ICT and Internet Acceptable Use Policy

Approved by:	Charmaine Baines	**Date:**	May 2024
Last reviewed on:	May 2024		
Next review due by:	May 2026		

Contents

Contents 2
1. Introduction and aims 3
2. Relevant legislation and guidance 3
3. Definitions 4
4. Unacceptable use 4
5. Staff (including volunteers, and contractors) 5
6. Pupils 8
7. Parents/carers 10
8. Data security 10
9. Protection from cyber attacks 11
10. Internet access 12
12. Related policies 13

1. Introduction and aims

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

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

This policy aims to:

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

This policy covers all users of our Provision's ICT facilities, including staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our IWYS - Staff Disciplinary Policy

2. Relevant legislation and guidance

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

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

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the Provision's ICT service
- **Users:** anyone authorised by the Provision to use the Provision'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 Provision to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the Provision's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

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

Unacceptable use of the Provision's ICT facilities includes:

- Using the Provision's ICT facilities to breach intellectual property rights or copyright
- Using the Provision's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Provision'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 Provision into disrepute
- Sharing confidential information about the school, its pupils, or other members of the Provision community
- Connecting any device to the Provision's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Provision'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 Provision'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 Provision's ICT facilities
- Causing intentional damage to the Provision's ICT facilities
- Removing, deleting or disposing of the Provision'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 Provision's filtering or monitoring mechanisms

- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- The use of artificial intelligence (AI) tools here, for example generative chatbots (such as ChatGPT and Google Bard) is unacceptable and will class as cheating. Student's marks will be disqualified: Students will have to re-do the work again in the presence of staff.
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The Provision reserves the right to amend this list at any time. The proprietor or any other relevant member of staff] will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Provision's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of Provision ICT facilities (on the Provision 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 Proprietor's discretion, for example, research or topic related to AI and artificial intelligence. The Proprietor and staff will research into good practise of other educational establishments approach to the acceptable use of artificial intelligence (AI) tools here, for example:]

- How Pupils may use AI tools and generative chatbots:
- How students use AI to research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the Provision's policies on IWYS-Staff-Disciplinary-Policy.pdf

- Revoking permission to use the Provision's systems
- Have specific filtering put on any devices they use.
- Put on their record for at least 6 months

  Please see our IWYS – Staff Disciplinary Policy IWYS – Mobile Phone Policy IWYS – Behaviour Policy IWYS – Allegations Against Staff and Low Level Concerns

  Staff Code of Conduct is located in the staff Induction Folder.

5. Staff (including volunteers, and contractors)

5.1 Access to Provision ICT facilities and materials

The Provision's filtering system managed by ICTn Ltd, manages access to the Provision's ICT facilities and materials for Provision 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 Provision'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 Proprietor, Business Manager or Compliance Officer.

5.1.1 Use of phones and email

The Provision 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 Provision 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 Proprietor 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 Provision to conduct all work-related business.

Provision 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.

IWYS Alternative Provision currently does not record incoming and outgoing phone conversations.

5.2 Personal use

Staff are permitted to occasionally use Provision ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Proprietor may request that ICTn Ltd 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/teaching hours/non-break 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 Provision'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 Provision's ICT facilities for personal use may put personal communications within the scope of the Provision'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 Provision's IWYS – Mobile Phone Policy

Staff should be aware that personal use of ICT (even when not using Provision 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 Provision's guidelines on use of social media (see appendix 1 on our website IWYS-Social-Media-Policy-.pdf and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

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

5.4 Provision social media accounts

The Provision has an official Facebook, X and SoundCloud account, managed by the Proprietor. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The Provision 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 Provision network and use of ICT facilities

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

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

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

The Provision monitors ICT use in order to:

- Obtain information related to Provision business
- Investigate compliance with Provision policies, procedures and standards
- Ensure effective Provision 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

The Proprietor and Compliance Officer is responsible for making sure that:

- The Provision 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 Provision's monitoring and filtering systems

The Provision'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 Provision's DSL and ICT manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

- "Computers and equipment in the Provision's ICT suite are available to pupils only under the supervision of staff"
- "Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff"

6.2 Search and deletion

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

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

This includes, but is not limited to:

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from Stoke-on-Trent ERT Team.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is IWYS-Banned-Items-Policy-1.pdf
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

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

If inappropriate material is found on the device, it is up to [the staff member in conjunction with the DSL / The Proprietor to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

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

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

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

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

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

6.3 Unacceptable use of ICT and the internet outside of school

The Provision will sanction pupils, in line with the IWYS-Behaviour-Policy.pdf if a pupil engages in any of the following **at any time** (even if they are not on Provision 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 Provision'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 Provision into disrepute
- Sharing confidential information about the school, other pupils, or other members of the Provision 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 Provision's ICT facilities
- Causing intentional damage to the Provision'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

Please see our sanction via our IWYS-Behaviour-Policy.pdf

7. Parents/carers

7.1 Access to ICT facilities and materials

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

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

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

7.2 Communicating with or about the Provision 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 Provision through our website and social media channels.

We ask parents/carers to sign the agreement in appendix 2.

7.3 Communicating with parents/carers about pupil activity

The Provision will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the Provision pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the Provision to ensure a safe online environment is established for their child.

8. Data security

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

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

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

8.1 Passwords

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

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

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

8.2 Software updates, firewalls and anti-virus software

All of the Provision'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 Provision's ICT facilities.

Any personal devices using the Provision's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the Provision's data protection policy. I.W.Y.S.-Data-Retention-Policy.pdf (iwys.co.uk)

8.4 Access to facilities and materials

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

These access rights are managed by the Proprietor and ICTn Ltd

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 Charmaine Baines (Proprietor) immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 Encryption

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

Provision staff may only use personal devices (including computers and USB drives) to access Provision data, work remotely, or take personal data (such as pupil information) out of Provision if they have been specifically authorised to do so by the Proprietor.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICTN Ltd.

9. Protection from cyber attacks

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

The Provision will:

- Work with ICTN Ltd to make sure cyber security is given the time and resources it needs to make the Provision secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the Provision'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 Provision will verify this using a third-party audit (such as 360 degree safe) at least annually], to objectively test that what it has in place is effective
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date:** with a system in place to monitor when the Provision 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 at least once a day and store these backups on cloud based backup systems/external hard drives that aren't connected to the Provision network and which can stored off the Provision premises.

- Delegate specific responsibility for maintaining the security of our management information system (MIS) to ICTn Ltd.

- Make sure staff:
  - Enable multi-factor authentication where they can, on things like Provision email accounts
  - Store passwords securely using a password manager
- Make sure ICTN Ltd conduct regular access reviews to make sure each user in the Provision has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Develop, review and test an incident response plan with the ICTn including, for example, how the Provision 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 at least annually though ideally every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
-

10. Internet access

The Provision's wireless internet connection is secure and maintained by ICTn Ltd

10.1 Pupils

- Students do not have access to the internet login
- Laptops passwords are accessible to staff only
- We use ICTn – Senso filtering system
- Wi-Fi is limited to education

10.2 Parents/carers and visitors

Parents/carers and visitors to the Provision will not be permitted to use the Provision's WiFi unless specific authorisation is granted by the headteacher.

The Proprietor will only grant authorisation if:

- Parents/carers are working with the Provision in an official capacity (e.g. as a volunteer)
- Visitors need to access the Provision'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 Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The Proprietor and ICTn Ltd monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Provision

This policy will be reviewed at least annually but every 2 years.

12. Related policies

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

- Online safety
- Social media
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Mobile phone usage

Appendix 6: Glossary of cyber security terminology

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

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

TERM	DEFINITION
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.
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.