BEACONSFIELD HIGH SCHOOL

A remarkable Grammar School

ACCEPTABLE USE POLICY FOR ICT SYSTEMS AND THE INTERNET

Date reviewed: November 2018

Next review date: November 2021

For review by: People, Performance & Pay/ FGB

Beaconsfield High School

ACCEPTABLE USE POLICY FOR ICT SYSTEMS AND THE INTERNET

November 2018

Aim

This policy aims to:

- Promote the professional, ethical, lawful and productive use of Beaconsfield High School's ICT systems and infrastructure.
- Define and identify unacceptable use of the school's ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites.
- Specify the consequences of non-compliance.

All users of the school's ICT systems and Cloud-based ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Statement (attached); while students confirm acceptance of the policy each time they log in to the school's ICT systems. Beaconsfield High School reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the school of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018 together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information. The School is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated in to U.K. law by the Human Rights Act 1998.

If you are in doubt and require clarification on any part of this document, please speak to the ICT Support Team.

Provision of ICT Systems

All equipment that constitutes the school's ICT systems is the sole property of Beaconsfield High School. Student devices permitted under our 'bring your own device' (BYOD) scheme are discussed in a separate paragraph.

No personal equipment should be connected to or used with the school's ICT systems (excluding removable media or devices, such as USB memory sticks and headphones). Users must not try to install any software on the ICT systems without permission from ICT Support, as this could jeopardise the integrity of the school's ICT systems and/or be in breach of copyright law or licence

agreements. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

It is the responsibility of ICT Support to purchase and/or allocate ICT equipment to individuals and subject areas. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Consequently it is the user's responsibility to back up any school or private work and/or data that may be stored on the user's computer hard drive. ICT Support cannot accept any responsibility for data loss incurred through regular maintenance of a computer, through hardware failure or malware attacks. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Beaconsfield High School cannot be held responsible or liable for the loss of any personal or private data stored on its ICT systems.

Users are not permitted to make any physical alteration, either internally or externally, to the school's computer and network hardware.

Access to the ICT Systems and Internet Policy

This policy is available on the school website for parents, staff, and students to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are included in Student Planners, for ease of reference you can see a copy of these guidelines on pages 13-14 of this document. E-safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHCE lessons where personal safety, responsibility, and/or development are being discussed.

Network Access and Security

All users of the ICT systems at Beaconsfield High School must first be registered. This Acceptable Use Policy forms part of the registration process and all users are expected to read and agree to this policy. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. Other application account credentials, such as SIMS.net and/or the VLE, may also be issued to the individual. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated.

Each user is personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not give or divulge them to any other person, except to designated members of the ICT Support team for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to ICT Support as soon as possible.

Access to user's accounts will only be granted in exceptional circumstances, for example where there is an urgent need and the user is not contactable. The exception to this is where access to another person's mailbox or calendar is granted, through the delegation facility, for shared mailboxes or the purpose of arranging meetings or checking schedules. Any attempt to access or use another person's user account is strictly prohibited.

Users must not leave any computer logged onto the school network unattended, unless it has been locked, as this could pose a security risk to the computer network and the school. Activity that

threatens the integrity of the school ICT systems, or activity which attacks or corrupts other systems, is forbidden.

Users' Internet activity, whether for professional or private use, must not knowingly compromise the security of the data on the school ICT systems or cause difficulties for any other users. User actions or inactions which intentionally, or unintentionally, aid the distribution of malicious software, such as viruses, are forbidden; this includes hoax virus messages. Users are also forbidden to create computer viruses or any other forms of malicious code. It is the user's responsibility to ensure that they do not download or run software that might contain malicious code. If users are in any doubt as to the authenticity or credibility of a piece of software, they must not download or run it.

Mobile 'phones (such as Smart Phones) and Internet dongles (such as 3G USB dongles), must not be used as a means of connecting any of the school's ICT systems to the Internet; thereby bypassing the school Internet connection(s). The school Internet connection(s) are protected by physical firewalls, web filters and antivirus/malware software; a user's mobile device is not and therefore poses a major security risk to the school network and ICT systems.

Using the Internet

Internet access is provided for academic and professional use, with reasonable personal use being permitted. Priority must always be given to academic and professional use. Personal use should be limited to short periods during recognised break times and comply with this acceptable use policy.

The Internet bandwidth is finite and therefore users must be considerate when accessing high bandwidth sites, as this may affect all other users on the school network. High bandwidth sites include video and audio streaming.

Access to or content on certain web sites may be blocked by a content filtering service in order to protect the user and the school. Beaconsfield High School cannot be held responsible or liable for any damage caused to the user by the accidental viewing of untoward material. Please note that 'untoward material' may be down to individual perception. The content filtering service is provided on a "best efforts" basis; it is not perfect and if users do accidentally access untoward material they should inform ICT Support immediately.

Staff must not therefore access from the School's system any web page or any files downloaded from the web which, in the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. As a general rule, if any person within the School (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the School's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

a. Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
b. transmitting a false and/or defamatory statement about any person or organisation;
c. sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
d. transmitting confidential information about the School and any of its staff, students or associated third parties;

e. transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School);
f. downloading or disseminating material in breach of copyright;
g. engaging in online chat rooms, instant messaging, social networking sites and online gambling;
h. forwarding electronic chain letters and other materials;
i. accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.
Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Conduct and Discipline Policy and procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.
If necessary such information may be handed to the police in connection with a criminal investigation.

Social Networking Sites

The use of social networking sites, such as Facebook, Twitter and YouTube, is becoming part of everyday life for many people and they can be a useful learning tool to engage and communicate with audiences if used well. Unfortunately, it can be all too easy for people to vent their frustration or anger on these sites in the heat of the moment, without truly thinking through the ramifications of what they have said, and for all to see. The misuse of social networking sites can have a negative effect on an organisation's reputation or image (and individuals within the school). In addition, thought must be given to safeguarding Beaconsfield High School's students and enforcing acceptable boundaries to protect users from accusations being made against them.

Therefore to help users at Beaconsfield High School decide what is and is not appropriate content to post on a social networking site (including School owned social networking sites or virtual learning environments), and help define the boundaries to safeguard students and staff, the following guidelines and restrictions most be adhered to:

- All users have a responsibility to ensure that they protect the reputation of the school, staff and students at all times and that they treat colleagues, students and associates of the school with professionalism and respect whilst using social networking sites.

- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the school's reputation, or the reputation of individuals within the school are compromised by inappropriate postings.

- It is important that users, to the best of their ability, try to protect themselves and all other users from allegations and misinterpretations that can arise from the use of social networking sites.

- Safeguarding students is the responsibility of all users and it is essential that users consider this and act responsibly when using social networking sites.

- Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the permission of the Headteacher.

- The use of the school's name, logo, or any other official representation of the school must not be used on any social networking site without prior written permission from the Headteacher.

- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.

- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school is strictly forbidden.

- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.

- Users must not write or say anything offensive, threatening, derogatory, defamatory or inappropriate about the school or anyone at or connected with the school on social networking sites.

- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook). If, in exceptional circumstances, users wish to do so (for example their child is a student at Beaconsfield High School), please seek advice from the designated person for child protection, to ensure that you are adhering to the school's safeguarding policies.

The school's Child Protection Policy provides further details about safeguarding and the use of social networking sites.

If in doubt about any aspects of the use of ICT and safeguarding, it is the user's responsibility to consult the school's Designated Safeguarding Lead for child protection.

School owned social network site accounts must not be used for the promotion of personal financial interests, personal campaigns or the personal opinions of the user.

Any users found in breach of this acceptable use policy in regards to social networking sites, will be expected to remove the offending material immediately upon request by the Head teacher. Depending on the circumstances, they may also be subject to disciplinary action up to and including termination of employment.

E-mail

The guidelines and restrictions related to social networking sites apply to e-mail. Additionally, where e-mail is provided, it is for academic and professional use, with reasonable personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this acceptable use policy. Users are responsible for all e-mail sent from their account and for any contacts made that may result in inappropriate e-mail being received.

All e-mail, whether internal or external, should be written to a professional standard of language and content. Remember e-mails are often forwarded without the original author's knowledge or may be inadvertently sent to the wrong person. The content of all e-mails should be checked, including the spelling and grammar, before being sent, because once the e-mail has been sent you have no further control over it. Personal names should not be included in the Subject line and 'Reply to all' should be used sparingly and only when essential.

Communication by e-mail is not a secure means of transmitting information. An e-mail can be intercepted or sent to the wrong person or organisation. It can easily be copied and widely distributed. These factors must be carefully borne in mind when sending e-mail messages. Posting anonymous messages and forwarding chain letters is forbidden.

The commercial and legal effects of sending and receiving e-mails are the same as any other form of written communication, as if it were written on school letter headed paper. The style, tone and content of e-mails have a direct impact on the way Beaconsfield High School is perceived by others. E-mails can contractually bind the school and any advice, opinion, guarantee, representation or other statement contained in an e-mail may be relied upon by parents, suppliers or other third parties. As e-mails are archived, they can be reproduced and used in evidence in legal or other proceedings.
You must not send e-mails which make representations, contractual commitments or any other form of statement concerning the school unless you have specific authority to do so. You also must not send e-mails that could reasonably be construed as defamatory, discriminatory, threatening, harassing, obscene or otherwise offensive.

Never open an e-mail attachment if you do not know or trust the sender, as the attachment may contain malicious code which could damage the integrity of the school's ICT systems. Any e-mails that you are unsure of should be deleted and their source reported to ICT Support.

Beaconsfield High School does permit users to connect their personal devices, such as Smart Phones or tablets, to their school mailbox on the condition that the device has either a PIN code or security key sequence set and the device automatically locks after a few minutes if left unattended. This is to protect any confidential or sensitive information that may be contained within the user's school emails and to stop other people using the user's email account. Please note that if an unlocked personal device is stolen or lost and someone gained access to the user's emails, this could potentially become a major breach of data protection and the safeguarding of students at Beaconsfield High School. Such a loss/theft must be reported immediately to allow school staff to take appropriate ICT action.

Remote Desktop

The remote desktop is an extension of the school network and therefore is subject to exactly the same conditions of use, as set out in this policy. Please bear in mind that anything you do whilst connected to the remote desktop, will appear to the rest of the world as coming directly from Beaconsfield High School's ICT systems.

Content Ownership and Intellectual Property Rights

All content on the ICT systems is the property of Beaconsfield High School. Copying or using material from the school ICT systems is prohibited unless you have been authorised to use the data as part of your role within Beaconsfield High School. Intellectual property rights and copyright ownership of any data, software, media content and/or design work created from the activities of students and/or staff employed by Beaconsfield High School, shall be vested in full in Beaconsfield High School, together with all associated development and marketing rights.

Staff leaving the school who would like to use material or resources that they have created or helped to develop during their time at Beaconsfield High School, at their new place of employment, must request permission from the Headteacher. Any such request would not be unreasonably refused. This also applies to all non-confidential material or data stored on the school's ICT systems. This statement does not include a user's own personal files. Under no circumstances should confidential data be copied for later personal or professional use.

Students leaving the school may retain any work they have created.

Monitoring of the ICT Systems

The school may exercise its right to monitor the use of its ICT systems. This includes, but is not limited to, websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the school's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the Designated Safeguarding Lead to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or Prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

Cyberbullying

The school, as with any other form of bullying, takes Cyberbullying, very seriously. Our policy and procedures in place to prevent and tackle bullying are set out in the school's **Anti-bullying** and **Behaviour for Learning** policies**.** The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. All students are required to sign the **Anti-Bullying and Cyberbullying Contract** in their Student planner.

Recruitment

The School may use internet searches to perform pre-employment checks on candidates in the course of recruitment. Where the School does this, it will act in accordance with its data protection and equal opportunities obligations.

Bring your own device (BYOD)

The school operates a Bring Your Own Device (BYOD) scheme in some year groups; this is separate from the permitted use of mobile phones which the school allows for all year groups outside of lesson times only.

BYOD is a scheme which allows students to bring to school their personally owned device to aid their learning typically a tablet or laptop device. BYOD usage is currently permitted in Key Stage 5 only. We continue to investigate an extension of the BYOD scheme to Key Stage 3 and 4.

Students use their devices under the conditions set out in the BYOD User Agreement. The key conditions for use of a device in school are set out below:

- The device is a tool for learning, not for playing games or engaging in social networking.
- Use of a device is only permitted with a teacher's permission.
- Use is only permitted in the designated areas. These are:
    - Classrooms during lesson time or tutor time when instructed by a teacher/tutor

- The Learning Resource Centre (LRC) with permission of the Librarian
- At extra-curricular activities such as drop-ins and clubs under the direct instruction and supervision of the teacher or staff member in charge

The school expects students and parents to accept sanctions issued for not meeting the expectations set out in the user agreement. Sanctions will be issued in accordance with our Behaviour Policy.

Privacy

It should be noted that members of the ICT Support team with the appropriate privileges have the ability to access all files, including e-mail files, stored on the school computer network. However, the appropriately privileged ICT Support staff will take all reasonable steps to ensure the privacy of the users and maintain professional discretion.

Access to a user's personal area of the school network, including files and e-mails, will not be given to another member of staff or an external organisation, unless authorised by the Headteacher. Such access will normally only be granted where a breach of the law or a breach of this policy is suspected, or when a documented and lawful request from a law enforcement agency, such as the police, has been received. Access to a user's personal files may also be granted where the user has left the employment of the school, to enable a managed transition of roles and responsibilities.

Data Security

Users are responsible for ensuring that confidential or sensitive data belonging to the school is kept safe and secure at all times. Users must therefore:

- Ensure that sensitive information cannot be viewed on a computer screen and/or external display (such as a data projector) by unauthorised individuals.
- Take care when printing sensitive information, checking the printer to which the information is being sent.
- Take care when sending sensitive information via e-mail, checking the addresses and number of people to whom it is being sent.
- Lock any unattended computer, irrespective of the location on the school site.
- Only allow another member of staff, student or visitor to use their user account when they are under direct supervision by the user for the entire duration that they are logged on.
- Not save any confidential or sensitive data onto removable media or devices, unless the media or device is encrypted to an appropriate standard, as defined by ICT Support.

Remember that both laptops and memory sticks are considered to be removable storage devices and it is important to safeguard both of them at all times. This is particularly true with memory sticks, as the data they contain is not normally protected by a password and is therefore easily accessed. Staff laptops are encrypted to an appropriate standard.

Before any data that you think may be confidential or sensitive is saved to an unencrypted removable storage device or media, think about the implications of it accidentally getting lost or stolen. What would be the consequences if the device or media was found by a student or a member of the public? Could the information be used against the school or even worse, one or more of the students? If in any doubt do not save the data to the device or media.

If sensitive data has to be put onto removable media or devices, then the user is responsible for its security. If any media or device with sensitive data on it is lost (even if it is encrypted), the loss must be reported to the user's line manager immediately, with as much information about the content of the data as possible.

Whilst Cloud storage systems can seem a safe and easy way to store and access data from both work and home, there can be clauses in the Terms and Conditions of these sites which allow the provider to access, read, copy and in some cases take ownership of any documents or data saved to their servers. For these reasons it is imperative that users do not save any school related data onto Cloud storage systems, such as Dropbox or SkyDrive, unless they have been approved by ICT Support. Under no circumstances should confidential or sensitive data be saved to any Cloud storage systems, as the administrators of these systems always have access to the data.

Under no circumstances should confidential or sensitive data files be emailed, sent in the post or uploaded to non-secured websites, without first being encrypted to an appropriate standard, as defined by ICT Support.

General Data Protection Regulation (GDPR) & Data Protection Act 2018

Beaconsfield High School is committed to protecting the rights and privacy of all individuals in accordance with GDPR and the Data Protection Act 2018. This includes all users of the ICT systems. The school needs to process certain information about its staff, students, and other individuals with which it has dealings for administrative purposes, e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and the government. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

It is the responsibility of every user of Beaconsfield High School's ICT systems to ensure that GDPR and the Data Protection Act 2018 is followed and adhered to. Any breach of the Act will be considered an offence and will be dealt with according to the school's disciplinary procedures.

As a matter of good practice, any individuals or other agencies working with the school, who will have access to other individuals' personal information, will be expected to have read, signed and comply with this policy. It is expected that individuals or departments within the school, who deal with external agencies, will take responsibility for ensuring that such agencies comply with the Act.

If you have any concerns regarding what is or is not acceptable use of the information stored about individuals on the school's ICT systems, please contact the ICT Support Manager.

For more information regarding Data Protection please see the School Data Protection Policy.

Copyright, Designs and Patents Act 1988

The Copyright, Designs and Patents Act 1988, together with a number of additional laws that have amended and extended it, controls copyright law. The Act makes it an offence to copy all or a substantial part (which can be quite a small section) of a piece of work that has been copyrighted. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation.

Copyright covers materials in print and electronic form. It includes words, images, sound, moving images, TV broadcasts, computer software code and many other media types.

For more information regarding the Copyright, Designs and Patent Act 1988, please see:

Copyright, Designs and Patent Act 1988: http://www.legislation.gov.uk/ukpga/1988/48/contents

Staff Termination of Employment

When an individual leaves the employment of Beaconsfield High School, any of their files, including e-mail, left on the school's ICT systems will be considered the sole property of the school. The school reserves the right to delete the files and close the user's account. When leaving the employment of the school, users should make arrangements to transfer to colleagues any files and/or e-mail held under their personal account that may be of value or use to the school.

Student Termination of Enrolment

When a student leaves Beaconsfield High School, any files, including e-mail, left on the school's ICT systems will be considered the sole property of the school. The school reserves the right to delete the files and close the user's account.

Legal Responsibilities

Users are personally responsible for ensuring that their use of the school's ICT systems, Internet, Cloud-based ICT systems and social networking site accounts is lawful. Failure to do so may result in:

- access to the school's ICT systems, Internet, Cloud-based ICT systems and/or social networking site accounts being withdrawn;
- a disciplinary procedure being initiated;
- prosecution in a court of law.

The following uses of the school's ICT systems, Internet, Cloud-based ICT systems and social networking site accounts are forbidden:

- personal financial gain, gambling, political purposes, advertising or criminal activity;
- accessing pornographic, racist or offensive material, unless it is for genuine school curriculum research;
- viewing and/or storing unlawful text, imagery or sound;
- retaining or distributing material which is offensive, obscene or abusive;
- causing annoyance, inconvenience or needless anxiety to others (cyber bullying);
- writing or saying anything offensive, threatening, derogatory, defamatory or libellous about another individual or company.

Users accessing inappropriate sites or content will have their permission to use the school's ICT systems withdrawn and may face disciplinary procedures.

Software Intellectual Property Rights, Copyright and Terms and Conditions must be respected and adhered to at all time. It is illegal to use or copy in part or full, any software without the licensor's permission, unless it is classed as freeware. Downloading, distribution, or storage of software or other electronic media, for which the user does not hold a valid licence or valid permission from the copyright holder, is strictly prohibited.

Any software that has been licensed under a school agreement and has been installed on a user's privately owned computer must be uninstalled upon termination of employment. Any school owned

data, such as documents and spreadsheets, stored on user's privately owned computers, memory sticks or other removable storage device or media, must be returned to the school and then deleted from the original device, upon leaving the school, unless permission to keep the data has been granted in writing by the Headteacher.

Users who use services external to the school ICT systems are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this policy and be dealt with accordingly. The use of Beaconsfield High School's credentials to gain unauthorised access to the facilities of any other organisation is forbidden.

Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal (for a member of staff) or permanent exclusion (for a student).

Non-employees in breach of this policy may have action taken against them, which may include terminating their engagement, appointment or contract under which they provide services.

Any unauthorised use of the school's ICT systems, Cloud-based ICT systems, the Internet, e-mail and/or social networking site accounts, which the Headteacher considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Definitions

User	Any person granted access to Beaconsfield High School's ICT systems, including but not limited to: ▪ Governors, employees and students ▪ Temporary and voluntary staff ▪ Employees of partner organisations ▪ Contractors and subcontractors ▪ Agents ▪ Work experience placements
Individual	Any person in the employment of, working voluntarily for or being educated by Beaconsfield High School, including any other external individuals with whom the school has dealings.
ICT Systems	Refers to the hardware and software that constitute the school's computer network, including any standalone computer equipment.
Personal Files	Files created by the user for their own personal use which do not relate to the user's work at Beaconsfield High School.
Offensive Material or Content	This may include but is not limited to: ▪ Pornographic or sexually explicit material ▪ Racist, sexist or homophobic material ▪ Tasteless material (such as depiction of injury or animal cruelty)
Malicious Code / Software (Malware)	Software or program code that has been designed to be annoying, intrusive or hostile that can infiltrate, damage or retrieve information from a computer system without the owner's informed consent. This includes computer viruses, worms, trojans, spyware, adware and any other malicious and unwanted software.
Complex Passwords	The password: • Must be a minimum of 8 characters • Must contain at least one number • Should contain punctuation and symbols • Must include UPPER and lower case letters
Remote Desktop (RD)	In the case of Beaconsfield High School, the RD is a secured private network that uses the Internet to connect remote users to Beaconsfield High School's computer network.
Network Account	Consists of a username and password issued to a user, which allows them to log onto and use the school's ICT systems
Application Account	A user account, different to a user's network account, used to access an application hosted on the school network or the Internet, for example. SIMS.net or the VLE.
User Account	Refers to both a user's school network account and/or application account(s).

Social Networking Sites	Defined by, but not limited to, websites such as Facebook, LinkedIn, MySpace, Bebo, Twitter, blogging sites, public forums, public media sites for posting material such as videos, images or comments on, such as YouTube, and any other sites which make available personal views to the general public.
Cloud-based ICT Systems	Refers to software or web applications that are hosted outside of Beaconsfield High School and accessed through the Internet, which the school subscribes to.
Cloud Storage	Defined by, but not limited to, websites such as DropBox and SkyDrive; where users can save their work on a hosted storage platform, which is accessible from anywhere in the world.

Staff Acceptable Use Statement

By signing this Acceptable Use Statement you:

- Confirm that you have read and understood the ICT Systems and Internet Acceptable Use Policy in force at the date of signature.
- Agree to abide by the terms and conditions set out in the policy.
- Agree to take note of and adhere to any changes to the policy that are agreed by Governors from time to time and which are communicated to all staff.

Signed: _____

Print full name: _____

Date: _____

Please return the signed Staff Acceptable Use Statement to the Headteacher's PA.

Anti-Bullying and Cyberbullying Contract

I believe that everybody should enjoy our school equally and also enjoy a peaceful life at home while on the Internet and feel safe, secure and accepted regardless of colour, race, gender, sexuality, popularity, athletic ability, intelligence, religion and nationality.

As a student I understand that:

- bullying can be pushing, shoving, hitting, and spitting, as well as name calling, picking on, making fun of, laughing at, and excluding someone
- cyberbullying is when an individual is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by someone else or a group of individuals using the Internet, digital technologies and/or mobile phones
- bullying and cyberbullying cause pain and stress to victims and is never justified or excusable
- the victim is never responsible for being a target of bullying or cyberbullying
- if the bullying is identified as harassment or threatening it becomes illegal

By signing this contract, I as a student agree to:

- value student differences and treat others with respect
- not become involved in bullying or cyberbullying incidents, or be a bully or cyberbully
- report all incidents of bullying/cyberbullying honestly and immediately, to a Form Tutor or Head of Learning
- support students who have been or are subjected to bullying/cyberbullying
- talk to teachers and parents about concerns and issues regarding bullying/cyberbullying
- acknowledge that if I see someone being bullied/cyberbullied and I don't report or stop the bullying/cyberbullying, I understand that I am just as guilty
- be aware of the support systems with regard to bullying/cyberbullying
- support school policies, to help the school deal with bullying/cyberbullying effectively
- provide a good role model for younger students and support them if bullying/cyberbullying occurs

By signing this contract, I as a parent agree to:

- support the school's anti-bullying policies, to help the school deal with bullying/cyberbullying
- help my child to understand the importance of not becoming involved in bullying or cyberbullying
- help my child understand how damaging bullying and/or cyberbullying can be for the victim
- monitor my child's usage of the Internet – particularly with regards to inappropriate use of social networking sites and make use of parental controls where necessary

- be aware that parental controls on home computers do not extend to mobile phone technologies which can use different networks to access the Internet
- support any sanctions that my child may receive if they are involved in bullying or cyberbullying

I and my parents understand that failing to follow this contract may have the following consequences:

Where bullying and/or cyberbullying incidents are found to have occurred in school time then the school will follow its policy on anti-bullying using one or more of the following:

- internal investigations
- meetings with anti-bullying mentors
- meetings with parents
- restorative justice (face to face meetings among the victims and the bullies/cyberbullies)
- support from the school counsellor
- exclusion from ICT suites at lunchtime and after school if necessary
- detentions
- internal isolation
- fixed term exclusion
- police involvement

Where incidents have occurred outside of school time the school will:

- inform the parents if they have knowledge that bullying and/or cyberbullying is happening outside of school
- offer some support to parents but it is the parents' responsibility to manage the situation
- periodically deliver bullying/cyberbullying messages via assemblies, PSHCE and tutor programmes

Student name (print)		
Student signature		Date:
Form Tutor signature		Date:
Parent signature		Date: