ICT Acceptable Use Policy

Effective from	01/05/2022	Document number	3.8
Formal review cycle:	Annual		
Next formal review due	01/05/2023		
Policy owner:	Head of Information Technology		

Approval required

SMT Y/N	Y	SMT approved/review date	May 2022
Governor Y/N	N	Governor approved/review date	N/A

Publication

Website Y/N	Y	Intranet Y/N	Y	Student VLE Y/N	N	Date published	15.12.2022
Audience	Staff						
Area/s of Staff Intranet	Strategies, Policies and Procedures						

Changes made

Version	Author	Date	Section	Changes summary

Policy description:

The College seeks to promote and facilitate the proper and extensive use of Information and Communications Technology (ICT) for the sole purpose of supporting the teaching, learning, research and business activities of the College; and may be used for any legal activity that further the aims and policies of the College.

It is the responsibility of all users of the College's ICT resources to read and understand this policy. This policy may be updated from time to time, to comply with legal and policy requirements.

This Acceptable Use Policy is intended to provide a framework governing the use of all ICT resources across all sites on which the College operates. It should be interpreted such that it has the widest application and to include new and developing technologies and uses, which may not be explicitly referred to.

Links to other policies:

- *Social and Electronic Media Policy*
- *Data Protection Policy*
- *Staff Development Policy*
- *Health and Safety Policy*
- *Teaching Learning and Assessment Strategy*
- *Student Disciplinary Policy*
- *Staff Code of Conduct*
- *Disciplinary and Dismissal Procedures*
- *Prevent Strategy*

1. **Acceptable Use**

Acceptable use of Craven College's ICT resources is defined as their use in the purpose of supporting the teaching, learning, research and business activities of the College, and which does not come under the category of unacceptable use.

Examples of acceptable use include anything necessary in line with your duties as staff or course of study as a student in the College. For staff this would include, for example, administrative, teaching and research activities. For students, it would include assignment, study and research work.

Electronic messages such as email or teams chat must comply with acceptable use policy guidelines and should be re-read and checked before sending, to ensure no unintentional breach of policy.

The conduct of all users when using the College's ICT facilities should always be in line with the College behaviours, including the use of online and social networking platforms.

The use of your own personal devices on the College network to gain access to the internet will be subject to this acceptable use policy.

The user account holder is deemed responsible for misuse of the account.

2. Unacceptable Use

Unacceptable use of the Craven College's ICT resources is defined as:

- Contravention of applicable laws or regulations or College policies and procedures.
- Intentionally accessing, creating, storing or transmitting material which the College may deem to be offensive, inflammatory, indecent or obscene.
- Sending threatening, defamatory, abusive, obscene or otherwise offensive messages to cause needless annoyance, inconvenience, harassment or anxiety to anyone else.
- Using in a manner which interferes with those activities covered within the definition of acceptable use.
- Use for unauthorised personal commercial gain.
- Transmitting material that infringes the copyright of another person.
- Use for deliberate, unauthorised access to facilities or services accessible via the College's ICT resources.
- Use in any way which otherwise acts against the aims and purposes of the College, as specified in its governing documents, or in rules, regulations and policies/procedures adopted from time to time.
- Creation or transmission of material with the intent to defraud or which is likely to deceive a third party, or which advocates or promotes any unlawful act
- Unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others
- Unsolicited or bulk email (spam), forge addresses, or use mailing lists other than for legitimate purposes related to College's activities.
- Material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party.
- Material that brings the College into disrepute.
- Deliberate unauthorised access to networked facilities or services or attempts to circumvent College security systems.
- Pursuance of commercial activities for personal gain.

Deliberate activities having, with reasonable likelihood, any of the following characteristics:

- Wasting staff effort or time unnecessarily on ICT management.
- Corrupting or destroying other users' data.
- Damaging hardware or corrupting software.
- Violating the privacy of other users.
- Disrupting the work of other users.
- Denying service to other users (for example, by deliberate or reckless overloading of access links or switching equipment).
- Continuing to use an item of networking software or hardware after a request that use should cease because it is causing disruption to the correct functioning of the network.
- Other misuse of network resources, such as the introduction of computer viruses, malware, or other harmful software.
- Introduce data-interception, password-detecting or similar software or

devices to the College's Network.
- Using excessive network bandwidth, thus slowing the network for other users.

In cases where there is doubt about material that may be inappropriate, or where there is a legitimate educational reason for accessing it, the individual should seek advice and obtain the permission of a senior member of staff before accessing the material.

3. Other Permissible Use

Some limited 'private' use, outside of those times that should be devoted to work or study, is permissible. Such use must remain within the guidelines laid down in this policy and in the College's Social and Electronic Media Policy.

4. Relevant Laws and Regulations

The use of College ICT systems and resources are subject to the following statutes and regulations:

- The Copyright, Designs and Patents Act 1988
- Computer, Copyright Software Amendment Act 1985
- The Computer Misuse Act 1990
- The Data Protection Act 1998
- General Data Protection Regulation (GDPR) (EU) 2016/679
- The Electronic Communications Act 2000
- The Freedom of Information Act 2002
- The Regulation of Investigatory Powers Act 2000
- Trade Marks Act 1994
- Criminal Justice and Public Order Act 1994

Copies of these documents are available online at http://www.opsi.gov.uk/

The use of the College's ICT resources is subject to all relevant College regulations and Data Protection legislation. The College is linked to the Internet by the Joint Academic Network (JaNet) high-speed connection for all further and higher education colleges and universities. The College therefore complies with JaNet acceptable use guidelines.

This policy is available online at:
https://community.jisc.ac.uk/library/acceptable-use-policy

5. Prevention of Misuse

The College reserves the right to engage in systematic monitoring and / or filtering and has the necessary hardware and software available to implement this. When or where there is reason to believe that misuse is occurring, then monitoring and checking of records will take place.

The College's policy on the prevention of misuse is:

- To expect all staff and students to be aware of this Acceptable Use Policy.
- To educate staff and students in matters relating to acceptable use.
- To take swift and effective action within existing disciplinary and /

or legislative frameworks against anyone found to be misusing the College's ICT resources.

The College retains a right of access to all information held on College ICT resources, for the purposes of investigating misuse and reserves the right to inspect files, in order to ensure compliance with this and other policies.

6. Responsibility for College Devices

Users should treat College devices with care and not cause any form of damage to the College's ICT equipment or software, nor to any of the rooms and their facilities and services which contain that equipment or software. The term "damage" includes modifications to hardware or software which, whilst not permanently harming the hardware or software, incurs time and/or cost in restoring the system to its original state. Costs associated with repairing or replacing damaged equipment or software and/or in providing temporary replacements may be charged to the individual.

You must report any damaged, faulty, missing or broken ICT resources to the IT Team

7. Storing of Files

College preference is to store work-related files on One Drive. One Drive is a cloud-based file storage, synchronization and collaboration service offered through Microsoft Office 365 and managed by the IT 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 syncing 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 syncing with One Drive to the IT 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 IT Team reserves the right to terminate any anonymous links to files at any time.
- Documents and files stored within OneDrive remain your responsibility.

8. Monitoring of Usage

The College believes that the overwhelming majority of staff and students are responsible in their use of ICT resources and therefore does not wish to have to put disproportionate resources, especially of staff time, into monitoring activities.

Instead, the College will focus on retention of tracking and audit records and will pursue reports of misuse vigorously. Records are kept only for the purposes of investigating misuse, and are discarded after twelve months, unless a specific investigation is in progress.

Currently the College uses a firewall solution that is supported under a third-party managed service which alerts safeguarding and the ICT Team to potential misuse. This hardware solution is a preventative measure, as it can prevent access to undesirable websites, as well as a tracking method of access to items on the internet.

9. User Tracking

In all cases where there is the potential for the Craven College's ICT resources to be misused, arrangements are in place to record the identity of the individual using the specific facility at any given time. These records are retained for the purposes of investigating complaints of misuse. The records will be destroyed after twelve calendar months unless required in connection with a specific investigation.

Tracking is through the system of logging in, using a username and password. Prevention of misuse will be achieved by close supervision by College staff.

10. Web Filtering

The College employs a web filtering system that contributes to its tracking measures. This records website usage against the registered user account that is accessing the website, which will have been pre-classified into a specific category. The categories and website classifications are managed by a 3rd party organisation and are updated daily. The College can, without warning and when deemed necessary, add or remove categories from our filtering system.

Web filtering is in place and is designed to block access to categories such as, but not limited to:

- Adult/mature content
- Gambling
- Malicious websites
- File sharing
- Games
- Web chat or instant messaging

- Known other illegal or offensive websites
- Time-wasting activities.

Where sites are blocked in error, or where genuine access is required, then this should be notified to the ICT Team for unblocking (valid reasons and, where required, senior management authorisation must be given by the staff member concerned).

Staff and students should also alert the Information Technology Services Team of offensive and other undesirable sites to which access is available, despite the above-mentioned filtering.

11. Prevent Strategy

In March 2015 the Government introduced the Counter-Terrorism and Security Act 2015 which is an extension of earlier work published under the National Security Strategy and which identified terrorism as one of the four highest risks facing the country. This resulted in multi-Agency working across Craven, to which the College is a contributing member.

The implementation of the Prevent Duty can be a sensitive issue for students, staff and families. It needs to be emphasised that this is part of the safeguarding duty. This is not about spying on students or staff and it is not about stopping conversations about controversial issues. The Prevent Duty is intended to safeguard communities from exploitation and to support students in discussing and understanding complex and in some cases controversial issues.

The College will:

- Maintain robust systems and appropriate records to show compliance with responsibilities and provide reports when requested.
- Pay due regard to guidance and directives within inspection regimes.
- Ensure staff, students and visitors comply with relevant legislation and any statutory responsibilities associated with the delivery of education and safeguarding of learners.

12. Disciplinary Procedures

A member of staff or student will be subject to appropriate disciplinary action if they are believed to be abusing the College's ICT resources and systems.

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

- Restrict or terminate a User's right to use the College IT 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.

13. ICT Code of Practice

The following measures must be observed whilst using ICT in Craven College:

- Do not disclose your password to others. Your login is your responsibility, do not let others use it.
- Do not attempt to gain access to areas on the College network that you are not permitted to use. Hacking of the network is a serious offence, and such attempts will be dealt with appropriately.
- Using the network to attempt to gain information from other people's devices is also hacking and will be dealt with in the same manner.
- People who are in a timetabled class with their tutor, have priority over people wishing to use any spare computers.
- Always leave the room and your workstation area clean and tidy.
- Make sure your computer has been logged out before leaving.
- No food or drink allowed in IT rooms or around computers.
- You may use the software provided on College computers. Students are not to install or use other software on College computers.
- Copying of College software (software piracy) is against the law. Anyone found violating the law will be subject to the College's Disciplinary Procedure.
- Always use antivirus software on your removable devices.
- The data that you save is your responsibility. Always back up your files.
- Do not change software settings or configurations without permission.
- All ICT related problems must be reported to a member of the teaching staff or by contacting the ICT Service Desk team either by email to servicedesk@craven-college.ac.uk or by phone on: 01756 693839.