BEACONSFIELD HIGH SCHOOL

A remarkable grammar school

ACCEPTABLE USE POLICY
For ICT Systems and the Internet

Beaconsfield High School

Acceptable Use Policy

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), Trustees, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.
However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.
This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and Trustees
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including Trustees, staff, pupils, volunteers, contractors and visitors.
Breaches of this policy may be dealt with under our discipline policy.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including Trustees, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 4 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).
Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school

- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher (or Business Manager in their absence) will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

This use should be brought to the Senior Leadership Team in advance of the activity, for example Use of AI systems when specifically studying and discussing AI in schoolwork, e.g. in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on discipline.

All policies can be found on the 'Staff Home' SharePoint.

5. Staff (including Trustees, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's ICT manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.
Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Team immediately.
Requests for equipment or file access should be made to helpdesk@beaconsfieldhigh.school

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).
All work-related business should be conducted using the email address the school has provided.
Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
If staff send an email in error that contains the personal information of another person, they must inform the Data Manager immediately and follow our data breach procedure.
Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business. School phones must not be used for personal matters.
Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Headteacher (or Deputy Headteacher or Business Manager in their absence) may withdraw or restrict this permission at any time and at their discretion.
Personal use is permitted provided that such use:

- Does not take place during contact time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos). Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken. Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's privacy policy. Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them. Staff should take care to follow the school's guidelines on use of social media (see appendix 1 and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. Social media settings should be set to the highest possible privacy settings.
The school has guidelines for staff on appropriate security settings for Social Media accounts (see appendix 1).

5.3 Remote access

Remote Access is managed by the ICT Team. Two factor authentication must be used when accessing the school systems via remote access.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the ICT Manager / Business Director or Headteacher may require against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.
Data protection policies can be found in the Staff Home SharePoint.

5.4 School social media accounts

The school has an official Instagram account, managed by the Communication and Development Manager. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.
The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.5 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school filters access to websites for all users accessing the school network. This is done via Net Sweeper on the school network, and Senso which is installed on all managed devices (Y7 & Y8 devices purchased through the school, plus desktop devices)
Monitoring is carried out by the DSL team, who receive weekly Net Sweeper reports on accessed websites and Senso notifications for those linked devices.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.
Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

Students have access to ICT facilities at the below:

- 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

6.2 Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out, **and/or**
- Is evidence in relation to an offence
- This includes, but is not limited to:
    - Pornography

- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Designated Safeguarding Lead.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (in line with the behaviour policy and Searching, screening, and confiscation policy)

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in the Behaviour Policy
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.
When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT facilities as a matter of course.

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Upon logging into school systems, users agree to comply with the Acceptable User agreement.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.
Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.
Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy which can be found under the Policies section of the school website and also by staff on Staff Home Sharepoint.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices. These access rights are managed by the ICT team.
Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert their line manager immediately.
Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.
School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.
Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Manager.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.
The school will:

- Work with Trustees and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **Proportionate**: the school will verify this using a third-party audit annually to objectively test that what it has in place is effective
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data regularly and store these backups securely.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT department
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification

- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our Local Authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The school's wireless internet connection is secure.

10.1 Pupils

The ICT team ensure all web material is filtered in school using Netsweeper when the device is connected to the school internet, namely if using a school device, BYOD or Y7/Y8 MDM.

Y7/Y8 MDM have filtering provided at home by a trusted third party which provides key stroke monitoring in school for school devices and Y7/Y8 MDM.

This produces instant notifications of critical violations to the DSL team who also receive weekly NetSweeper reports on website access.

Pupils can go to the ICT team for any issues gaining access.

Bring your own device (BYOD)
The school operates a student Bring Your Own device (BYOD) scheme; this is separate from the permitted use of mobile phones which the school allows for all year groups outside of lesson times only. 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 (in the appendix 2). Sanctions will be issued in accordance with our Behaviour Policy.

10.2 Parents/carers and visitors
Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.
The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)

- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The headteacher and Business Manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.
This policy will be reviewed every 2 years.

12. Related policies

This policy should be read alongside the school's policies on:

- Safeguarding and child protection
- Searching, Screening, and Confiscation Policy
- Behaviour
- Data protection
- Anti-Bullying

13. 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 digitally sign the **Anti-Bullying and Cyberbullying Contract.**

14. 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.

15. Data Protection Act 1998

Beaconsfield High School is committed to protecting the rights and privacy of all individuals in accordance with the Data Protection Act 1998. 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 the Data Protection Act 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 the Data Protection Act 1998, please see:

Data Protection Act 1998: http://www.legislation.gov.uk/ukpga/1998/29/contents

16. 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

17. 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.

18. 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.

19. 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.

20. 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.

Date last reviewed:	November 2024
Next review date:	November 2027
For review by:	HT

Appendix 1: Social Media guidelines for staff

These guidelines can be found of the Staff Home Sharepoint under Policies

Appendix 2: Bring Your Own Device User Agreement

Can be found under the School Guidance Policies on our website- at this **link**

Appendix 3: Acceptable use agreement for staff, Trustees, volunteers and visitors

Beaconsfield High School

Acceptable Use Policy

for the ICT Systems and the Internet

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.

Appendix 4: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

TERM	DEFINITION
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

]

Appendix 5: 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.

Appendix 6: Anti-Bullying and Cyberbullying Contract

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 daughter to understand the importance of not becoming involved in bullying or cyberbullying
help my daughter understand how damaging bullying and/or cyberbullying can be for the victim
monitor my daughter'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 daughter 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: