SHINE

ACADEMIES

ICT and Acceptable Use Policy

Policy Type	Non-Statutory Trust Policy
Author	Governance and Compliance Manager
Approved By	Director of Operations
Approved Date	July 2024
Date of next review	Two Years
Version	1
Description of changes	N/A

CONTENTS

1. Introduction and Aims

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

Breaches of this policy may be dealt with under the following policies:

- Disciplinary Procedure
- School Behaviour Policy (for Pupils)
- Staff Code of Conduct
- Parent Code of Conduct
- Trustee and Governor Code of Conduct
- Volunteer 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 2024

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 school's ICT service

Users: anyone authorised by the school to use the school's ICT facilities, including governors, staff, trustees, 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 A for a glossary of cyber security terminology.

4. Unacceptable Use

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

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams

- Activity which defames or disparages the Trust or school, or risks bringing the Trust or school into disrepute
- Sharing confidential information about the Trust or school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting, or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic, or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):

  i. During assessments, including internal and external assessments, and coursework
  ii. 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 Trust reserves the right to amend this list at any time. The Trust Executive Leadership Team, 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 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 discretion of the Headteacher.

Permission must be sought from the Headteacher following the completion of a Risk Assessment.

- Pupils may use AI tools and generative chatbots:

i. As a research tool to help them find out about new topics and ideas

ii. 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 school's policies on:

- Disciplinary Procedure
- School Behaviour Policy (for Pupils)
- Staff Code of Conduct
- Parent Code of Conduct
- Trustee and Governor Code of Conduct
- Volunteer Policy

Copies of these policies can be found in the staff shared area or, in the case of the behaviour policy for each school, on the school website. Copies of policies can also be made available on request.

5. Staff (including Governors, Volunteers and Contractors)

5.1 Access to school ICT facilities and materials

The Trust's IT Service Provider Services4Schools 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 Office Manager / School Data Protection Lead.

Requests to access files or facilities will be assessed on a case-by-case basis by the Trust Central Team.

5.1.1 Use of phones and email

The Trust 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 school has provided.
Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the School Data Protection Lead or Trust Data Protection Officer immediately and follow our procedures set out in the Trust Data Protection Policy.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Staff who would like to record a phone conversation should speak to SHINE Director of Operations.

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

The following are examples of where the Trust may expect staff to want to record a telephone conversation (this list is not exhaustive):

- 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 CEO 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 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, books, videos or photos).

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

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media in the SHINE Social Media policy and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

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

5.3 Remote access

SHINE Academies allows staff to access the school's ICT facilities and materials remotely.

Staff should dial in using a virtual private network (VPN).

Access to school resources from remote locations is permitted through Office 365. To access school resources users must wither have a school managed device with Bitlocker. Or use MultiFactor authentication to access to portal. All users must be within the UK for access unless a request has been made prior to travelling abroad.

All requests must be process through the IT Service Desk.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the IT Service provider 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.

5.4 School social media accounts

The Trust and all schools have various social media accounts for Facebook, X and LinkedIn, managed by dedicated members of staff (a list can be provided on request).

Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

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

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

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

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

Further details about what systems and processes are used to filter and monitor online use and how you communicate this information to parents can be found on page 47 of SHINE's Safeguarding and Child Protection policy.

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 Trust Board is responsible for making sure that:

i. The Trust meets the DfE's filtering and monitoring standards

ii. Appropriate filtering and monitoring systems are in place

iii. Staff are aware of those systems and trained in their related roles and responsibilities

iv. For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns

v. It regularly reviews the effectiveness of the school's monitoring and filtering systems

The Trust's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place. Lightspeed Systems filtering agent runs on all school managed devices to control and monitor access to the Internet. Lightspeed Systems Alert runs on all school managed devices to safeguard. This is currently configured to report all safeguarding for student users only.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

ICT Facilities are made available under the following circumstances:

- Computers and equipment in the school ICT suites are available to pupils only under the supervision of staff
- Computers and equipment as an aid to learning e.g. Timetables practice, SEND provision
- 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

School staff have a responsibility to provide a safe environment in which pupils can learn as highlighted within Working Together to Safeguard Children and Keeping Children Safe in Education.
Under the Education Act 2011, the Headteacher, or any member of staff authorised by the Headteacher to do so, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting, ensuring it is justified and proportionate. Refer to Searching, Screening and Confiscation (July 2022) for more information. The Designated Safeguarding Lead (DSL) should be informed of any searching incidents. If the DSL finds evidence that child is at risk, they should make a referral to Children's Social Care.

Consider the following:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school Behaviour Policy 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 the headteacher or designated safeguarding lead.
- 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 (if the pupil refuses to co-operate, you should proceed according to the DfE Searching, Screening and Confiscation guidance).

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 available in the Behaviour Policy.
- 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 school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to Headteacher 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

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

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the school's 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
- 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 Trust, or any of the schools within the Trust, or brings the Trust or schools into disrepute
- Sharing confidential information about the Trust or any school within the Trust, other pupils, or other members of the Trust or 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 Trust's ICT facilities
- Causing intentional damage to the Trust'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 governor, 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 as it applies to staff.

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.

7.3 Communicating with parents/carers about pupil 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 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 school pupils 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

All users of the Trust'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.

All staff will use the password manager required by the IT Service Provider Services4Schools 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 Trust's ICT devices that support software updates, security updates and anti-virus products will have these installed and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the Trust or any of 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 SHINE's Data Protection Policy.

8.4 Access to facilities and materials

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

These access rights are managed by the Trust's IT Service Provider EdTech Solutions.

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 EdTech Solutions 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

SHINE Academies makes sure that its devices and systems have an appropriate level of encryption. Trust 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 relevant member of staff.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Trust's IT Service Provider EdTech Solutions.

9. Protection from Cyber Attacks

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

The Trust will:

- Work with Trustees and Governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:

i. Check the sender address in an email
ii. Respond to a request for bank details, personal information or login details
iii. 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:

i. **Proportionate**: the Trust will verify this using a third-party audit (such as 360 degree safe) to objectively test that what it has in place is effective
ii. **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe

iii. **Up to date:** with a system in place to monitor when the school needs to update its software

iv. **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 Offsite and in a separate cloud instance.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Arbor Support.

Make sure staff:

i. Dial into our network using a virtual private network (VPN) when working from home

ii. Enable multi-factor authentication where they can, on things like school email accounts

iii. Store passwords securely using a password manager

- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials 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'

10. Internet Access

The school's wireless internet connection is secure.

Each School has a filtering school wireless network. With its own VLAN to segregate traffic from other SSIDs.

Guest Wifi is available in all schools with filtering provided by Lightspeed DNS. Guest traffic is on its own VLAN. Filtering incidents can be reported via the IT Helpdesk.

10.1 Pupils

WiFi is available throughout the school. All pupils have a separate more restrictive level of filtering based on security groups.

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 to the SHINE Guest Wifi 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 Director of Operations for SHINE Academies will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every three years or when there are any changes to guidance or advancements in technology

12. Related Policies

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

- Codes of Conduct for Staff, Parents, Visitors and Governors/Trustees
- Social media
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote education

Appendix A – Glossary of Cyber Terms

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

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
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

TERM	DEFINITION
	computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
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

TERM	DEFINITION
	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.