



Acceptable Use of ICT Policy

6.11

This policy should be read in conjunction with the ICT policy, Safeguarding policy, Safeguarding Code of Conduct and Child Protection policy.

This policy meets the agreed aims of Beacon Hill School in the following ways.

- **that has ambitious expectations for individual improvement to achieve excellence for all.**

Information Technology is a powerful tool which will help all young people make progress. This policy puts in place and provides for the ongoing review of systems to ensure these tools are used in a safe professional way.

- **in which all partners include, involve and inform each other.**

This policy ensures that all those involved in school are aware of its policies and procedures in relation to the acceptable use of ICT.

- **that actively develops parental partnerships for the benefit of the pupils**

This policy will be disseminated to parents to demonstrate to them the ways in which school seeks to ensure the safe use of ICT with their young people.

- **that values communication and provides the time and opportunity to make it effective.**

This policy will help meet this school aim by ensuring that technological communication systems are used for the young people and by the young people in a way which helps them learn to communicate whilst also keeping them safe.

- **that promotes an happy, healthy atmosphere of security, trust and respect.**

The security of young people is very important and will be enhanced by the measures in this policy.

- For the purposes of this document, Beacon Hill school as an establishment will be referred to as "BH".
- The BH administrators referred to herein are those members of the BH information technology (IT) support team with administrator-level access on the BH network. As of October 2011, these administrators are David Vincent and John Wardle.

- While BH desires to provide a reasonable level of privacy for its network users, users should be aware that all data stored on the BH network is property of BH. BH governors cannot guarantee confidentiality of information stored on any network device.
- For security and network maintenance purposes, authorised individuals such as the network administrators may monitor systems, equipment, network traffic, internet usage and stored data at any time.
- BH governors reserve the right to audit networks and systems on a periodic basis.
- This acceptable use policy will be reviewed on a six monthly basis and updated where necessary to reflect the speed at which technology changes. More frequent updates may be included if specific, relevant technological changes occur between review periods.


Core statements

- All users must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally.
- All users must be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.
- No communications device, whether school provided or personally owned, may be used for the bullying or harassment of others in any form.
- No applications or services accessed by users may be used to bring the school, or its members, into disrepute.
- All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.
- All users have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
- All users have a duty to report failings in technical safeguards which may become apparent when using their systems and services.
- All users have a duty to protect their passwords and network logins, and will log off the network when leaving workstations unattended. Any attempts to access, corrupt or destroy other users' data or compromise the privacy of others in any way, using any technology, is unacceptable.
- All users will use network resources responsibly. Wasting staff effort or networked resources, or using the resources in such a way so as to diminish the service for other network users, is unacceptable.

- All users will understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- All users will be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to check and/or confiscate personal technologies such as mobile phones.
- All users must take responsibility for reading and upholding the standards laid out in the AUP.
- All users should understand that the AUP is regularly reviewed and consistently enforced.

General security

- When thinking about storing data on the BH network, users should try to classify information as either confidential or non-confidential. Any document containing full names, contact details or information about a specific pupil or member of staff must be deemed confidential. If a user is in doubt about the level of confidentiality required when storing a document, they must treat it as being confidential.
- Confidential information must be kept securely on an account that only one person plus administrators have access to. The BH individual accounts were designed for this purpose, the "My Documents" storage on each account can only be accessed by the user and the administrators. Users will take all necessary steps to prevent unauthorised access to confidential information.
- All members of staff at BH and users of the BH computer infrastructure that are not employed by BH will be given access to an individual account with personal storage space. These accounts, depending on employment role, will also be connected to certain "shared areas" for sharing files between users.
- Each classroom will be given use of a class account to quickly and easily allow pupils' access to computers. These classroom accounts must be used as intended and not used as a one-stop account for every purpose. The teacher or acting teacher of each class is responsible for this account and will ensure that it is being used appropriately.
- BH network administrators have access to all user accounts but will not abuse this ability to invade the privacy of members of staff.
- Passwords must be kept secure and accounts must not be shared. It is vital that only the user has access to their personal account. Never give an administrator or other member of staff your password, even for maintenance purposes, as an administrator can reset your password via the BH server.

- Passwords must consistently maintain a level of strong complexity. Simple passwords using only lowercase letters such as "car" are unacceptable. Numerical and alphabetical formats of the user's birth date should be avoided, as should simple versions of a user's child's name such as "301185" or "monica". Where possible, passwords will contain at least one uppercase letter and one digit, and be over eight characters long. Certain applications allow the use of special characters such as hyphens (-), slashes (/ and \) and exclamation marks (!). Again, if possible, one of these characters should be employed in passwords to heighten complexity.
- An administrator will change system level passwords every three months.
- Users will change their individual passwords every six months. If the user is unsure of how to change a password in a certain application, they should contact an administrator.
- When users leave a workstation during the day, they must select the "Log Off" option from the Start Menu, allowing other users to quickly and easily access the computer after them, whilst keeping the previous user's account secure. If a user is leaving a workstation after 16:00, they must select the "Shut Down" option from the start menu. If a user leaves their workstation temporarily, they must press the "Windows start key"  and the "L" key at the same time to lock the computer, then use the on-screen instructions to unlock it when they return.
- Users leaving accounts logged on whilst not at a PC may have their account logged off by an administrator, for security purposes. Please avoid this as it may incur data loss.

USB Device Usage

- All teachers at BH and other members of staff that are deemed to require a memory stick will be provided with specific 100% encrypted memory sticks. No other memory stick will be granted access on BH computers unless a BH network administrator is first consulted.
- The utmost care must be taken when using memory sticks on the BH network. Avoid storing confidential information on a memory stick for any length of time, including photographs of any person. If confidential information has to be transferred, it is strongly recommended that an encryption tool such as WinRAR be used to create an encrypted, passworded archive to contain the confidential information. Such an encrypted archive should be used on top of the hardware encryption provided by the encrypted memory sticks used at BH. The archive

and the confidential information must be deleted from all but one source, which must not be the memory stick, when the transfer has been completed.

- If you are given a memory stick to use on the BH network by someone that isn't a user of the network, for whatever purpose, do not use it on a BH network computer. It must be first given to a network administrator to test on a non-networked machine. Bear in mind that users may not be malicious, but viruses can be transferred from personal computer to memory stick without the user knowing.
- If a memory stick is lost, a network administrator must be informed as soon as possible, and they will ask you to try and recite the contents of the stick.
- External hard drives must be registered with a network administrator and if deemed virus free and safe for use, will only be granted temporary usage.
- An external program will be used to monitor and whitelist USB devices so that unknown USB devices cannot be used on BH network computers.
- Only cameras provided by BH can be used on machines connected to the BH network as such devices can also be used as memory sticks.

E-Mail Usage

- BH network administrators and governors have access to, and reserve the right to, check e-mails sent from the domain.
- It is acceptable for staff to send personal e-mails *before* 08:45, *between* 11:45 and 13:15, or *after* 15:40. Users must be aware that all e-mails sent are sent from a BH e-mail address and as such have to be carefully considered before sending.
- Personal e-mails between staff must follow the same rules as those sent to persons not employed by BH.
- Personal e-mail accounts accessed via websites such as Hotmail, Yahoo and Google are deemed inappropriate for school usage because BH can't control the content displayed. Access will be available at all times in case of emergency but a line-manager must be consulted before using such an account. All internet access is monitored as per "Internet Usage" chapter.
- The use of inappropriate, derogatory or insulting is not acceptable in communication to or from a BH e-mail address. Any illegal topics broached in e-mail including racial slur, will be dealt with by the police.
- Personal e-mails sent during working hours must first be granted permission by a line-manager. Personal e-mails sent during work hours without permission will be treated as a misuse of paid time.
- E-mail attachments must be considered carefully when sending or opening. It is safe to presume the majority of files on BH network are virus-clean, but files with the following extensions may need advice from an administrator if they

need to be e-mailed as they can automatically be deemed virus-ridden by some e-mail hosts: .exe, .js, .vb, .vbs, .rar.

- While BH is using the North Tyneside Learning Platform (ntlpl) system, it is generally safe to presume that attachments have been virus checked by NTC systems. If a user is unsure about the safety of an attachment, they should contact a network administrator before opening the file(s).
- E-mails sent to organisations outside of BH must be composed in a professional manner without the use of informal abbreviations, acronyms or emoticons (such as ☺ smiles/faces).

Internet Usage

- All internet access at BH is monitored and checked on a continuing basis by the Local Authority (LA).
- BH internet access is provided by North Tyneside Council and uses their bespoke primary school filtering hardware and software to offer the most appropriate protection for BH usage.
- The filter disallows access to Facebook, MySpace, Twitter, YouTube and a number of other social networking websites. This is for the protection of BH's pupils and general school reputation.
- The filter allows access to most shopping websites such as Next, Burton, Marks and Spencer and so on. The filter also allows access to most online banking websites. Members of staff at BH may use such websites *before* 08:45, *between* 11:45 and 13:15, or *after* 15:40, as long as these websites aren't being used during paid time.

Users must not:

- Visit internet sites that contain obscene, hateful, pornographic or otherwise illegal material.
- Use any computer on either BH site to perpetrate any form of fraud or software, film or music piracy. Only sample music clips of up to 30 seconds can legally be used and stored on the BH network.

BH Pupils and Internet/E-mail Usage

- Pupils will always be supervised when accessing the internet.
- When a pupil is composing an e-mail, the contents and e-mail address the e-mail is being sent to must be supervised and accepted before the e-mail message is sent.

- Any inappropriate e-mails sent or received will be dealt with as quickly as possible by filling in an incident form and notifying a line manager or network administrator.

Mobile Phone Usage

- Personal mobile phones must not be carried around school in pockets or bags. They must be locked away securely.
- Personal mobile phones may be checked and/or carried outside/into the staff room *before 08:45, between 11:45 and 13:15, or after 15:40.*
- Personal phone calls or the sending of text messages must not be made outside of these hours without permission from a line-manager.
- BH will provide specific work mobile phones to those members of staff deemed to require one. If the phones are equipped with cameras, the lenses will be scratched off to remove the phone's ability to take pictures.
- The taking of pictures from a mobile phone on BH's grounds is unacceptable unless specific permission is granted from a line-manager, for instance if a digital camera isn't available at the time.

Social Networking

Taken from Safeguarding Policy

Adults will:

- Uphold the law and maintain a good standard of behaviour both inside and outside of school; both online and offline. The content in cyberspace does not elude the law - a posting in the public domain can still constitute a defamatory publication. Employers can take disciplinary action if they can prove your conduct has caused detriment.
- Note that they may lose respect in their post and defamation of character by placing things in the public eye that relate to their role or other members of staff.
- In all instances, not disclose anything on social networking sites that are related or could be related back to their work. If it is necessary to disclose information by these means it is advised to do so via private means and not, for example, on a 'Face Book' wall.

Propriety and Behaviour

Adults will not:

- Place images and videos of themselves on a public space on the internet such as 'YouTube', or 'Facebook', which could show themselves or other members of council staff in a way which could damage the council's reputation must be

avoided and the council will take seriously any action deemed to show a lacking in standards both online and offline.

- Discuss other members of staff or students in a negative fashion in a public space on the internet goes against the 'Code of Conduct' and does not treat people with respect and courtesy.
- All staff have the responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children and young people.
- Members of staff must not become "friends", "link" with or "follow" parents or guardians of children at Beacon Hill on social networking sites. It will be made clear to parents that this is inappropriate. Such requests must be mentioned to a line manager.
- Any unauthorised contact between parents and members of staff at Beacon Hill must be recorded on an incident form.

Communication with Children and Young People

- Communication between children and adults by whatever method should always take place with clear and explicit professional boundaries.
- Staff must not share any personal information with any young people or children. They must not respond to requests or request any personal information from the child/young person, other than that which may be appropriate as part of their professional role.
- Staff will ensure that all communications are transparent and open to scrutiny.