



KETTLETHORPE HIGH SCHOOL

<https://kettlethorpehigh.co.uk>

ICT Acceptable Use Policy

Policy Version: 2026-27
Approved By Governors:
Next Review: September 2028



Contents

- 1. Introduction & Aims..... 2
- 2. Relevant legislation and guidance..... 2
- 3. Definitions 3
- 4. Unacceptable Use..... 3
 - 4.1 Exceptions from unacceptable use 5
 - 4.2 Sanctions 5
- 5. Staff (Including governors volunteers and contractors) 5
 - 5.1 Access to school ICT facilities and materials..... 5
 - 5.1.1 Use of phones and email 5
 - 5.2 Personal use 6
 - 5.2.1 Personal social media accounts..... 7
 - 5.3 Remote Access 7
 - 5.4 School social media accounts..... 7
 - 5.5 Monitoring and filtering of the school network and use of ICT facilities 7
- Data Security..... 8
 - 6.1 Passwords 8
 - 6.2 Software updates, firewalls and anti-virus software 8
 - 6.3 Data protection..... 9
 - 6.4 Access to facilities and materials..... 9
 - 6.5 Encryption 9
 - 6.6 Personal Devices 9
 - 6.7 Storage Restrictions 9
- Protection from cyber attacks 9
- Internet access 10
 - Pupils..... 11
 - Staff / Governors / Visitors..... 11
 - Filtering..... 11
- Monitoring and review 11
- Using Artificial Intelligence 11
- Social media..... 11

10 rules for staff to follow.....	12
Check your privacy settings.....	12
What to do if	12
Appendix 1: Glossary of cyber security terminology	14

1. Introduction & Aims

Information and communications technology (ICT) is an integral part of the way Kettlethorpe High School works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors.

However, the ICT resources and facilities Kettlethorpe 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 staff, governors, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our 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 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 2026](#)
- [Generative artificial intelligence \(AI\) in education](#)
- [Filtering and monitoring: core standard](#)
- [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](#)
- [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 governors, 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 1 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 Artificial Intelligence (AI) tools and generative services (including but not limited to Microsoft Copilot, ChatGPT, Gemini and similar technologies):

- Must only be used in accordance with the school's [Artificial Intelligence Policy](#).
- Must not be used to process confidential, safeguarding-sensitive, examination-sensitive or personal data unless explicitly authorised and covered by a Data Protection Impact Assessment (DPIA).
- Must not be used to circumvent learning, assessment or examination requirements.
- AI-generated work submitted by pupils must comply with published assessment guidance and teacher instructions.
- Staff remain responsible for all content generated through AI tools and must verify accuracy before use.
- Users must not rely on AI-generated content without appropriate checking for factual accuracy, bias, safeguarding implications or copyright concerns.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher and Senior Leadership Team (SLT) 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. See approval process below:

1. Staff member to discuss with a member of the Senior Leadership Team (SLT).
2. Member of SLT to discuss with the IT Manager of the school who will ensure that this request is in accordance with IT safety, GDPR regulations and that this request is reasonable.
3. Once confirmation from the IT Manager has been provided, SLT member to seek approval from the headteacher.
4. Headteacher to provide formal approval for this exemption and an agreed timeframe set.

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 behaviour, staff discipline and the staff code of conduct.

Code of Conduct

Culture and Behaviour Policy

5. Staff (Including governors volunteers and contractors)

5.1 Access to school ICT facilities and materials

The school's IT 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 Manager.

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 must enable multi-factor authentication on all school accounts where available.

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 IT 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 IT Manager 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 and teaching hours
- 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 personal device 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 the use of social media section of this policy) 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 always appropriate.

The school has guidelines for staff on appropriate security settings for social media accounts (see 'Social Media').

5.3 Remote Access

Whilst Kettlethorpe High School does not permit remote access to internal facilities, the school uses Microsoft 365 which, by definition, is 'remote' as this is a cloud-based service. This enables staff to access applications, for example Outlook and OneDrive

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 IT Manager 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.

<https://kettlethorpehigh.co.uk/wp-content/uploads/2024/05/GDPR-Policy.pdf>

5.4 School social media accounts

The school has an official Facebook and X (Twitter) account, managed by the Marketing and Events Officer. 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 IT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. This is carried out using various systems such as Firewalls and internet filtering packages for both internal and external 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 IT Manager, as appropriate.

The school's filtering and monitoring arrangements will be reviewed regularly to ensure compliance with current DfE Filtering and Monitoring Standards.

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 cybercrime technologies. Staff, pupils, parents/carers and others who use the school's ICT facilities should always use safe computing practices. 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

6.1 Passwords

All users of the school's ICT facilities must 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.

Password managers are only used by the IT support department. The IT support department is available to support staff members and pupils when required by logging a support ticket.

The IT Support department is not contactable by radio, except in extremely urgent circumstances (eg. Internet connection is down in an entire section of the school).

6.2 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.

6.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

<https://kettlethorpehigh.co.uk/wp-content/uploads/2024/05/GDPR-Policy.pdf>

6.4 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 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 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 shut down completely at the end of each working day.

6.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff are not permitted to use external hard drives or USB drives. School staff can access systems via Microsoft 365 services and files using Microsoft OneDrive.

If there is a requirement for the use of either an external hard drive or USB drive, this must be granted through the approval process as outlined in section 4.1. If permission is granted, the IT Manager will provide a school's USB drive which will have the appropriate levels of security and encryption.

6.6 Personal Devices

Any personal device authorised to access school systems must:

- Be protected by a password, PIN or biometric authentication.
- Have its local storage encrypted where possible.
- Have up-to-date operating system and security updates installed.
- Use supported anti-malware and anti-virus protection where applicable.
- Be reported immediately if lost, stolen or compromised.

Access to the Schools' network on personal devices is at the discretion of the IT Manager and can be revoked at any time.

6.7 Storage Restrictions

School information must only be stored within approved school systems, including Microsoft 365 services.

Users must not store school data within unauthorized cloud services. AI platforms or personal storage accounts.

Protection from cyber attacks

Users must immediately report suspected phishing emails, malicious software, unauthorised access attempts, accidental disclosure of information, lost devices, data breaches or any other cyber security incident to the IT Support Team and Data Protection Officer.

Please see the glossary (appendix 1) to help you understand cyber security terminology.
The school will:

- Work with governors and the IT Support 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:
 - 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: Kettlethorpe High School follows the 3-2-1 backup policy which requires regular back up of all stored information. Backups are undertaken daily throughout the week with full backups taking place on weekends. This ensures all data is securely backed up with failsafes in place if required.
- Make sure staff:
 - Enable multi-factor authentication where they can, on things like school email accounts
 - 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 Support 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 following any significant cyber security incident. Tabletop exercises may also be undertaken throughout the year using NCSC Exercise in a Box resources.
- Work with our LA 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 and wired internet connection is secure and monitored daily (including weekends) using filtering software. All computers within school are connected via a wired connection. Wireless access is available for staff and school issued devices only.

Pupils

Pupils at Kettlethorpe High School do not have access to the school's WIFI. Pupils are only able to connect to the WIFI via school issued devices. Personal devices are not permitted to join the wireless connection.

Staff / Governors / Visitors

Staff are encouraged to use wired connection devices only within school. However, if connection to the school's WIFI is required, a ticket to the IT Support Team must be raised to enable the team to make an informed decision. The final decision to approve connection to the school's WIFI falls to the IT Manager of Kettlethorpe High School.

Note: When devices (both work related and personal) are connected to the school's wireless internet connection, apps and websites are monitored through the school's filtering system. Inappropriate sites are automatically logged and if required, relevant action taken.

Filtering

The school uses a filtering system, Smoothwall, to monitor internet usage both internal and external of school. This filtering system applies to both staff and pupils and a record of all sites visited is kept.

Staff can report inappropriate sites to the IT helpdesk using the ticket system.

Monitoring and review

The headteacher, Business Manager and IT 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 two years, unless significant changes are required as a result of guidance or regulation changes.

The governing board is responsible for reviewing and approving this policy

Using Artificial Intelligence

Kettlethorpe High School understands the valuable potential of artificial intelligence (AI). For example, it can be used to enhance lesson planning, customise learning experiences and progress educational innovation. However, there are significant risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations

Please find below the link to 'Using Artificial Intelligence' policy.

[Kettlethorpe High School - Use of Artificial Intelligence](#)

Social media

Social media and online communication platforms (including but not limited to Facebook, X, Instagram, TikTok, Snapchat, WhatsApp, Threads, LinkedIn and any future platforms) must be used appropriately with the correct privacy settings in place to ensure personal accounts are protected.

The number one rule: DO NOT ACCEPT FRIEND REQUESTS FROM PUPILS ON SOCIAL MEDIA.

10 rules for staff to follow

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure 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 happy showing your pupils
6. Don't use social media sites during school hours
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 Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

Check your privacy settings

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 and 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. 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 that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

It is at your discretion whether to respond. Bear in mind that:

- Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school

- Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

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 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/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 1: Glossary of cyber security terminology

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.

TERM	DEFINITION
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.
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.

TERM	DEFINITION
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.