IT Policy

IT Acceptable Use Policy for Students

Date of document establishment	*25th September 2023*
Reference and Version number	*HRC IT Acceptable Use for Students Policy V1*
Author	*Head of IT*
Designated Owner	*Deputy Principal - Finance & Resources*
Approving body	*Board of Governors*
Date Approved	*25th September 2023*
Linked policies and procedures	▪ *CCTV Monitoring Procedure*
Date of next review	*25th September 2024*

1. Introduction

Students are responsible for their actions, conduct and behaviour whilst using Hertford Regional College IT resources in the same way that they are responsible during classes or at break time. Use of technology should be safe, responsible, and lawful and should not be used in anyway which could damage the reputation of HRC.

Hertford Regional College (HRC or the College) is committed to safeguarding and promoting the welfare of staff and students at the College. IT Services expect Students to conform to this policy as outlined below and will take appropriate action if evidence is provided to the contrary.

Any questions which arise from this policy should be directed to your tutor.

These regulations incorporate the acceptable use policy of our service provider, JISC (Joint Information Systems Committee), which manages network connections between Colleges and the Internet (the JANET Network). The full text of their policy can be found at: https://community.jisc.ac.uk/library/acceptable-use-policy

2. Definition of College IT Resources

College IT resources are all hardware, software, services, and equipment made available for staff and students which includes:

- Computer networks (wired or wireless)
- Computers (desktops and laptops)
- MFDs (All-in-one printer/scanner/copier)
- Mobile devices (mobile phones/tablets)
- Storage (on device/server/Cloud)
- Audio Visual systems (TVs/Smartboards/Digital Signage Players)
- All HRC applications and systems e.g. Moodle, ProSolution suite
- All account credentials provided to access HRC applications and systems
- Cloud services e.g. Office 365, Myday

3. What does this Policy Cover?

- The use of all IT resources provided by HRC
- All devices irrespective of ownership when connected to the HRC My Device Wi-Fi network which may be used by any member of HRC student
- This policy also applies to College and non-College owned equipment e.g. personal Laptops, home PCs when connected to the College network or systems, directly and/or via the VPN, for the duration that the equipment is using the College network or systems.

4. Acceptable Use of IT Resources

What constitutes authorised use?

- Any use associated with a programme of study or course for which a student is registered
- Reasonable personal use.

What does reasonable personal use mean?

Reasonable personal, social, or non-educational use of the internet and email is tolerated in LC's and other common areas subject to the availability of resources. Priority is given to students undertaking work as part of their studies.

- disrupt or distract the individual or other users from their programme of study or course (i.e. due to volume, frequency, time expended, or time of day used)
- involve accessing, downloading, storing, or sending offensive or inappropriate material or information, or is such as to amount to a criminal or civil offence
- restrict the use of those systems by other legitimate users
- risk bringing HRC into disrepute or placing HRC in a position of liability
- add significantly to running costs to the College
- breach the regulations set out by our internet provider, JANET

5. General Conditions of the IT Acceptable User Policy

By agreeing to this policy, a HRC student is expected to follow the conditions as outlined below and in the following sections. For the protection of all staff and

students, use of all College systems including e-mail and the Internet may be monitored by the College as outlined in the monitoring section of this document.

Students must:

- when using College IT resources, staff must comply with this Acceptable Use Policy, Jisc Acceptable Use Policy, and all relevant statutory and other provisions, regulations, rules, and codes of practice
- be aware that the College is not responsible for emails they send and will be required to pass on their details to a suitable authority if a complaint is received
- only access their own folders on the network or within Office 365 or Team folders which they have been given permission to
- use the appropriate methods of communication with staff, and external contacts as outlined in the section below
- leave computing areas tidy when they leave
- remember to log off every time they have finished using a shared computer
- if leaving a PC unattended for more than 20 seconds, lock it. To do this, press the Ctrl + Alt + Delete keys together then click 'lock this computer'
- If using a computer which does not require a log in (e.g. in an Internet Café), they must close all Internet browser* windows when finished using the computer
- take reasonable precautions to prevent the introduction of any virus, malware, worm, Trojan Horse or other harmful program to any computer, file, or software
- respect the copyright of all material and software made available by the College and third- parties and not use, download, copy, store or supply copyrighted materials including software and retrieved data other than with the permission of the copyright holder or under the terms of the licence held by the College
- establish the terms of the licence for any material and software which is used through any platform and must not breach such licences
- when holding data about living individuals, abide by the College's Data Protection Policy and General Data Protection Regulations, to process information (collect, use, share and dispose of) in accordance with the Principles of the data protection legislation
- Comply with the Computer Misuse Act of August 1990 which makes activities such as hacking or the deliberate introduction of viruses and other malware a criminal offence
- report any incidents or service requests in relation to IT resources or cyber security to their tutor or staff at one of the Learning Centres who will liaise with the IT Helpdesk
- be aware that all information assets created/owned/stored by the user on or connected to College IT resources may, in the instance of suspected wrongdoing, be subjected to inspection by College or by statutory authorities. Should the information be encrypted the decryption key must be provided.

Students must not:

- disclose or share College credentials e.g. password to others, or use accounts or passwords belonging to others, or access their files / emails, or destroy, copy, alter or move anyone else's files or otherwise to circumvent registration procedures
- share your logon with anyone as you will be liable for any misuse

- eat or drink in computer areas
- change any access rights to folders on computers or network areas
- click open emails from unknown sources and never click on links in emails
- use College resources to undertake any form of Cyber bullying including making abusive comments, sharing pictures, videos or personal information without the consent of the owner, creating or posting on websites to make fun or spread malicious rumours about someone or blackmailing individuals for any purpose
- download program files, including gaming software or media files (unless required to deliver courses) or install any software without permission from IT Services
- make copies of any software, music or video files downloaded from the Internet unless the owner has provided permission
- download illegal, offensive, or obscene material
- downloading or accessing materials that infringe personal liberties or promote extreme political views or radicalization
- create content or websites that are obscene, defamatory, infringe copyright, infringe personal liberties, or promote extreme political views or radicalization
- download any form of ‘virus’ software, the College provides and manages this
- send any offensive messages by email or social networks
- use material or programs in a way which is unlawful, defamatory, or invasive of another’s privacy
- add, engage in, or encourage conversations with students on social networking sites
- use the IT resources in such a way as to risk or to cause loss, damage or destruction of data or breaches of confidentiality of data
- use the IT resources in a way which infringes any patent, trademark, trade secret, copyright, moral right, confidential information, or other proprietary right of any third party
- jeopardise the provision of IT resources (for example by inappropriate use of bulk e-mail, or by recreational use that deprives other users of resources)
- publish, create, store, download, distribute or transmit material that is offensive, obscene, indecent, or unlawful. Such materials will always include, but at the College’s discretion may not be limited to, items deemed to be offensive, discriminatory, obscene, indecent, or unlawful
- forge email signatures and/or headers, initiate and/or forward 'chain' or 'junk' or 'harassing' emails, must not impersonate others in electronic communication and generate junk or offensive communications
- access or attempt to access IT resources at College or elsewhere for which permission has not been granted or facilitate such unauthorised access by others
- not use or produce materials or resources to facilitate unauthorised corruption, changes, malfunction, or access to any IT resources at the College or elsewhere, e.g. port scanning
- not display, store, receive or transmit images or text which could be considered offensive or which is likely to bring the College into disrepute, e.g. material of a pornographic, paedophilic, sexist, racist, libellous, threatening, defamatory, illegal, discriminatory, or terrorist nature
- use IT resources in a way that brings or could bring the College into disrepute. This includes associating HRC with external facilities such as Web sites that could bring the College into disrepute by association

- attempt to circumvent any firewall or software designed to protect any IT resources against harm
- interfere or attempt to interfere with or destroy systems or software set up on public facilities (this includes loading or attempting to load unauthorized software on to any College IT resources
- attempt to disrupt services. Hacking is defined here as the unauthorized access or modification of a computer system (locally or through a network), or the use of resources that have not been allocated, with intent to access, modify or damage another's files or system files, or to deny service to legitimate users, or to obtain or alter records, or to facilitate the commission of a crime
- Interfere with, disconnect, damage, or remove without authority any IT resources.

6. Communicating with Staff, and External Contacts

All college-related correspondence with Staff, and external contacts should be undertaken using IT resources.

Do use:

- College email address to correspond with students, or external contacts
- Teams meetings and channels
- Other collaboration tools should only be used with prior agreement from IT Services that Teams cannot provide the feature required or if the meeting is being held by an external contact for the benefit of staff and students

Do not use:

- Correspond with staff using their personal email address
- Use WhatsApp, Facebook, or other social media to communicate privately on a one-to-one basis with an individual member of staff.

7. Bring Your Own Device (BYOD)

Students are permitted to connect their personal devices; mobile phones, laptop or tablets to the HRC My Device network and will be allowed to connect to the internet for personal use and some key College systems such as Moodle and ProSolutions web applications as controlled by the College's firewall policies.

- Electronic equipment such as tablet computers, laptops, iPads etc. are brought onto College premises entirely at the risk of the staff member. Inappropriate use of such equipment will be dealt with in accordance with this policy
- Students may bring mobile telephones to College at their own risk and should be used respectfully and quietly at break-times and in free periods only. Mobile telephones should be set to silent mode during lesson times (at your tutor's discretion). Mobile phones may be used in LC's for any purpose other than voice calls, but headphones must be worn, if playing audio
- It is expected that any BYOD which is used for College work must be using a supported Operating system and regularly updated to make sure that all security patches have been applied
- BYODs are covered by this policy and all the same rules apply

- It is expected that the BYOD is protected by pin, password, or biometrics and if it is lost or stolen the College is informed so that IT Services can take appropriate action
- It is not permitted to connect active network devices such as network switches, hubs, wireless access points and routers to the College network. All IP addresses will be allocated and administered only by HRC.

8. Passwords and Encryption

Cyber security is a major concern for all businesses and managing password and user credentials can play a big part in protecting the College's IT resources and data. All staff are required to use MFA for access to their Office 365 account and regularly change their password when prompted.

Students should:

- use different passwords for each account
- be sure no one watches when you enter your password
- always log off or lock their computer if left unattended
- not tell anyone their password
- change your passwords periodically, and avoid reusing a password
- use strong passwords (at least 10 characters) which can include numbers, letters, and spaces
- use at least one capital letter and least one number
- not use words that might be easily guessed e.g. your pet's name, child's name, or month of birth

All College provided laptops have encryptions enabled which will protect the data which is stored on it in the event of theft. However, where possible, avoid storing sensitive data on the laptop as it is not backed up and will be lost if the laptop is stolen or broken.

Use the College provided OneDrive to store your college related files as much as possible or store files within your Class Notebooks and Teams.

9. Security and IT Equipment

Lost or Stolen Devices

What do if you lose your laptop, phone, or a college device?

- It is important that all students look after college equipment if they are provided with it, however, should something be stolen/lost it is vitally important to report this to your tutor or Learning Centre staff as soon as possible. This will ensure it is wiped, locked out and data/ information is not accessible.

Disposal Devices

- All IT devices must be disposed of though the colleges designated electrical disposal company. The company will provide a certificate to prove safe disposal. Computing equipment returned to lease companies must provide the same certification. Please return college equipment to the Learning Centre so that it can be dealt with appropriately.

Monitoring and handling misuse of IT resources
The college monitors its systems and networks.

- Computer systems may be monitored or recorded to secure effective system operation and for other lawful practices. For example, monitoring of user accounts might occur if the college has reason to believe that its IT resources were being misused to send unsolicited commercial e-mail
- The College reserves the right to check for insecure and vulnerable systems and to block access to systems and/or services (ports) which place at risk the integrity of its network or services, or which may pose a threat to third parties
- In the event of a suspected or actual information security incident or an unacceptable network event, the Head of IT Services may decide to take any action necessary to remedy the situation. This may include blocking access by users to systems and examination of any devices connected to the network
- The college does not monitor live video feeds from its CCTV however, it may refer to specific events if required. All requests for CCTV footage must be requested to Estates and conform to their CCTV policy
- In the event of suspected misuse of IT resources, user accounts maybe suspended and be inspected, monitored, files maybe accessed where necessary. The IT Services team may also disconnect network services, prevent access to the facilities without notice while investigations proceed
- Other than as per any applicable statutory obligation, the College will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of, or prevention of use of, any IT resource provided and/or managed by the College.

The Firewall and End Point protection software provided by the College will block or restrict access to any sites which are deemed inappropriate, including:

- Sexually explicit content
- Drug Abuse
- Explicit Violence
- Extremist Groups
- Illegal or Unethical activities
- Gambling
- Sports Hunting and War Games
- Weapons
- Peer-to-peer File Sharing
- Malicious Websites
- Phishing, SPAM URLs

All access to blocked sites is logged and authorised staff may investigate what sites staff or students have been accessing for example in the case of criminal investigation however, all requests must be raised formally through the IT Helpdesk and only provided if approved by Head of IT Services or Director of HR and Corporate Development for staff.

10. Procedures for accessing students accounts

On rare occasions it may be necessary to access a student's account for a business-critical or time-sensitive reason and the student is unavailable to provide access. All requests should be raised with the IT Helpdesk and they will request authorisation before allowing any access.

For student accounts the request should come from the Curriculum Area Manager or the Safeguarding team and must be approved by a Curriculum Director and the Head of IT Services.

11. Breach of policy

Breach of these conditions may lead to College disciplinary procedures being invoked, with penalties which could include suspension from the use of all College IT resources for extended periods and/or fines. Serious cases may lead to expulsion or dismissal from the College and may involve civil or criminal action being taken against the person.

All schools and colleges are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015 (the CTSA 2015), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism." This is known as the Prevent Duty.

The college seeks to protect its students against the messages of violent extremism including, but not restricted to, those linked to Islamic extremism, far right extremism, and extremist animal rights movements.

Behaviours and actions which are deemed to be of an extremist or radical nature will be dealt with in line with the College's safeguarding policy, available on the College website and on Staffnet.

12. College use of Students personal data

- Whilst the College takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data it cannot and does not give any warranties or undertakings to the user about security, confidentiality or integrity of data.
- Student's name, address, photograph, status, e-mail name, login name, alias, Student Identifier and other related information will be stored in computerised form for use for administrative and other purposes e.g. monitoring system usage and in line with the College's GDPR responsibilities.

13. Agreeing to this policy

- It is important that all students understand their responsibilities, if there is any uncertainty of what is permitted, discuss with your tutor, or speak to the Learning Centre staff
- When you log on to Moodle you are reminded that you agree to abide by the College's IT Code of Practice. Make sure that you have also read this and are aware of your responsibilities
- All students are expected to have read and confirmed acceptance of this policy as part of the enrolment process.