



West End Primary School

We work hard together to be excellent in all that we do. We are confident and compassionate, happy and have fun.

ICT and Internet Acceptable Use Policy

Document Detail	
Policy written by:	Becky Linton
Date:	July 2026 To be ratified by FGB in November 2026
Next review date by:	July 2027

Contents

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

Appendix 1 – Acceptable use of the internet agreement for parents/carers

Appendix 2 – Acceptable use agreement for pupils

Appendix 3 – Acceptable use agreement for staff, governors, volunteers and visitors

Appendix 4 – Glossary of cyber security terminology

1. Introduction

Information and communication technology (ICT) is an integral part of the way our school works and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, and administrative and pastoral functions of the school.

We recognise, however, that the ICT resources and facilities we use could pose risks to data protection, online safety and safeguarding.

This policy aims to:

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

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors, visitors, and anyone who has access to our IT and communication systems.

Misuse of IT and communications systems can damage our school and our reputation. Breaches of this policy may be dealt with under our staff code of conduct and behaviour policy.

2. Relevant legislation and guidance

This policy refers to, complies with, or otherwise has regard to, 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

Data (Use and Access) Act 2025

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 2025](#)

[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](#)

[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 4 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 any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral

Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful

Making or sharing of nude or 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

Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel

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 internet and 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

Please refer to West End Primary School AI policy for more information about this aspect.

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

5.1 Access to school ICT facilities and materials

Next Gen, Becky Linton (Headteacher) and Lindsey James (School Business Manager) manage 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.

5.1.1 Use of school-supplied equipment

School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required. Staff must:

- Use equipment and devices primarily for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality

- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations

- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device

- Lock devices with a password when unattended. Passwords must:

 - Not be shared with others and must be changed regularly

 - Be suitably strong

 - Not be reused across multiple accounts

- Update software, operating systems and applications when prompted, or as directed by the Next Gen

- Connect to the school network using approved and secure methods. When connecting to wi-fi networks outside of the school, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks

- Report any loss, theft, damage or compromise of a school device promptly to the School Business Manager (Lindsey James) or the Designated Safeguarding Lead (Becky Linton).

5.1.2 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.

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 subject access requests from individuals under the UK GDPR and 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 using a strong, state-of-the-art encryption standard 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 Becky Linton or Lindsey James immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. In circumstances where staff are provided with phones, these staff must use the 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.

If staff record phone calls, callers MUST be made aware that the conversation is being recorded and the reasons for doing so.

These might include but are not limited:

- Conversations around behaviour
- Conversations around attendance
- Discussing requests for term time holidays
- Taking advice from relevant professionals

We are a mobile phone free environment and pupils do not have access to phones during the day. Year 5 and Year 6 pupils who bring phones to school always place them into a box as they enter the classroom. The teacher then gives the phones back at the end of the school day as the pupils are leaving.

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 headteacher or school business 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 teaching 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 are also permitted to use their personal devices (such as mobile phones or tablets) in line with information set out in the Staff Code of Conduct & Online Safety Policy about personal device use - Staff must not use personal mobile phones or cameras in areas where children are present. Personal devices must be stored securely in classroom cupboards (if the staff member is class based) and not a pocket or a desk drawer. Staff must not use phones while walking through the school or playground, when the pupils are still in school, learning time or after school clubs. This includes speaking on the phone, sending a text or looking at the internet. Staff may only access personal phones during breaks and in designated staff-only areas. All photographs of children must be taken using school-owned devices.
- Staff may not store any school-related data on personal devices, on cloud storage or on personal removable storage devices.

- 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 Staff Code of Conduct and use of email (see section 5.1.2) 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 school has guidelines for staff on appropriate security settings for social media accounts (see Staff Code of Conduct).

5.5 Monitoring and filtering of the school network and use of ICT facilities

To comply with Department for Education (DfE) guidance on meeting digital and technology standards, and 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 ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. We use SENSO for filtering and monitoring purposes and the DSL (Becky Linton) and DDSLs (Karen Odell, Helen Dillon and Andrew Kelsey) have access to this account and are responsible for this.

The school reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the school, including for the following purposes:

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy
- To find lost messages or retrieve messages lost due to computer failure
- To help in the investigation of alleged wrongdoing
- To comply with any legal obligation

The list above is not exhaustive.

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 ICT manager, as appropriate.

Systems are reviewed once a year by Becky Linton, Lindsey James and Next Gen and this review is recorded – all records kept in central file. This is to ensure systems are working effectively on all devices.

6. Pupils

6.1 Access to ICT facilities

Computers and iPads are available to pupils only under the supervision of staff.

Emails and passwords are provided to pupils for educational purposes only. Pupils must not share their passwords with others, or use their email account to download files, including software from the internet or inappropriate content.

6.2 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with our behaviour policy if a pupil engages in any of the following **at any time** (even if they are not on school premises):

Using ICT or the internet to breach intellectual property rights or copyright

Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination

Breaching the school's policies or procedures

Any illegal conduct, or making statements which are deemed to be advocating illegal activity

Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

Making or sharing of nude or semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)

Activity which defames or disparages the school, or risks bringing the school into disrepute

Sharing confidential information about the school, other pupils, or other members of the school community

Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities

Causing intentional damage to the school's ICT facilities or materials

Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation

Using inappropriate or offensive language

7. Parents/carers

7.1 Access to ICT facilities and materials

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

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer 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/carers are granted access in this way, they must abide by this policy.

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

We ask parents/carers to sign the agreement in appendix 1.

8. 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 cyber crime technologies.

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

- Firewalls

- Security features

- User authentication and multi-factor authentication

- Anti-malware software

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users must not use the same passwords across multiple platforms.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. You must keep these passwords confidential and change them regularly.

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.

All staff will use the password manager required by the headteacher and the school business manager to help them store their passwords securely. Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

8.2 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 should not delete, destroy or modify existing systems, programs, information or data. Users must not download or install software from external sources without authorisation from the headteacher or the school business manager.

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.

8.3 Data protection

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

8.4 Access to facilities and materials

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

These access rights are managed by Next Gen, the school business manager and the headteacher.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the headteacher or 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 shut down completely at the end of each working day.

8.5 Encryption

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

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

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

9. Protection from cyber attacks

Staff need to know and will be trained through online safety training on the following:

How to check the sender address in an email

How to respond to a request for bank details, personal information or login details

How to 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:** use of fire wall
- **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

Delegate specific responsibility for maintaining the security of our management information system (MIS) to Next Gen

- 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

Make sure all necessary firewalls are in place and switched on (and that all areas of the network are secured effectively)

Make sure effective cyber breach prevention measures and processes are in place, e.g. endpoint detection and response systems

Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are

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

Work with Leed 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

Conduct a cyber risk assessment at least annually, and revisit it every term, or after a significant event has occurred

Appoint a digital lead (Karen Odell) to oversee cyber risk assessment.

10. Internet access

The school's wireless internet connection is secure. We use a firewall and SENSO to filter and monitor the use of the internet.

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

The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer 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) including supply teachers

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

11. Monitoring and review

The headteacher (Becky Linton), the digital lead monitor (Karen Odell) and the school business manager (Lindsey James) oversee the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed annually.

The governing board is responsible for reviewing this policy.

12. Related policies

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

- Online safety

- Safeguarding and child protection

- Behaviour

- Staff Code of Conduct

- Data protection

- Remote education

- Artificial Intelligence (AI) – including generating fake and deep fake images

Appendix 1: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carers:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school.
The school uses the following channels:

- Parent Mail
- School website
- School email addresses

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a school-related behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers

Signed:

Date:

Appendix 2: Acceptable use agreement for younger pupils (KS2)

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- Share my password with others or log in using someone else's name or password
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

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

Signed (pupil):

Date:

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

Signed (parent/carer):

Date:

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors

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

Name of staff member/governor/volunteer/visitor:

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

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

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

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

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

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 4: 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. Many of these terms are from the National Cyber Security Centre (NCSC)

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove viruses and other kinds of malicious software.
Breach	When your data, computer systems or networks are accessed or affected without authorisation.
Cloud	An on-demand, massively scalable service, hosted on a shared infrastructure 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	Any event that threatens the confidentiality, integrity, or availability of data within your computer network, or where the security of your system or service has otherwise been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from unauthorised 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 who uses their technology skills to gain unauthorised access to computers, systems and networks.
Malware	Malicious software. Any kind of software that can damage computer systems, networks or devices, which includes viruses, trojans or any code or content that is harmful.
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 with the end aim of fixing them.
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 or text messages sent to many people asking for sensitive information (such

TERM	DEFINITION
	as bank details or passwords) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems, usually by encrypting your files, until you make a payment (a ransom) for decryption.
Social engineering	Manipulating people into giving information or carrying out specific actions that's of use to an attacker.
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.