ICT and Internet Acceptable Use Policy

Title:	ICT and Acceptable Use Policy	
Document owner:	Head of IT	
Reviewed/updated by:	Head of IT	
Version:	2	
Review cycle:	Annual	
Date of update:	October 2025	
Next due:	October 2026	
Approval Level:	SLT	Y
	Governors	Y via Audit
Date Approved:	November 2025	
Publication:	Intranet	Y
	Website	Y
	Students	Y

Version	Author	Date	Section	Changes summary
2	A Lawson A Campbell	October 2025	4	Changes made in relation to AI in line with the updated policy on “the Key” (Education Policy template resource platform)

ICT and Internet Acceptable Use Policy

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, governors, volunteers, contractors and visitors.
- 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, parents, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our College Disciplinary Policy or Student Positive Behaviour 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 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
- UKCIS 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
- Generative AI: product safety expectations - GOV.UK

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 which 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 4 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, 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
- 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 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, Google Gemini and Microsoft CoPilot):

- 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
- Craven College will treat any use of AI to access harmful content or bully students in line with this policy and our Safeguarding Children and Vulnerable Adults Policy.

This is not an exhaustive list. The college reserves the right to amend this list at any time. The Principal 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 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.

Using AI Tools:

- Students may use AI tools and generative chatbots:
  - As a research tool to help them find out about new topics and ideas
  - 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

Approval requests for such activities should be emailed to servicedesk@craven-college.ac.uk with a subject of "Unacceptable Use Exception Request" where the request will be initially reviewed by the ICT Team and forwarded to the Principal for authorisation.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the College Disciplinary Policy or Student Positive Behaviour Policy.

In the event of any failure to comply with the conditions of this Acceptable Use Policy, the College may in its sole discretion:

- Restrict or terminate a user's right to use the College ICT facilities.
- Withdraw or remove any material uploaded by that User in contravention of this Policy.
- Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.
- Any disciplinary action, arising from breach of this policy, shall be taken in accordance with the College's Disciplinary Policy. Disciplinary action may ultimately lead to dismissal.

Staff can find the latest version of the College disciplinary Policy on the staff intranet.

Students can find the latest version of the Student Positive Behaviour Policy on the Craven College website.

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

5.1 Access to college ICT facilities and materials

The college's ICT Team manage 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 access college ICT facilities remotely will be prompted to setup multi-factor authentication either using the Microsoft Authenticator App or via a Token fob by IT upon request.

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 ICT Team by email to servicedesk@craven-college.ac.uk

5.1.1 Use of phones and email

The college provides each member of staff with a College email address.

This email account should be used for work purposes only. Staff must enable multi-factor authentication on their email account(s).

All work-related business must be conducted using the email address the college has provided.

Staff must not share their personal email addresses with parents 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 Data Protection Officer by emailing dpo@craven-college.ac.uk immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents 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.

5.1.2 Storing of Files

College preference is to store work-related files on One Drive. One Drive is a cloud-based file storage, synchronisation, and collaboration service offered through Microsoft Office 365 and managed by the College ICT Team. It enables files to be stored in the Microsoft cloud and allows files to be accessed by staff and students through a web browser, desktop synchronization client, or mobile device app.

The following guidelines must be observed whilst using OneDrive in Craven College:

- One Drive should be used to store your work-related files, in accordance with this acceptable use policy. It should not be used for personal files, photos, media files, etc.
- The IT Team does not have the ability to extend your space allowance, you are responsible for managing your allocated space accordingly.
- All your computers and devices that are synced with One Drive shall be password protected with a strong password to prevent unauthorized data access.
- You shall report any lost or stolen computer or device that is synced with One Drive to the ICT Team as soon as possible.
- You can share files outside of Office 365 (e.g. with students or outside entities). You should limit file sharing to those with a legitimate need in order to perform College business and ensure that files with protected personal information (e.g. personally identifiable information, student numbers, grades, etc.) or confidential information are not shared inappropriately. Remember, once a file is shared with someone, they can download it and share it with others
- Remove individuals when they no longer require access to shared files or folders.
- Be careful sending links to shared folders because they can often be forwarded to others who you did not provide access to.
- Any files or documents that are shared externally will expire after 30 days. The ICT Team reserves the right to terminate any anonymous links to files at any time.
- Documents and files stored within OneDrive remain your responsibility.

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

Staff may not use the 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 also permitted to use their personal devices (such as mobile phones or tablets) in line with the college’s Bring your own device Policy.

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 could see them.

Staff should take care to follow the college’s guidelines on use of social media (our Social and Electronic Media Policy can be found on our staff intranet) 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 always appropriate.

The college has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access the bulk of college's ICT facilities and materials remotely via our Myday portal accessed here https://craven.myday.cloud/ using a College email address secured with multi-factor authentication.

Some systems are not accessible remotely without using virtual private network (VPN) software. Access to the VPN software must be requested by your line manager with an email to servicedesk@craven-college.ac.uk detailing what systems are required to access and why.

The ICT Team will then review the request and if access is granted to use the VPN software you will be asked to visit the ICT office to have the software installed with an explanation on how to use and access those systems.

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 take precautions such as:

- screen lock your computer whenever it is left unattended;
- ensure you're not using a shared login that could be accessed by anyone else;
- store confidential papers securely when not in use;
- ensure the secure disposal of confidential materials;
- ensure the device you are using is fully up to date with security patches and operating system updates. If you believe the device is old and potentially vulnerable do not access College ICT facilities on that device.
- ensure the device has appropriate and up-to-date anti-virus software;
- ensure the device can only be accessed with a unique PIN (at least 8 characters) or Password (at least 14 characters);
- be diligent with checking for a potential cyber security issue, such as virus, ransomware, phishing or attempt to gain credentials. Issues such as these should be reported to servicedesk@craven-college.ac.uk
- be mindful of anyone who may be looking over your shoulder;
- ensure you're not connected to an open, password less Wi-fi system which can be found for example in some Cafés or Hotels.
- don't write down any usernames or passwords that could be found by someone else;
- USB drives are not recommended;

Staff are responsible for ensuring the security of all college equipment, documents and information while you are working remotely. You must take all necessary steps to ensure that private and confidential material is kept secure at all times.

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

Our Data Protection Policy can be found on the staff intranet.

Staff working flexibly from home should also refer to the Hybrid Working Policy which can be found on our staff intranet.

5.4 College social media accounts

The college has official social media accounts, managed by Marketing Team. Staff members who have not been authorised to manage, or post to, any of the accounts, must not access, or attempt to access, those accounts.

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.

5.5 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:

- 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 systems in use by for monitoring are:

Hardware based:

Our College firewall solutions at the Aireville Campus, Auction mart site, Ripon site and Leeds site which are managed and monitored by a 3rd party supplier.

Software based:

- Smoothwall Monitor safeguarding solution installed on all College Windows devices. For further information on the Smoothwall monitoring solution, see section 13.
- Data collected from the following:
    - Microsoft Windows
    - Microsoft Active Directory and Azure Active Directory
    - Microsoft Office 365
    - Malwarebytes Anti-Malware Solution

The effectiveness of any filtering and monitoring will be regularly reviewed. Where appropriate, authorised personnel may raise concerns about monitored activity with the college's designated safeguarding lead (DSL) and Head of IT, as appropriate.

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

- Detect or prevent potential safeguarding issues

The governing board will receive regular reports on the effectiveness of the college's monitoring and filtering systems.

6. Students

6.1 Access to ICT facilities

- Computers and equipment in the college's Learning Hub are available to students only under the supervision of Learning Resource Centre staff
- Specialist ICT equipment, such as that used for music, esports, photography or design and technology, must only be used under the supervision of staff"
- Computers and equipment are available in certain classrooms but only under the supervision of staff.
- Certain classes may require you to loan a laptop from a laptop caddy under the supervision of staff.
- Laptops are available for short term loan (8 Hours) via laptop locker solutions accessed using student college ID Passes. Loans are recorded electronically and monitored for misuse or non-return.
- A small number of laptops are available for those students that have no access to a device at home but may need them as part of their course. These should be requested to our Student Services team.
- Students will be provided with a college account linked to the college's virtual learning environment, which will be explained during student induction.
- Students can access a dedicated home page with systems related only to students via: https://craven.myday.cloud/ (there is also a mobile app version called MyCraven which can be downloaded from the relevant app stores)

6.2 Search, confiscation 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 that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or students, **and/or**
- Is identified in the college rules 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:

- Assess how urgent the search is and consider the risk to other students and staff. If the search is not urgent, they will seek advice from Principal and Designated Safeguarding Lead (DSL)or Deputy Designated Safeguarding Leads (DDSL).
- 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
- Seek the student's co-operation

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a student was in possession of a banned item.
- 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, or could be used to:

- Cause harm, **and/or**
- Undermine the safe environment of the college or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL / Principal / DDSL or other members of the senior leadership team 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 if there is a good reason to erase data or files from a device, staff members will consider if 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 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 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:

- **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) 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:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Student Positive Behaviour Policy / Searching (non-contact), Screening and Confiscation Policy and Guidelines

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

6.3 Unacceptable use of ICT and the internet outside of college

The college will sanction students, in line with the Student Positive 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
- 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

For sanctions see section 4.2 above.

6.4 Monitoring and filtering of the college network and use of ICT facilities

College devices available to use for Students are monitored, please see Section 5.5 for details.

7. Parents

7.1 Access to ICT facilities and materials

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

However, parents working for, or with, the college in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access, or be permitted to use the college's facilities at the Principals discretion.

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

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 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.

7.3 Communicating with parents about student activity

Parents will be made aware should a student breach the terms of this acceptable use policy.

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 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

8.1 Passwords

All users of the college's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Passwords must:

- Be at least 14 characters Long
- Contain 3 of the following, lowercase, uppercase, number, special characters
- Be easy to remember, hard to guess. Think of two longer or three or four words that mean something to you, eg. PurpleFlower1234
- Not contain your name or username

With guidance from the National Cyber Security Centre passwords are no longer set to periodically expire.

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 students who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls and anti-virus software

All of the 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 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 personal devices using the college's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the college's data protection policy.

Our Data Protection Policy can be found on our website www.craven-college.ac.uk and searching for data protection.

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 ICT Team for most systems.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should immediately alert servicedesk@craven-college.ac.uk to correct the access and dpo@craven-college.ac.uk if a data breach has occurred.

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, staff must not share or write down their Bitlocker encyption code in a place that someone else may find it, for example stuck to the device, or in a bag used to carry a device.

9. Protection from cyber attacks

Please see the glossary (appendix 4) to help you understand cyber security terminology.

The college will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the college secure
- Provide bi-annual training for staff (and include this training in any induction for new starters, if they join outside of the college's bi-annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data

- Put controls in place that are:
    - **Proportionate**: the college will verify this using a third-party audit to objectively test that what it has in place is effective
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the college needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT and MIS Departments.
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like college email accounts
- Make sure ICT staff conduct regular access reviews to make sure each user in the college 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 college 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 College wireless internet connection is secure and has two Wi-fi networks available:

1) CC-Wifi which is to be used by staff and students using their college username and password.
    a. The CC-Wifi network is able to detect if you are using a College device or personal device, with College devices being able to access the internet and internal resources but personal devices are only able to access the internet, not any internal systems.
    b. However all systems students need can be accessed via the internet.
    c. Printing is unavailable if using personal devices.

2) CC-Internet which is to be used by guests visiting the College.
    a. Access must be requested in advance to servicedesk@craven-college.ac.uk
    b. All connections to CC-Internet need a unique key

Internet filtering is in place for any connections via the College Wi-fi, you may find certain categories of sites are blocked for access. However, category blocking isn't perfect and relies on 3rd Party classification of websites, if you deem a website inappropriate that should be blocked or want to access a website needed for your course, please email a request to servicedesk@craven-college.ac.uk for review.

10.1 Students

Students can access the Wi-fi named “CC-Wifi” as explained above using their college username and password.

- Wi-fi is available across many of the classrooms and communal areas across College. There are certain exceptions such as workshops where use of wireless devices isn’t expected. Should you experience a Wi-fi outage or believe there should be Wi-fi in an area of College not currently covered please email your request to servicedesk@craven-college.ac.uk with specifics of the area e.g. room number.

10.2 Parents and visitors

Parents and visitors to the college will not be permitted to use the college’s WiFi unless specific authorisation is granted or a limited time key is generated for specific events such as open evenings.

Authorisation could be granted if:

- Parents are working with the college in an official capacity (e.g. as a volunteer)
- Visitors need to access the college’s WiFi 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 senior leadership team, the head of IT and safeguarding team 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 year.

The senior leadership team is responsible for reviewing and approving this policy.

12. Related policies

This policy should be read alongside the college’s policies on:

- Social and Electronic Media Policy
- Safeguarding Children and Vulnerable Adults Policy
- Student Positive Behaviour Policy
- Staff Disciplinary Policy
- Data protection Policy
- Hybrid and Remote Working Policy
- Searching (non-contact), Screening and Confiscation Policy and Guidelines
- Zero Tolerance Policy

13. Further Information on Smoothwall Monitoring solution:

For any college owned machines that have a Windows Operating System which includes staff laptops and classroom machines the Smoothwall software is installed and constantly monitoring. Key points are:

- The software monitors keystrokes so it doesn’t matter if you type something but don’t press send, it will capture that it’s been typed.

- It doesn’t matter what application you're using on the college device as it’s monitoring keystrokes, so all applications are monitored.
- It doesn’t monitor non-college owned devices.
- It also doesn’t matter if you are r offline from the internet or online, it will still monitor while offline and then report in when back online.
- It doesn’t matter what College site you're at, or even at home, it will continue to monitor.

Alerts to the safeguarding team are sent in real-time by phone depending on alert level, email, and also stored within a portal for the safeguarding team to review.

The software monitors and assesses for the following risks:

Profile	**Description**
Cyberbully (Bullying and Discrimination)	A person who singles out individuals for a campaign or intimidation, abuse, harassment and exclusion and may encourage others to join in. Someone who may post material intended to shame and humiliate their target and who regularly engages in personal abuse against others.
Cybersexer	A person who makes frequent sexual overtures to others or engages in cybersex or talk of a highly sexual nature.
Offensive User	A person who engages in high use of profanity, without personally abusing others in a bullying manner. One who may introduce subjects or images that are highly distressing to others.
Oversharer	A person who regularly attempts to share personal information that would make them contactable online or offline or would result in a serious personal data breach.
Potential Pedophile (Grooming and child sexual exploitation)	A person who is suspected to be over the age of 18 who has contact with someone who is suspected to be under 18 for sexual purposes. Who may establish trust with the child by appearing sympathetic to their problems and on their side, who may encourage the child to share details about their life or share information that will make then contactable online or offline. A person who may establish the child’s sexual experience, desensitise the child to sexual discussion, normalise it and encourage the child to participate in it. Someone who may send or request nude photos or webcam sessions with the child and who may ultimately attempt an offline meeting.
Terrorist	A person who makes direct threats to undertake acts of terrorism including bombing, biological attack, kidnap and execution, against a high-profile person or the general public.

	OR A person who promotes terrorist activity carried out by others as rational, morally just or a duty. One who encourages others to carry out unofficial or unauthorized acts of violence or intimidation against others in the pursuit of their political or religious aims. A person who encourages demonization of those outside their ideological sphere, often with the use of political or religious propaganda.
Vulnerable Person **(Suicide / Self Harm)**	A person who makes credible threats of suicide or self-harm or engages in suicidal talk. Someone who appears to be at current risk of sexual or physical abuse offline or is giving indications of suffering from an untreated eating disorder, being severely distressed.
General Risk	This is used for situations where our Risk Analysts have spotted something unusual or concerning which they feel the school should be alerted to, which doesn't fit clearly inside any of the other category descriptions.

DO NOT ACCEPT FRIEND REQUESTS FROM STUDENTS ON SOCIAL MEDIA

Appendix 1: Facebook cheat sheet for staff

10 rules for college staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if you don't, ensure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Don't share anything publicly that you wouldn't be just as happy showing your students.
6. Don't use social media sites during college hours.
7. Don't make comments about your job, your colleagues, our college or your students online – once it's out there, it's out there.
8. Don't associate yourself with the college on your profile (e.g. by setting it as your workplace, or by 'checking in' at a college event).
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information.
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or students).

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent's friend request or message might set an unwelcome precedent for both you and other teachers at the college
    - Students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use agreement for students

Acceptable use of the college's ICT facilities and internet: Agreement for students
Name of Student: **Student Reference Number:**
When using the college's ICT facilities and accessing the internet in college: • I will only use ICT systems in School, including the internet, e-mail, digital video, mobile technologies, etc. for College purposes. • I will not download or install software on College technologies. • I will only log on to the College network with my own user name and password and not share my personal information with other parties. • I will make sure that all IT communications with Students, Tutors or others is responsible and sensible. • I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use. • I will not use the colleges ICT facilities to bully or harass someone else or to promote unlawful discrimination. • I will support the College approach to online safety and will not deliberately browse, download, upload or forward/share material that could be considered offensive or illegal (this can include photographs, images, videos, emails, sound clips which are pornographic, obscene or otherwise inappropriate or offensive). If I accidentally come across any such material, I will report it immediately to my Tutor or Head of Department. • I will not use the colleges ICT facilities to engage in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way • Images of Students and/or Staff will only be taken with the permission of the person involved and will be stored and used for College purposes in line with College Policy. Images should not be distributed outside the College network without the permission of the Head of Department. • I will not gain or attempt to gain access to restricted areas of the network or to any password protected information. • I will not use the college ICT devices for any online gambling, inappropriate advertising, phishing and/or financial scams. • I will ensure that my online activity, both in College and outside College, will not cause Craven College, the staff, Students or others distress or bring into disrepute. • I will respect the privacy and ownership of others' work online at all times. • I will not attempt to bypass the internet filtering system. • I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to appropriate staff. • I understand that these rules are designed to keep me safe and that if they are not followed, College sanctions will be applied, and my parent/ carer may be contacted if I am under 18. • I understand that the college will monitor the websites I visit and my use of the college's ICT facilities and systems • I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. • I will always use the college's ICT systems and internet responsibly.

- I understand that the college can discipline me if I do certain unacceptable things online, even if I'm not in college when I do them.
- I will use AI tools and generative chatbots (such as ChatGPT)
    - During assessments, including internal and external assessments, and coursework
    - To present AI-generated text or imagery as my own work

Please refer to the Student Positive Behaviour Policy for disciplinary information

Signed (student):	**Date:**

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

Acceptable use of the college's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the college's ICT facilities and accessing the internet in college, or outside college on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the college's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the college's network • Share my password with others or log in to the college's network using someone else's details • Share confidential information about the college, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the college	
I understand that the college will monitor the websites I visit and my use of the college's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside college, and keep all data securely stored in accordance with this policy and the college's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the college's ICT systems and internet responsibly and ensure that students in my care do so too. I have read and understood the contents of the college's ICT and Internet Acceptable Use Policy.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the 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 details) or encouraging them to visit a fake website.

TERM	DEFINITION
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.