St Bede's Catholic College

IT Acceptable Use Policy

Approved by Governors October 2023

To be reviewed October 2025

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.

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

This policy aims to:

I. Set guidelines and rules on the use of college ICT resources for staff, students, parents/carers and governors

II. Establish clear expectations for the way all members of the college community engage with each other online

III. Support the college's policies on data protection, online safety and safeguarding

IV. Prevent disruption that could occur to the college through the misuse, or attempted misuse, of ICT systems

V. 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 and visitors.

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

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, and complies with, the following legislation and guidance:

I. Data Protection Act 2018

II. 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

III. Computer Misuse Act 1990

IV. Human Rights Act 1998

V. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

VI. Education Act 2011

VII. Freedom of Information Act 2000

VIII. Education and Inspections Act 2006

IX. Keeping Children Safe in Education 2023

X. Searching, screening and confiscation: advice for colleges 2022

XI. National Cyber Security Centre (NCSC): Cyber Security for Colleges

XII. Education and Training (Welfare of Children) Act 2021

XIII. UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

XIV. Meeting digital and technology standards in colleges and colleges

3. Definitions

I. **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

II. **Users:** anyone authorised by the college to use the college's ICT facilities, including governors, staff, students, volunteers, contractors and visitors

III. **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user

IV. **Authorised personnel:** employees authorised by the college to perform systems administration and/or monitoring of the ICT facilities

V. **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:

I. Using the college's ICT facilities to breach intellectual property rights or copyright

II. Using the college's ICT facilities to bully or harass someone else, or to promote unlawful discrimination

III. Breaching the college's policies or procedures

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

V. Online gambling, inappropriate advertising, phishing and/or financial scams

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

VII. Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams

VIII. Activity which defames or disparages the college, or risks bringing the college into disrepute

IX. Sharing confidential information about the college, its students, or other members of the college community

X. Connecting any device to the college's ICT network without approval from authorised personnel

XI. 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

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

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

XIV. Causing intentional damage to the college's ICT facilities

XV. Removing, deleting or disposing of the college's ICT equipment, systems, programmes or information without permission from authorised personnel

XVI. 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

XVII. Using inappropriate or offensive language

XVIII. Promoting a private business, unless that business is directly related to the college

XIX. Using websites or mechanisms to bypass the college's filtering or monitoring mechanisms

XX. Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

XXI. Using AI tools and generative chatbots (such as ChatGPT and Google Bard):

- 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.

4.2 Sanctions

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

5. Monitoring and filtering of the college network and use of ICT facilities

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:

I. Internet sites visited

II. Bandwidth usage

III. Email accounts

IV. Telephone calls

V. User activity/access logs

VI. 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 monitors ICT use in order to:

I. Obtain information related to college business

II. Investigate compliance with college policies, procedures and standards

III. Ensure effective college and ICT operation

IV. Conduct training or quality control exercises

V. Prevent or detect crime

VI. 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:

I. The college 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
    a. For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
IV. 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 Senior Network Manager, as appropriate.

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

6.1 Access to college ICT facilities and materials

The college's Senior Network Manager manages access to the college's ICT facilities and materials for college staff. That includes, but is not limited to:

I. Computers, tablets, mobile phones and other devices
II. 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 Senior Network Manager.

6.1.1 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 enable multi-factor authentication 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 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 Business Manager immediately and follow our data breach procedure.

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

6.2 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 Senior Network Manager may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

I. Does not take place during contact time

II. Does not constitute 'unacceptable use', as defined in section 4

III. Takes place when no students are present

IV. 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 and personal information about the college community must not be stored on the device.

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 5.1.1) to protect themselves online and avoid compromising their professional integrity.

6.2.1 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.

6.3 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 Senior Network Manager 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 Google Account to access this system, which is protected with multi-factor authentication.

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 Senior Network Manager 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 site.

6.4 College social media accounts

The college has an official Twitter account, managed by the Office Manager. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The college 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.

7. 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.

7.1 Access to ICT facilities

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

I. Computers and equipment in the college's ICT suite are available to students only under the supervision of staff
II. Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
III. Students will be provided with an account linked to the college's Google Workspace for Education environment, which they can access from any device using the official Google apps or by visiting accounts.google.com
IV. Sixth-form students can use the computers in the Directed Study room or Library independently, for educational purposes only

7.2 Search and deletion

Under the Education Act 2011, the Principal, and any member of staff authorised to do so by the Principal, can search students and confiscate their mobile phones, computers or other devices. In every case, the authorised staff member will consult with the Principal and Designated Safeguarding Lead to consider when it is appropriate to;

- Confiscate a device OR
- Confiscate a device, search and view content

Possible reasons to **confiscate** a device;

- Content poses a risk to staff or students, and/or
- Is evidence in relation to a potential offence
- Poses a threat to the disruption of teaching

This includes, but is not limited to:

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

The device will not be searched or content deleted at this stage.

NOTE: Confiscation because of breaking the "on site, out of sight" rule falls outside of this guidance. In these cases all staff may confiscate a mobile phone.

Searching content on a confiscated device - Urgency

Before a search and viewing of content, the Principal or authorised staff member will consult with the Designated Safeguarding Lead and carry out the following steps;

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. For example, if there is data or files on the device that might cause immediate harm to a person, or persons, or the college as an organisation, a search should follow.
- If the search is not urgent, seek further advice from other staff and outside agencies before proceeding (e.g Pastoral team, Children's Services, Police) and contact parents/carers to inform them that a search is necessary.
- If a search is agreed, proceed to 'Viewing content' below.

Viewing content

When searching a device, particular care must be taken to follow these steps;

1. Seek the student's co-operation, explain to the student why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it.
2. Select an appropriate location away from other children
3. Ensure that there is a witness to the search of the device
4. Record the date and time, name of the child and where, when and why the search took place

A special note - Indecent Images of Children:

If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must **never copy, print, store, share or save such images.** When an incident might involve an indecent image of a child and/or video, the member of staff should do the following;

a) Confiscate the device
b) Avoid looking at the device
c) Report the incident to the Designated Safeguarding Lead or Deputy DSL. The DSL will then follow safeguarding procedures as described in KCSIE.

Deleting content

If a member of staff finds any image, data or file that they suspect might constitute a specified offence, then they must be delivered to the police as soon as possible. In those instances, the data or files **should not be deleted**.

If the data or files are not suspected to be evidence of a crime, a member of staff may delete the data or files if the continued existence of the data is likely to continue to cause harm to any person and the person and/or the parent refuses to delete the data or files themselves.

The DSL (or deputy) should:

- record any searching incidents
- record that a search has revealed a safeguarding risk and take appropriate action

References

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

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

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

7.3 Action to reduce risk of future harm

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, to prevent future harm.

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 could be, used to:

I. Cause immediate harm, **and/or**
II. Undermine the immediate safe environment of the college or disrupt teaching, **and/or**
III. Commit an offence in the future

If inappropriate material is found on the device, it is up to the Principal and the Designated Safeguarding Lead 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. If possible, a photograph of the screen should be taken as evidence before deletion.

7.4 Action to deal with suspected historical harm

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 historical 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:

I. They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**

II. The student 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:

I. **Not** view the image

II. **Not** copy, print, share, store or save the image

III. 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 students will be carried out in line with:

I. The DfE's latest guidance on searching, screening and confiscation

II. UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

III. Our behaviour policy

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

7.5 Unacceptable use of ICT and the internet outside of college

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

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

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

III. Breaching the college's policies or procedures

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

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

VI. 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)

VII. Activity which defames or disparages the college, or risks bringing the college into disrepute

VIII. Sharing confidential information about the college, other students, or other members of the college community

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

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

XI. Causing intentional damage to the college's ICT facilities or materials

XII. 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.

XIII. 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

XIV. Using inappropriate or offensive language

XV. Uploading, downloading or accessing any materials which are illegal or inappropriate or may cause harm or distress to others.

XVI. Attempt to use any programmes or software that might allow the filtering / security systems in place to be bypassed.

XVII. Taking or distributing images of anyone without their permission.

XVIII. 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).

XIX. Installing or attempting to install or store programmes of any type on any school device, nor attempt to alter computer settings.

7.6 Student Safety

To ensure student safety:

I. The college will visually monitor students' use of the systems, devices and digital communications.
II. Students must keep passwords safe and secure - they must not share them, nor will they try to use any other person's username and password. Students should not write down or store a password where it is possible that someone may steal it.
III. The college systems and devices are primarily intended for educational use and students will not use them for personal or recreational use unless they have permission from their teacher.
IV. Students will not try (unless they have permission from their teacher) to make large downloads or uploads (large is classed as any file above 1GB) that might take up internet capacity and prevent other users from being able to carry out their work.
V. Students must respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
VI. Students must be polite and responsible when they communicate with others. They must appreciate that others may have different opinions.
VII. Students must immediately report any damage or faults involving equipment or software, however this may have happened, to their class teacher or to IT Support.

7.7 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.

7.8 Social Media

Students must not use social networking sites, such as Twitter or Facebook, 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.

7.9 Internet Use

Students should ensure that they have permission to use the original work of others in their own work.

Where work is protected by copyright, students will not try to download copies (including music and videos).

When students use the internet to find information, they should take care to check that the information that they access is accurate, and understand that the work of others may not be truthful and may be a deliberate attempt to mislead them.

8. Parents/carers

8.1 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 PTA) may be granted an appropriate level of access, or be permitted to use the college's facilities at the Principal's discretion.

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

8.2 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.

8.3 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.

9. 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 colleges and colleges, including the use of:

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

Further information on data security such as a password policy, firewall policy and multi-factor authentication can be found in the IT Security Policy. Information about data protection can be found in the Data Protection Policy.

10. Monitoring and review

The Principal and Senior Network Manager 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.

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

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. They're from the National Cyber Security Centre (NCSC) glossary.

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

TERM	DEFINITION
	details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.