Benjamin Britten School

Acceptable Use Policy

Policy led by: ITh and ACo Reviewed: September 2023 Next review: September 2025

Introduction

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff, governors and visitors.

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 governors
- 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 governors, staff, pupils, volunteers, contractors and visitors.

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

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 governors, staff, pupils, 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 the school to perform systems administration and/or monitoring of the ICT facilities. In relation to the school's web filtering system, Smoothwall, notifications are received by ICT Support, Year Teams, senior leadership and Headteachers.

Materials: files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages and social networking sites

See appendix 6 for a glossary of cyber security terminology.

Unacceptable use

The following is considered unacceptable use of the school's ICT facilities:

- 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 or facilitating a breach of the school's other policies or procedures, including it's Data Protection policy
- 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
- Unauthorised sharing of 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, misogynistic, 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 own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteachers 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.

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 Headteachers' discretion.

Sanctions

Members of the school community who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour and conduct, listed at the end of this policy.

Staff (including governors, volunteers, and contractors)

Access to school ICT facilities and materials

The school's ICT Support team 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

Access permissions for the school's information management system, Bromcom, is managed by the Admissions and MIS Coordinator in conjunction with the Headteachers' PA.

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities. Staff must ensure that this information is not shared with any other member of the school community.

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 ICT Support Team or Admissions and MIS Coordinator.

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 Protection Lead immediately and follow the school's 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.

Staff must not take photographs or videos of pupils on personal phones. Staff leading school trips will be given a mobile phone in their trip pack which must be returned to the trip co-ordinator, who will download the photographs and videos and clear the phone. Staff must be guided by the photo consent information available on Bromcom and in the trip pack when taking photographs or videos of pupils. Pupils without photograph or video consent must not have their image taken or recorded in accordance with data protection legislation.

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:

Staff should refrain from using 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. 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 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 to protect themselves online and avoid compromising their professional integrity.

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, even where security settings have been set to 'private'.

The school has guidelines for staff on appropriate security settings for social media accounts (see appendix 1).

Remote access

We allow staff to access the school's ICT facilities and materials remotely. 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 required against importing viruses or compromising system security.

Online learning and safeguarding protocols for virtual/'live' teaching. Guidance for staff and raising awareness for parents/carers. These protocols focus on:

- Pre-recorded screen, video and / or audio lessons.
- Using comments in Google Classroom.
- Running live lessons via Google Classroom.

Pre-recorded Screen Recordings, Video and/or Audio Lessons Protocols:

Voice recording – this is where you record yourself talking through an activity, model or giving feedback. Ensure you speak using formal English in the way you would in a normal classroom. Only use a student's name if you are praising individual work.

Screen recording – this is where you share with students a recording of your computer desktop. Ensure that the video does not record any personal background/information. You can do this by either changing the settings on your recording to record a 'window' or a 'tab' only OR ensuring you have a neutral background, and there is no personal information available (i.e. nothing saved to the desktop).

Video recording - this is when you record yourselves talking through an activity, explaining a model or giving feedback. It is your choice whether you choose to turn the video on or not in these videos. If you choose to turn video on, please ensure that:

- The background is neutral and professional. At all times the setting should be in a location suitable for delivery of a video lesson e.g. a living space or a study area. Videos should not be recorded in a bedroom and should not include other adults or children in the background.
- Teacher dress code is the same as it is in school – smart and professional.

Using Comments in Google Classroom

- Use academic English in your comments to students.
- Students must use academic English at all times and only comment on the work.
- Any inappropriate comments will be recorded in a screenshot and sent to the relevant Year Team, who will communicate with parents.
- Ensure any behaviour concerns are recorded in Bromcom, where appropriate they are reported to the Head of Department / Year Team.
- If students are not following the expectations you have of them, they can be muted in Google Classroom, so they can no longer make comments.
- Ensure any welfare/safeguarding concerns that arise during the communication are recorded and reported straight away on Bromcom.

Running Live Lessons via Google Classroom

- Staff must only use platforms provided by Benjamin Britten Music Academy to communicate with students once they have taken part in live lesson training i.e. no communication with students should be done using your mobile phone, WhatsApp, any other social media platform etc.
- Security settings must be enabled.
- Teacher dress code is the same as it is in school – smart and professional.
- If teacher camera is on, the background must be neutral and professional. At all times the setting should be in a location suitable for delivery of a video lesson. Any computers used should be in appropriate areas, for example, not in bedrooms and should not include other adults or children in the background.
- Staff can record live lessons provided that children cannot be seen or heard.
- Staff are advised to consider screen time for both themselves and the students.
- Language must be professional and appropriate.
- Staff need to ensure they are the organiser of the Google Classroom live lesson and close the video once the lesson is over so students cannot contact each other without supervision.
- Staff should not enter a Google Meet that has been set up by a student.

Protocol for Students

- Students must only join using their school account through Google Classroom.
- Students must only join the class once the teacher has announced it live on the google classroom stream.
- Students must mute their microphones unless asked to unmute by the teacher.
- If students have a question, they can write ‘question’ or type the question into the comment box or press the raised hand button.
- All comments made by students must be focused on the work and be relevant to the lesson being taught.
- Teachers can see the comments so students must write in an appropriate way at all times i.e. use academic English at all times.
- At no point, should students take any form of recording or photo of the session. If it is found that this has happened, it will immediately be referred to the Year Team and students will face serious sanctions in line with our behaviour policy.
- In live lessons students and any parent in view must be in appropriate clothes and have a neutral and appropriate background (e.g. they must not be in a bedroom or have any siblings or other family members in the background).
- At the end of the lesson you must, end the recording, leave the lesson and close the window.

Behaviour Systems to Support these Protocols

Any students who don’t follow our protocols will be subject to one or more of the following sanctions:

- The student(s) in question will be muted in the classroom by the teacher.
- The student(s) in question will be removed from the classroom by the teacher. The Head of Department and relevant Head of Year will be notified via the behavioural referral system and we will also contact home.

- If necessary, the lesson will be stopped and closed.
- Sanctions will follow the school's behaviour policy.

Our ICT facilities contain information which is confidential and subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy, available here: https://www.benjaminbritten.school/31/PXURK2H2YOHPFSJV2H.pdf/Data-Protection-Policy

School social media accounts

The school has an official Facebook account, managed by the PA to the Headteacher and the Head of Upper School. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

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 in which 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 through 3CX
- User activity/access logs
- Any other electronic communications

The school uses a comprehensive software package called Smoothwall, for web filtering, firewall protection, digital monitoring and digital record keeping. Smoothwall notifies ICT Support, Heads of Year, senior leadership and Headteachers when unacceptable use of ICT facilities has taken place.

The school monitors ICT use in order to:

- Safeguard members of its school community
- Ensure 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) and online safety lead 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.

Pupils

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 safeguarding risk to staff or pupils, **and/or**
- Is identified in school policy as a banned item for which a search can be carried out, **and/or**
- Is evidence in relation to an offence

Please see page 10 of the school's Behaviour Policy for further information on searching and confiscation.

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

Parents/carers

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) 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.

Communicating with or about the school online

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

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

Pupil learning platforms

The school uses a variety of online learning platforms, such as Google Classroom, MathsWatch, Bedrock Learning and Unifrog. These platforms facilitate access to the school curriculum. Students may be required to access these platforms outside of school, for homework for example. Should parents/ carers have any questions or concerns about these platforms, they should contact their child's Head of Year, who will forward it on to the appropriate staff member.

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 and students. 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.

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

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. Supply/ agency staff, parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

All staff will use the password manager required by the ICT Support team to help them store their passwords securely. If pupils forget their log-in details, they should see a member of the ICT Support team.

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 and the responsibility of this falls to the owner of the device.

Data protection

All personal data must be processed and stored in line with data protection regulations and the school's Data Protection Policy and Data Protection Privacy Notice, both of which are available on the school's website.

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 Support team or Admissions and MIS Coordinator.

Users should not access, nor 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 ICT Support Team immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access.

Teachers must ensure Prowise boards do not display personal information of any other individuals. For example, class registers must not be displayed on the Prowise board.

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 Support team.

Protection from cyber attacks

Please see the glossary to help you understand cyber security terminology.

The school will:

- Work with governors 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.

- 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
  - Multi-layered
  - Up to date
  - Regularly reviewed and tested
- Back up critical data and store this as per the school's incident response plan.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Bromcom.
- 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
- Review and test the 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 Trust to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

Internet access

The school's wireless internet connection is secure. Pupils are not permitted to connect their own devices to the school's internet.

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)
- 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.

Monitoring and review

The Online Safety Lead and Headteachers 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.

Related policies

This policy should be read in conjunction with the following policies, available on the school website and in the staff shared drive:

- Child Protection and Safeguarding Policy
- Anti-bullying Policy
- Behaviour Policy
- Staff Discipline, Conduct and Grievance Policy
- Whistleblowing Policy
- Data Protection Policy
- Data Protection Privacy Notice

School staff and social media- Key areas

1. Do not accept friend requests from pupils
2. Change your display name
3. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
4. Check your privacy settings regularly and ensure these are set to private
5. Be careful about tagging other staff members or the school in images or posts
6. Don't share anything publicly that you wouldn't be happy showing your pupils
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school 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 WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings on Facebook/ other social networking sites

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils 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 pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and notify the DSL. If the pupil persists, take a screenshot of their request and any accompanying messages and pass these on to the DSL.

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 the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and 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

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

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.
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.

TERM	DEFINITION
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.