ICT 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 Head of Year / Leadership and the necessary Sanctions will be applied. The network manager will disable the account and even delete the student's user account from the network, therefore disallowing any further network access.

- Eating and drinking is strictly prohibited within the vicinity of computers. Any student found doing so will have their account disabled on the network and reported to the appropriate Head of Year.
- Computer equipment theft is a serious offence and should never take place. Any student that has been found to have taken equipment without consent (either by a member of staff witnessing this directly or being notified by another student) will have their network account disabled / deleted and will be reported to the Head of Year / 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 such files that have

been saved the NHGS network are located automatically on a daily basis and deleted without notification to the student.

- User's must not attempt to guess another users password or provide their account information to friends. Any users that have accessed another user's account will have their account disabled / deleted (dependent upon the severity) and reported to the Head of Year / Leadership.
- All student files that are held on the network / VLE are regularly reviewed by teachers and staff
- 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 student's work, photographs, sound and video). Other sites that the school has include: <http://www.nhgsonline.co.uk> and <https://vle.nhgs.co.uk>.

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 refers 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 on the VLE (Virtual Learning Environment) or other sites that the school owns. 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 signing 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.
