St Bede's Catholic College

ICT and internet acceptable use policy

Contents

---

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our college 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 college.

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

This policy aims to:

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

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

By using the college's ICT facilities, governors, staff, students, volunteers, contractors and visitors acknowledge and accept this Acceptable Use Policy.

Misuse of IT and communications systems can damage our college and our reputation. Breaches of this policy may be dealt with under our Behaviour policy, E-Safety policy, Code of Conduct for employees and CES Disciplinary policy and procedure.

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 college's ICT service
- **Users:** anyone authorised by the college to use the college'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 college to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the college's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 1 for a glossary of cyber security terminology.

4. Unacceptable use

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

Unacceptable use of the college's ICT facilities includes:

- Using the college's ICT facilities to breach intellectual property rights or copyright
- Using the college's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the college'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 college, or risks bringing the college into disrepute
- Sharing confidential information about the college, its students, or other members of the college community

- Using the college'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 college's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the college'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 college'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 college's ICT facilities
- Causing intentional damage to the college's ICT facilities
- Removing, deleting or disposing of the college'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 college
- Using websites or mechanisms to bypass the college'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 Gemini):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

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

4.1 Exceptions from unacceptable use

Where the use of college ICT facilities (on the college 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 Principal's discretion. Applications should be made to the Principal in writing, explaining why the exemption is needed and why there are no workarounds available.

Students may use AI tools and generative chatbots:

I. As a research tool to help them find out about new topics and ideas
II. When given permission by the class teacher
III. When specifically studying and discussing AI in college work, for example in IT lessons or art homework about AI-generated images
IV. All AI-generated content must be properly attributed and declared by the student.

Sanctions

Students and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the college's policies on Behaviour, E-Safety, Code of Conduct and CES Disciplinary Policy and Procedure. These policies can be found on the college website or the internal staff intranet.

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

5.1 Access to college ICT facilities and materials

The college's Director of IT manages access to the college's ICT facilities and materials for college 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 college'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.

5.1.1 Use of college-supplied equipment

College-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 college. All college-supplied equipment remains the property of the college 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 college purposes and in line with the college's policies on safeguarding, data protection and confidentiality
- Treat the devices with the utmost care at all times. Where accidental damage occurs that is beyond acceptable levels of wear and tear, staff risk being charged for repairs or for a replacement device. Examples of accidental damage include water damage, scratched screens and dropped devices. Please note that this is not an exhaustive list.
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations (including cars). Staff risk being charged for a replacement device if one is stolen or damaged that has been left unattended.
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from college. 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 college'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
- Connect to the college network using approved and secure methods. When connecting to wi-fi networks outside of the college, 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 college device promptly to the Director of IT, designated safeguarding lead and data protection officer

5.1.2 Use of phones and email

The college 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.

All work-related business should be conducted using the email address the college 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 School Business Manager 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 college to conduct all work-related business.

College 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 college 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 for example, "All calls to the college office are recorded to aid administrators" or "Calls are recorded for use in staff training"

Staff who would like to record a phone conversation should contact the Safeguarding Lead via email setting out the reasons why they feel a recording should be made. Examples may include discussing complaints, discussing poor behaviour or taking advice from relevant professionals regarding safeguarding.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved. If a staff member feels threatened or is receiving abuse during a phone call, they must inform the other party that the recording is going to be switched on and then contact the Safeguarding Lead as soon as the call has been terminated.

5.2 Personal use

Staff are permitted to occasionally use college ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Director of IT 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
- 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 college'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 college's ICT facilities for personal use may put personal communications within the scope of the college's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are permitted to use their personal devices (such as mobile phones or tablets). However, screen locks must be in place, devices must be secured with anti-virus software where available and personal information about the college community must not be stored on the device.

Staff may not store any college-related data on personal devices, on personal cloud storage accounts or on personal removable storage devices.

Staff should be aware that personal use of ICT (even when not using college 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 college's guidelines on use of social media 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 college has guidelines for staff on appropriate security settings for social media accounts.

5.3 Remote access

We allow staff to access the college's ICT facilities and materials remotely using the Virtual Office and files stored in Google Drive.

The Virtual Office is managed by the Director of IT and staff should be aware that the system records their IP address and the length of time they are using it. Staff are required to use their ICT account to access this system, and must enable multi-factor authentication when available.

Staff accessing the college'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 college's ICT facilities outside the college and must take such precautions as the Director of IT 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. For further information, staff should consult the Data Protection Policy which can be found on the internal intranet.

5.4 Monitoring and filtering of the college 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 college reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

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

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The college uses Sophos Intercept X to filter web traffic, Impero to monitor internet usage and Sophos Central to manage application control.

The college 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 college, 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 college monitors ICT use in order to:

- Obtain information related to college business
- Investigate compliance with college policies, procedures and standards
- Ensure effective college 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 college 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 college's monitoring and filtering systems

The college'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 college's DSL and Director of IT, as appropriate.

6. Students

If students fail to comply with this Acceptable Use Policy, they will be subject to disciplinary action. This may include loss of access to the college network / internet, detentions, suspensions, contact with parents and, in the event of illegal activities, involvement of the police.

6.1 Access to ICT facilities

The college has a large collection of devices and software available for students to use.

- Computers and equipment in the college's ICT suite are available to students only under the supervision of staff
- Email addresses and passwords are provided to students via our Google Workspace for Education subscription. These accounts should be used 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 class teacher
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Sixth-form students can use the computers in the Directed Study room or Library independently, for educational purposes only

6.2 Unacceptable use of ICT and the internet outside of college

The college 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 college 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 college'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 college, or risks bringing the college into disrepute
- Sharing confidential information about the college, other students, or other members of the college 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 college's ICT facilities
- Causing intentional damage to the college's ICT facilities or materials
- Using the college ICT systems or devices for online gaming, online gambling or internet shopping. File sharing or video broadcasting (e.g. YouTube) must only be carried out with the direct supervision of the teacher.
- 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
- Uploading, downloading or accessing any materials which are illegal or inappropriate or may cause harm or distress to others.
- Attempt to use any programmes or software that might allow the filtering / security systems in place to be bypassed.
- Taking or distributing images of anyone without their permission.
- Opening any hyperlinks in emails or attachments in emails if they have any concerns about the validity of the email, unless they know and trust the person / organisation who sent the email (due to the risk of the attachment containing viruses or other harmful programmes).
- Installing or attempting to install or store programmes of any type on any school device, nor attempt to alter computer settings.

6.3 Personal Devices

Students must only use their own personal storage devices (e.g. USB devices and portable storage devices. This does not include mobile phone storage.) in college if they have permission from their teacher. Students are encouraged to use Google Workspace to store and access their files from home.

Only 6th form students are permitted to use their own digital devices (mobile phones, laptops and tablets) in college.

If students do use their own devices in the college, they must follow the rules set out in this policy, in the same way as if they were using college equipment and they accept that the college will not accept responsibility for damage or loss of any such equipment.

6.4 Social Media

Students must not use social networking sites either at college or elsewhere, to make public comments about St. Bede's Catholic College or Areté Sixth Form, staff or students, which are defamatory, liable to cause offense or bring the college or Sixth Form into disrepute.

Only 6th Form students are permitted to use social media sites at college, but not during lesson times.

7. Parents/carers

7.1 Access to ICT facilities and materials

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

However, parents/carers working for, or with, the college in an official capacity (for instance, as a volunteer or as a member of the governing body) may be granted an appropriate level of access, or be permitted to use the college'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 college 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 college through our website and social media channels.

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

7.3 Communicating with parents/carers about student activity

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

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

8. Data security

The college 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 college'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 college'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.

All users are encouraged to follow the advice given by the National Cyber Security Centre when setting their own passwords (https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online). As a minimum, all passwords are required to have at last 8 characters, contain a capital letter, number and symbol.

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.

Staff and Sixth Form students will be required to change their network and Google password every 90 days. Students in years 7 to 11 will have their passwords for the network and Google accounts set for them.

Further information about the password policy and requirements can be obtained from the Director of IT.

8.2 Software updates, firewalls and anti-virus software

All of the college'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 Director of IT.

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 college's ICT facilities.

Any incoming files are always virus-checked by the anti-virus program through 'Real-time Scanning'. Any personal devices using the college's network must all be configured in this way.

8.3 Data protection

All users must store and process personal data in line with data protection regulations and the college's Data Protection Policy. This policy can be found the college website.

8.4 Access to facilities and materials

All users of the college's ICT facilities will have clearly defined access rights to college systems, files and devices. These access rights are managed by the Director of IT.

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 Director of IT 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 college makes sure that its devices and systems have an appropriate level of encryption.

College staff may only use personal devices (including computers and USB drives) to access college data, work remotely, or take personal data (such as student information) out of college if the devices have appropriate levels of security and encryption, as defined by the Director of IT.

9. Wireless access

The college's wireless internet connection is secure.

All devices connected to the college wireless network will be filtered and monitored in line with section 5.5 of this policy. Filtering levels are based on the network to which the user has connected.

To ensure users connect to the appropriate network, there are separate 'Bring Your Own Device' (BYOD) networks for staff and sixth form students to which they can connect their personal devices should they choose to do so. These are secured using a generic password at stage 1, and entering network credentials at stage 2. Students in Years 7 to 11 should not attempt to connect to the college wireless networks.

Devices connected to the wireless network should only be used in line with the conditions of this policy.

9.1 Parents/carers and visitors

Parents/carers and visitors to the college are able to connect their devices to a specific 'guest' network. This is secured using a password, and is only allowed to access the internet with the strictest level of filtering. Parents/carers and visitors should not attempt to access any other part of the network.

Parents/carers and visitors should only access the college's wireless network 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 wireless password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Monitoring and review

The Principal and Director of IT monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the college.

This policy will be reviewed every two years.

Updated January 2026
To be reviewed January 2028

Appendix 1: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the college will put in place. Many of these terms are from the National Cyber Security Centre (NCSC) glossary.

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.

TERM	DEFINITION
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 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.