

ASHTON GATE PRIMARY SCHOOL



ICT AND INTERNET USE POLICY

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. However, the ICT resources and facilities our school uses 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 and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption 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.

Breaches of this policy may be dealt with under our behaviour policy/staff discipline policy.

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 2025
- Searching, screening and confiscation: advice for schools
- 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 the school to use the 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
- **“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 2 for a glossary of cyber security terminology.

4. Principles of Screen Use in School

- **Educational Purpose:**
Screens are used only when they add value to teaching and learning—for example, accessing online resources, practising digital literacy, or supporting inclusion (e.g. for SEND pupils).
- **Balanced Learning:**
Lessons should include a balance of screen-based and non-screen activities. Staff are encouraged to design lessons that include discussion, hands-on learning, reading, writing, and outdoor experiences alongside digital tools.
- **Health and Wellbeing:**
 - Pupils will not use screens continuously for long periods (no more than 20 minutes for EYFS and KS1 or 30 minutes for KS2 without a break).
 - Teachers will ensure regular screen breaks and promote good posture, movement, and eye health.
 - Screens will not be used as a behaviour management tool (e.g. as a reward or to occupy children for extended periods).
- **Online Safety and Digital Citizenship:**
 - All online activity will be monitored in line with our **Online Safety and Safeguarding Policies**.
 - Pupils will be taught how to use screens safely, respectfully, and responsibly.
 - Staff will model appropriate screen use at all times.
- **Use in EYFS and KS1:**
 - Screen use will be occasional, short, and purposeful (e.g. to support phonics, counting, or guided story time).
 - Devices will not replace play-based, sensory, and social learning experiences.
- **Use in KS2:**
 - Screens will be used to support research, presentation, coding, and creative projects.
 - Pupils will begin to develop independent, safe, and critical use of technology.

Using screens for educational content can enhance learning through dynamic and interactive displays, but it should be balanced with traditional methods.

Benefits of using screens

Engaging content:

Screens can present dynamic content like videos, animations, and interactive quizzes that capture young children's attention and make learning more fun.

Interactive learning:

Touch screens allow children to actively participate in lessons, promoting collaboration and critical thinking.

Catering to different learning styles:

Multimedia can appeal to various learning styles, creating a more inclusive and visually stimulating environment.

Enhancing communication:

Digital screens can be used to display important announcements, events, and messages to children, staff, and parents.

Developing digital skills:

Early exposure to technology can help young children develop essential digital literacy skills for the future.

Potential drawbacks

Over-information:

Excessive screen time can lead to a sense of addiction or obsessiveness, especially if not managed properly.

Displacing other activities:

Screen use might displace essential activities like hands-on play, physical activity, and face-to-face social interaction, which are crucial for early development.

Shallow learning:

There is a risk that children might be passively consuming information rather than engaging in deeper learning or creative thinking.

Potential harm:

Some research suggests that the harms of screen time and social media use may significantly outweigh the benefits for very young children.

Best practices for implementation

Prioritize interactive and age-appropriate content:

Choose high-quality educational content that is designed for young learners and encourages active participation rather than passive consumption.

Ensure adult mediation:

View media with children and help them process the information by asking questions and making connections to their own lives.

Limit screen time:

Keep screen use to a minimum and integrate it with a variety of other learning activities, such as reading, art, and outdoor play.

Use screens as a tool, not a replacement:

Screens should be used as a supplementary tool to enhance learning, not as a replacement for traditional teaching methods and human interaction.

Focus on real-time communication:

Use screens in reception areas to provide updates, share student achievements, and welcome visitors, ensuring that parents and staff are kept informed.

5. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. 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 (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, 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 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 the school's 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 the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way
- AI tools must not be used independently unless under the direct and supervision of a member of staff.

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

5.1 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 Executive Headteacher's discretion.

5.2 Sanctions

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

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

6.1 Access to school ICT facilities and materials

The school's ICT support provider, 2IT, 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 log-in/account information and passwords that they must use when accessing the school's 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 School Business Manager.

6.1.1 Use of phones and email

- The school provides each member of staff with an email address.
- This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.
- 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 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 School Business Manager immediately and follow our data breach procedure.
- Staff must not give their personal phone numbers to parents 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.
- Staff must keep personal mobile phones on silent or switched off when with pupils. If there is a specific reason why staff need to take a phone call whilst they are with children, they must discuss this with their Head of School or School Business Manager in advance. Under no circumstances should staff take pictures of pupils on their mobile phones.
- Staff who would like to record a phone conversation should speak to the Executive Headteacher and the Data Protection Officer. All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.
- We may grant requests to record conversations when:
 - Discussing a complaint raised by a parent/carer or member of the public
 - Calling parents to discuss behaviour or sanctions
 - Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.

6.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Executive Headteacher 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 working time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present

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

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

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

Staff 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 could see them.

Staff should take care to follow the school's 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.

6.2.1 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.

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

6.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely using Log Me In. Access can be requested from the School Business Manager.

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 take such precautions as the school 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.

6.4 Monitoring of school network and use of ICT facilities

The school 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.

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

7. Pupils

7.1 Access to ICT facilities

- Computers and IT equipment in the school are available to pupils only under the supervision of staff.

7.2 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 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 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 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

8. Parents

8.1 Access to ICT facilities and materials

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

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

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

8.2 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 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.

We ask parents to sign Acceptable Use Agreements.

9. Data security

The school 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, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

9.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

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

9.2 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 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.

9.3 Data protection

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

9.4 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 2IT.

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 School Business 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.

9.5 Encryption

The school ensures 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 2IT.

10. Protection from cyber attacks

Please see the glossary (appendix 2) 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, including how to:
 - Check the sender address in an email
 - Respond to a request for bank details, personal information or login details
 - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
 - **'Proportionate'**: the school will verify this using a third-party audit to objectively test that what it has in place is up to scratch
 - **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 up to scratch and secure as they can be
 - Back up critical data daily and store these backups on a cloud based backup systems.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Cathedral Schools Trust.
- 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 seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department, for example, including how the school 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 every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with Cathedral Schools 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.

11. Internet access

The school wireless internet connection is secured.

- The school uses web filtering. Inappropriate sites are reported to Trading with Schools IT Helpdesk who are also able to unblock sites that are filtered in error.
- The school has a separate connection for staff and pupils. A visitor connection is available for parents and the public.

11.1 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the Executive Headteacher.

The Executive Headteacher will only grant authorisation if:

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

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

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

12. Monitoring and review

The Executive Headteacher and the School Business Manager will 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 3 years.

The Full Governing Body is responsible for approving this policy.

13. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Preventing Radicalisation

Date – October 2025

Review Date – October 2028

Appendix 1:

ICT and Internet Use Agreement - EYFS and KS1

Digital technologies have become integral to the lives of children, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. Children have an entitlement to safe internet access at all times, and the school will do everything it can to ensure that reasonable precautions and systems are in place.

You have been sent an 'Acceptable Use Agreement' that has been discussed with your son/daughter. We aim to provide good access to digital technologies to enhance your child's learning and in return your child will have the knowledge and support to know how to use the internet and digital technologies safely and responsibly.

Your child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school. Please support your child's online safety education by talking to them about the pupil acceptable use agreement and completing the form below.

* Indicates required question

1. As the Parent/Carer, I give permission for my child to have access to the internet * and to use computers and ipads at school.

I understand that the school has discussed the Acceptable Use Agreement with my child and that they will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe from inappropriate or damaging content, including that from extremist groups, when they use the internet and computing systems in schools.

I will encourage my child to adopt safe use of internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Mark only one oval.

Yes

2. Pupil Name *

3. Pupil's Class *

4. Parent Name *

Appendix 2:

ICT and Internet Use Agreement - KS2

Digital technologies have become integral to the lives of children, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. Children have an entitlement to safe internet access at all times, and the school will do everything it can to ensure that reasonable precautions and systems are in place.

You have been sent an 'Acceptable Use Agreement' that has been discussed with your child and they have agreed to be a responsible user by signing it.

Your child will receive online safety education to help them understand the importance of safety when using the internet – both in and out of school. Please support your child's online education by talking to them about the pupil acceptable use agreement and completing the form below.

* Indicates required question

1. Parent/Carer *

As the Parent/Carer, I give permission for my child to have access to the internet and to computing systems at school.

I understand that my son/daughter will receive online education to help them understand the importance of safe use of technology and the internet– both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe from inappropriate or damaging content, including that from extremist groups, when they use the internet and computing systems in schools.

I will encourage my child to adopt safe use of internet and digital technologies at home and will inform the school if I have concerns over my child's online safety. I have discussed this information with my child and have completed this form with them.

Mark only one oval.

Yes

2. Pupil

This is how we stay safe when we use computers:

I will ask permission before entering any Web site, unless my teacher has already approved that site.

I will not look at or delete other people's files.

I will not bring memory storage devices into school without permission.

I will only e-mail people my teacher has approved using the group email address. The messages I send will be polite and sensible.

When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.

I will ask for permission before opening an e-mail or an attachment.

I will only do activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment.

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that the school may check my computer files and many monitor the Internet sites I visit.

I know that if I break the rules I might not be allowed to use a computer.

Mark only one oval.

Yes

3. Pupil Name *

4. Pupil's Class *

5. Parent Name *

Appendix 3: Glossary of cyber security terminology

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

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
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 encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.

TERM	DEFINITION
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.