BHES

ICT and Internet Acceptable Use policy

Note: in this policy reference to governing body or governors refers to the management committee and its members.

Where contextually appropriate for BHES read service.

Date adopted: Click here to enter a date.

HISTORY OF POLICY CHANGES

Date	Page	Details of Change
April 2022	All	New policy written inline with The Key and Forbes Solicitors using model policy.

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way BHES works, and is a critical resource for students, staff (including senior leadership teams), governors, volunteers and visitors and the management committee. It supports teaching and learning, pastoral and administrative functions of BHES.

However, the ICT resources and facilities BHES uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

> Set guidelines and rules on the use of BHES ICT resources for staff, students, parents and governors

> Establish clear expectations for the way all members of BHES community engage with each other online

> Support BHES' policy on data protection, online safety and safeguarding

> Prevent disruption to BHES through the misuse, or attempted misuse, of ICT systems

> Support BHES in teaching students safe and effective internet and ICT use

This policy covers all users of BHES' ICT facilities, including governors, staff, students, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under BHES' or Bristol City Council's disciplinary policy/behaviour policy/staff discipline policy/staff code of conduct.

2. Relevant legislation and guidance

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

> Data Protection Act 2018

> The General Data Protection Regulation

> 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

> The Education and Inspections Act 2006

> Keeping Children Safe in Education 2021

> Searching, screening and confiscation: advice for BHESs

> National Cyber Security Centre (NCSC)

> Education and Training (Welfare of Children Act) 2021

3. Definitions

> **"ICT facilities":** includes 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 which may become available in the future which is provided as part of the ICT service

> **"Users":** anyone authorised by BHES to use the ICT facilities, including governors, staff, students, volunteers, contractors and visitors

> **"Personal use":** any use or activity not directly related to the users' employment, study or purpose

> **"Authorised personnel":** employees authorised by BHES to perform systems administration and/or monitoring of the ICT facilities

> **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 5 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of BHES' ICT facilities by any member of BHES community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of BHES' ICT facilities includes:

> Using BHES' ICT facilities to breach intellectual property rights or copyright

> Using BHES' ICT facilities to bully or harass someone else, or to promote unlawful discrimination

> Breaching BHES' 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 (also known as sexting or youth-produced sexual imagery)

> Activity which defames or disparages BHES, or risks bringing BHES into disrepute

> Sharing confidential information about BHES, its students, or other members of BHES community

> Connecting any device to BHES' ICT network without approval from authorised personnel

> Setting up any software, applications or web services on BHES' network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the 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 BHES' ICT facilities

> Causing intentional damage to ICT facilities

> Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel

> Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

> Using inappropriate or offensive language

> Promoting a private business, unless that business is directly related to BHES

> Using websites or mechanisms to bypass BHES' filtering mechanisms

> Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. BHES reserves the right to amend this list at any time. The headteacher or designated safeguarding lead will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of BHES' ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of BHES ICT facilities (on BHES 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.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with BHES' and Bristol City Councils policies on behaviour/discipline/staff discipline/staff code of conduct.

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

5.1 Access to BHES ICT facilities and materials

The IT department at Bristol City Council manages access to BHES' ICT facilities and materials for BHES 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 log-in/account information and passwords that they must use when accessing BHES' ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT manager at Bristol City Council.

5.1.1 Use of phones and email

BHES 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 accounts.

All work-related business should be conducted using the email address BHES has provided.

Staff must not share their personal email addresses with parents and students, 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 ICT manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or students. Staff must use phones provided by BHES to conduct all work-related business.

BHES 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 BHES ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher or IT manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

> Does not take place during teaching/contracted hours

> Does not constitute 'unacceptable use', as defined in section 4

> Takes place when no students are present

> Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes

Staff may not use BHES' ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of BHES' ICT facilities for personal use may put personal communications within the scope of BHES' ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using BHES ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where students and parents could see them.

Staff should take care to follow BHES' guidelines on 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 ensure their use of social media, either for work or personal purposes, is appropriate at all times.

BHES has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access BHES' ICT facilities and materials remotely.

Staff can access BHES documents and information via:

> Teams

> Google drive

> Outlook 365

> CPOMS

> Global protect

Staff accessing BHES' 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 BHES' ICT facilities outside BHES and take such precautions as the ICT manager and headteacher may require from time to time 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.

5.4 BHES social media accounts

BHES has official Facebook/Twitter/Instagram pages, managed by the designated safeguarding lead. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

Posts on the social media pages will only be of relevance to BHES community. No posts will present political bias or bring the service into disrepute. Student faces/names will only be used with parental permission.

5.5 Monitoring of BHES network and use of ICT facilities

BHES reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

> Internet sites visited

> Bandwidth usage

> Email accounts

> Telephone calls

> User activity/access logs

> Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

BHES monitors ICT use in order to:

> Obtain information related to BHES business

> Investigate compliance with BHES policies, procedures and standards

> Ensure effective BHES 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

6. Students

6.1 Access to ICT facilities

> Computers and equipment in BHES' ICT suite are available to students only under the supervision of staff

> Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff

> Students will be provided with an account linked to BHES' virtual learning environment, which they can access from any device via Google classrooms

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, BHES has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under BHES rules or legislation.

BHES can delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break BHES' rules.

Staff members may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse contains an online element.

6.3 Unacceptable use of ICT and the internet outside of BHES

BHES will sanction students, in line with the behaviour policy, if a student engages in any of the following **at any time** (even if they are not on BHES 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 BHES' policies or procedures

> Any illegal conduct, or 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 and 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 BHES, or risks bringing BHES into disrepute

> Sharing confidential information about BHES, other students, or other members of BHES 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 BHES' ICT facilities

> Causing intentional damage to ICT facilities or materials

> Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

> Using inappropriate or offensive language

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to BHES' ICT facilities as a matter of course.

However, parents working for, or with BHES 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 BHES' facilities at the headteacher's discretion.

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

7.2 Communicating with or about BHES online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with BHES through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

8. Data security

BHES is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, BHES cannot guarantee security. Staff, students, parents and others who use BHES' ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of BHES' 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 students who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

BHES allocates passwords to student gmail accounts and computer logins.

8.2 Software updates, firewalls and anti-virus software

All of BHES' ICT devices that support software updates, security updates and anti-virus products will 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 BHES' ICT facilities.

Any personal devices using BHES' 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 BHES' data protection policy.

8.4 Access to facilities and materials

All users of BHES' ICT facilities will have clearly defined access rights to BHES systems, files and devices.

These access rights are managed by Bristol City Council IT manager.

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 the headteacher and BCC IT 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 closed down completely at the end of each working day.

8.5 Encryption

BHES ensures that its devices and systems have an appropriate level of encryption.

BHES staff may only use personal devices (including computers and USB drives) to access BHES data, work remotely, or take personal data (such as student information) out of BHES 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.

9. Protection from cyber attacks

Please see the glossary (appendix 5) to help you understand cyber security terminology.

BCC IT team will:

> Work with governors and BHES to make sure cyber security is given the time and resources it needs to make BHES secure

> Provide annual training for staff (and include this training in any induction for new starters, if they join outside of BHES' annual training window) on the basics of cyber security, including how to:

- o Check the sender address in an email
- o Respond to a request for bank details, personal information or login details
- o 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:

- o **'Proportionate'**: BHES will verify this using a third-party audit (annually), to objectively test that what it has in place is up to scratch
- o **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
- o **Up-to-date:** with a system in place to monitor when BHES needs to update its software
- o **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be

> Back up critical data and store these backups – this is done by BCC.

> Delegate specific responsibility for maintaining the security of our management information system (MIS) to BCC It manager.

> Make sure staff:

- o Dial into our network using a virtual private network (VPN) when working from home
- o Enable multi-factor authentication where they can, on things like BHES email accounts
- o Store passwords securely

> Make sure ICT staff conduct regular access reviews to make sure each user in BHES 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 seeing if they have the [Cyber Essentials](#) certification

> Develop, review and test an incident response plan with the IT department, for example, including how BHES will communicate with everyone if communications go down, who will be contacted when, and who will notify [Action Fraud](#) of the incident. This will be reviewed and tested and after a significant event has occurred, using the NCSC's '[Exercise in a Box](#)'

> Work with BHES to see what it can offer regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

BHES wireless internet connection is secured by BCC IT team.

10.1 Students

Wi-fi is only available to students via BHES designated equipment.

10.2 Parents and visitors

Parents and visitors to BHES will not be permitted to use BHES' Wi-Fi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

> Parents are working with BHES in an official capacity (e.g. as a volunteer or as a member of the PTA)

> Visitors need to access BHES' Wi-Fi 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 Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The headteacher and BCC IT manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of BHES.

This policy will be reviewed annually.

The governing board is responsible for approving this policy.

12. Related policies

This policy should be read alongside BHES' policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote learning

Appendix 1: Social media platforms cheat sheet for staff

Don't accept friend requests from students or parents on social media

10 rules for BHES staff on social media

1. Consider changing your display name – use your first and middle name, use a maiden name, or put your surname backwards instead

2. Consider changing your profile picture to something unidentifiable, or if not, ensure that the image is professional

3. Check your privacy settings regularly

4. Be careful about tagging other staff members in images or posts

5. Don't share anything publicly that you wouldn't be just as happy showing your students

6. Don't use social media sites during BHES hours

7. Don't make comments about your job, your colleagues, BHES or your students online – once it's out there, it's out there

8. Don't associate yourself with BHES on your profile (e.g. by setting it as your workplace, or by 'checking in' at a BHES event)

9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or students)

Check your privacy settings

> Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

> Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

> The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

> **Google your name** to see what information about you is visible to the public

> Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

> Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A student/parents adds you on social media

> In the first instance, ignore and delete the request. Block the student/parent from viewing your profile

> Check your privacy settings again, and consider changing your display name or profile picture

> If the student/parent asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students/parents and that if they persist, you'll have to notify senior leadership and/or their parents. If the student/parent persists, take a screenshot of their request and any accompanying messages

> Notify the senior leadership team or the headteacher about what's happening

You're being harassed on social media, or somebody is spreading something offensive about you

> **Do not** retaliate or respond in any way

> Save evidence of any abuse by taking screenshots and recording the time and date it occurred

> Report the material to Facebook or the relevant social network and ask them to remove it

> If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

> If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

> If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers
Name of parent/carer: **Name of child:**
Online channels are an important way for parents/carers to communicate with, or about, BHES. BHES uses the following channels: • Our official Facebook, Twitter and Instagram pages • Email/text groups for parents (for BHES announcements and information) • Our virtual learning platform
When communicating with BHES via official communication channels, or using private/independent channels to talk about BHES, I will: • Be respectful towards members of staff, and BHES, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through BHES' official channels, so they can be dealt with in line with BHES' complaints procedure I will not: • Use private groups, BHES' social media pages, or personal social media to complain about or criticise members of staff. This is not constructive and BHES can't improve or address issues if they aren't raised in an appropriate way • Use private groups, BHES' social media pages, or personal social media to complain about, or try to resolve, a behaviour issue involving other students. I will contact BHES and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed: https://forms.gle/A83pnvKpvRWeuZ6F7 https://forms.gle/sfbZaRJjkeY6tpUY6	Date:

Appendix 3: Acceptable use agreement for students

Acceptable use of BHES' ICT facilities and internet: agreement for students and parents/carers

Name of student:

When using BHES' ICT facilities and accessing the internet in BHES, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break BHES rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo
- Share my password with others or log in to BHES' network using someone else's details
- Bully other people

I understand that BHES will monitor the websites I visit and my use of BHES' ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use BHES' ICT systems and internet responsibly.

I understand that BHES can discipline me if I do certain unacceptable things online, even if I'm not in BHES when I do them.

Signed (student):	Date:

Parent/carer agreement: I agree that my child can use BHES' ICT systems and internet when appropriately supervised by a member of BHES staff. I agree to the conditions set out above for students using BHES' ICT systems and internet, and for using personal electronic devices in BHES, and will make sure my child understands these.

Signed (parent/carer): https://forms.gle/2mRHit7NqzCSAA749	Date:

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of BHES' ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using BHES' ICT facilities and accessing the internet in BHES, or outside BHES on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm BHES' reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to BHES' network
- Share my password with others or log in to BHES' network using someone else's details
- Share confidential information about BHES, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to BHES

I understand that BHES will monitor the websites I visit and my use of BHES' ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside BHES, and keep all data securely stored in accordance with this policy and BHES' data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use BHES' ICT systems and internet responsibly, and ensure that students in my care do so too.

Signed (staff member/governor/volunteer/visitor):	Date:
https://forms.gle/pGofsSUbx4vJmSKV7	

Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures BHES 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.
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.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or

TERM	DEFINITION
	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	Programs 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 executives.