



# ICT and Internet Acceptable Use Policy

**Approved by Governors: September 2026**

**To be Reviewed: September 2027**

## Contents

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

## 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 students, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

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

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, 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 students safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, students, 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 [Professional code of conduct 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, students, 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 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
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams

- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its students, 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
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

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

#### **4.1 Exceptions from unacceptable use**

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

#### **4.2 Sanctions**

Students and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on staff code of conduct

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

### **5.1 Access to school ICT facilities and materials**

The school's Director of IT manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Director of IT Systems.

### 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, in accordance with the school's password policy (see section 8.1)
  - Not be reused across multiple accounts
- Update software, operating systems and applications when prompted, or as directed by the Director of IT Systems
- 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 Director of IT Systems, designated safeguarding lead and data protection officer

### 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. Staff must make sure multi-factor authentication is enabled on their email account(s).

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers and students, 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 the Director of IT Systems immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or students. 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.

The school can record incoming and outgoing phone conversations.

If you record calls, callers **must** be made aware that the conversation is being recorded and the reasons for doing so. Your school's phone system probably has an automated option you can use/adapt.

Explain when you record phone conversations and why. For instance:

- "All calls to the school office are recorded to aid administrators"
- "Calls are recorded for use in staff training"

Staff who would like to record a phone conversation should speak to the Director of IT Systems and the Head Teacher.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

Access may be granted to record conversations when:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

## 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 Director of IT Systems may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/non-break time.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no students are present
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes

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

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

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone policy.

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 students and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (see [Professional code of conduct policy](#)) 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. [Professional code of conduct policy](#)

### 5.3 Remote access

We allow specific staff to access the school's ICT facilities and materials remotely. They should do so using their Splashtop Business account as set up and configured by the ICT Support team.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the Director of IT Systems may require against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Our Data Protection Policy can be found on our website - <https://www.mardenhigh.net/about-us/policies/>

### 5.4 School social media accounts

The school has an official Facebook and X. account, managed by the Mass Media Coordinator. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

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

To 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. Web filtering is applied by our Fortigate Firewall and internet activity is monitored using NetSupport DNA. Emails are scanned/inspected for malware by Sophos Email Security.

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 body 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 Director of IT Systems, as appropriate.

## 6. Students

### 6.1 Access to ICT facilities

- Computers and equipment in the school's ICT suite are available to students only under the supervision of staff
- Email addresses and passwords are provided to students, for educational purposes only. Students must not share their passwords with others, or use their email account to share or download files, including software from the Internet or inappropriate content, without the permission of the Director of IT Systems
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Students will be provided with an account linked to the school's Google Workspace, which they can access from any device by using the following URL <https://www.mardenhigh.net>

### 6.3 Unacceptable use of ICT and the internet outside of school

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

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other students, 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 students, 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. .

### 7.3 Communicating with parents/carers about student activity

The school 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 students 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 school students will be interacting with online, including the purpose of the interaction.

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

## 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, students, 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 students 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 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 Director of IT Systems.

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 incoming files should always be virus-checked by the ICT department before they are downloaded.

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.

Our Data Protection policy can be found on our website - <https://www.mardenhigh.net/about-us/policies/>

## 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 Director of IT Systems.

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 Director of IT Systems 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 student 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 Director of IT Systems.

# 9. Protection from cyber attacks

Please see the glossary (appendix) 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 all users, including staff, students and governors (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:

- The methods hackers use for tricking people into disclosing personal information, including phishing
- Online safety and password security
- Social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
- The physical security of devices, for example not leaving a laptop unlocked and unattended
- The risks of using removable storage media, such as USBs
- Multi-factor authentication
- How and when to report a cyber incident or attack
- How and when to report a data breach
- Data protection for all staff. Staff who are exposed to higher-risk data will have more frequent training
- 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: the school will verify this using a third-party audit (such as 360 degree safe) [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 school needs to update its software
- Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be
- Back up critical data daily and store these backups on cloud-based backup systems that aren't connected to the school network and which can be stored off the school premises
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to School ICT and the ICT department

Make sure staff:

- Only use their designated Splashtop Business account for remote access when working from home
- 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
- 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 and checking if they have the Cyber Essentials (or a similarly effective and recognised) certification
- 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 our [LA] to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement
- Conduct a cyber risk assessment at least annually, and revisit it every term, or after a significant event has occurred
- Appoint a digital lead (from the senior leadership team) to oversee cyber risk assessment

## 10. Internet access

The school's wireless internet connection is secure.

- Access is filtered
- We have a designated SSID/Wireless Network for Curriculum devices, Governors and Visitors
- Any inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) must be reported to ICT Support.

### 10.1 Students

- WiFi is limited for use to connect school and 1:1 lease Chromebooks to the internet
- All internet activity is filtered by our Fortigate firewall
- students should not attempt to connect a personal device to the school WiFi at any time

### 10.2 Parents/carers and visitors

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

The headteacher will only grant authorisation if:

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

## 11. Monitoring and review

The headteacher and the Director of IT Systems 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 four years.

The governing body is responsible for reviewing/approving this policy.

## 12. Related policies

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

- Online safety

- Professional code of conduct
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote education
- Mobile phone usage
- Artificial Intelligence (AI)

## Appendix: 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) [glossary](#).

| TERM                   | DEFINITION                                                                                                                                                                                                        |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Antivirus</b>       | Software designed to detect, stop and remove viruses and other kinds of malicious software.                                                                                                                       |
| <b>Breach</b>          | When your data, computer systems or networks are accessed or affected without authorisation.                                                                                                                      |
| <b>Cloud</b>           | 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. |
| <b>Cyber attack</b>    | An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.                                                                                                                   |
| <b>Cyber incident</b>  | 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.                       |
| <b>Cyber security</b>  | The protection of your devices, services and networks (and the information they contain) from unauthorised theft or damage.                                                                                       |
| <b>Download attack</b> | Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.                                                                                          |
| <b>Firewall</b>        | Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.                                                                     |
| <b>Hacker</b>          | Someone who uses their technology skills to gain unauthorised access to computers, systems and networks.                                                                                                          |
| <b>Malware</b>         | 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.                                           |
| <b>Patching</b>        | Updating firmware or software to improve security and/or enhance functionality.                                                                                                                                   |

| TERM                                          | DEFINITION                                                                                                                                                                     |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Pentest</b>                                | 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.                        |
| <b>Pharming</b>                               | 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.                          |
| <b>Phishing</b>                               | Untargeted, mass emails or text messages sent to many people asking for sensitive information (such as bank details or passwords) or encouraging them to visit a fake website. |
| <b>Ransomware</b>                             | 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.                       |
| <b>Social engineering</b>                     | Manipulating people into giving information or carrying out specific actions that's of use to an attacker.                                                                     |
| <b>Spear-phishing</b>                         | 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.                                                 |
| <b>Trojan</b>                                 | A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.                                                                |
| <b>Two-factor/multi-factor authentication</b> | Using 2 or more different components to verify a user's identity.                                                                                                              |
| <b>Virus</b>                                  | Programmes designed to self-replicate and infect legitimate software programs or systems.                                                                                      |
| <b>Virtual private network (VPN)</b>          | An encrypted network which allows remote users to connect securely.                                                                                                            |
| <b>Whaling</b>                                | Highly-targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.                                                         |