

IT Policy

IT Acceptable Use Policy

<i>Reference and Version number</i>	<i>IT Acceptable Use Policy V1.2025</i>
<i>Author</i>	<i>Head of IT</i>
<i>Designated Owner</i>	<i>Deputy Principal – Finance and Resources</i>
<i>Approving body</i>	<ul style="list-style-type: none"> • <i>Policy and Procedure Panel</i> • <i>Senior Leadership Team</i> • <i>Resources Committee</i>
<i>Date Approved including Impact Assessment</i>	<i>July 2025</i>
<i>Linked policies and procedures</i>	<ul style="list-style-type: none"> • <i>CCTV Monitoring Procedure</i> • <i>Safeguarding Children & Vulnerable Adults and Prevent Policy</i>
<i>Date of next review</i>	<i>July 2027</i>

1. Introduction

- 1.1 This IT Acceptable Use Policy (AUP) outlines the rules and guidelines for the appropriate use of Information Technology (IT) resources provided by Hertford Regional College (HRC). Its purpose is to ensure the integrity, security, and appropriate use of IT resources in support of teaching, learning, research, and administration. It is essential that all users understand and adhere to policy to ensure a secure and productive computing environment.
- 1.2 By accessing HRC IT systems or using any IT resources, users automatically agree to adhere to this policy.

2. Scope

The policy applies to:

- 2.1 **Users:** Members of the college and all other users (staff, students, visitors, contractors and others)
- 2.2 **Resources:** include, but are not limited to, any hardware, software, services, and equipment made available to users, such as:

- All account credentials provided to access HRC applications and systems
- All HRC applications and systems e.g. Moodle, ProSolution suite
- Cloud services, e.g. M365 (Emails, OneDrive), MyDay, etc.
- Storage (on device/server/Cloud)
- Computer networks (wired or wireless)
- Computers (desktops and laptops)
- MFDs (Multi-functional Device / All-in-one printer/scanner/copier)
- Mobile devices (mobile phones/tablets)
- Audio Visual systems (TVs/Smartboards/Digital Signage Players)
- Encourage and create a culture for all staff and students to be active participants in environmental initiatives.
- Improve the way the College manages its own environment.
- Work with the local community, public and private sector organisation's to improve the local environment and promote sustainable development.
- Integrate environmental and sustainability principles into the College's operational procedures and promote best practice at every level.
- Deliver measurable reductions in energy use and investing in energy saving technologies.
- Provide regular updates to staff and students
- The College will play its part in mitigating the impact of climate change

3 Roles and Responsibilities

- 3.1 **Security:** Protecting the organisation's IT infrastructure from security threats, including malware, unauthorised access, and data breaches.
- 3.2 **Compliance:** Ensuring that users comply with legal and regulatory requirements related to data protection, privacy, and industry standards.
- 3.3 **Operational Efficiency:** Promoting the efficient use of IT resources, ensuring that they are used for their intended purpose without unnecessary consumption or misuse.
- 3.4 **Ethical Use:** Encouraging responsible and ethical use of IT resources, fostering a work environment free from activities like cyberbullying, harassment, or illegal downloads.
- 3.5 **Protection of Reputation:** Safeguarding the organisation's public image by preventing misuse that could lead to reputational damage.

4 The College Environment

- 4.1 HRC students confirm acceptance of this AUP by enrolling with the College. Once a student enrolment is confirmed. Students are responsible for their actions, conduct, and behaviour when using Hertford Regional College's IT resources, just as they are during lessons or break times. Technology must be used in a safe, responsible, and lawful manner, and never in a way that could harm the reputation of HRC or conflict with its interests in any form.
- 4.2 HRC staff are responsible for familiarising themselves with this Policy. Staff are responsible for ensuring IT resources allocated to them or used by staff and students in the classroom, are stored securely and kept in a good state of repair. Staff should ensure equipment is adequately charged

and securely locked away when not in use. Damaged/ faulty equipment must be reported to the IT Support immediately including any incidents of equipment being deliberately damaged or defaced.

- 4.3 HRC is committed to safeguarding and promoting the welfare of its staff and students. IT Support expects staff and students to conform to this policy as outlined below and will take appropriate action through CPOMS for safeguarding issues or passed to curriculum department to follow college disciplinary procedure, Staff would be reported through management channels and HR if evidence is provided to the contrary.
- 4.4 Any questions which arise from this policy should be directed to the Head of IT via email.
- 4.5 This policy complies with the Joint Academic Network ([JANET](#)) Acceptable Use policy, JANET provide high-speed internet access and other networking services to the UK's research and education community

5 User Login, Password and Encryption

- 5.1 All users who require access to the College Network must have a valid user login and password and are required to set up Multi-Factor Authentication (MFA).
- 5.2 Users must adhere to the following:
- Do not attempt to gain unauthorised access to College IT systems.
 - Passwords must never be written down or disclosed to another individual or organisation.
 - Do not use passwords which are easily guessed e.g, Password 123
 - Passwords must be strong including upper- and lower-case letters, numbers, symbols.
 - Always ensure that you log off or lock your computer whenever it is left unattended.
 - Where applicable, change your passwords regularly and avoid reusing the same password.
- 5.3 All HRC-provided laptops have encryption enabled to protect stored data in the event of theft, but where possible, sensitive data should be avoided on the laptop as it is not backed up and may be lost if stolen or damaged; instead, use the HRC-provided OneDrive or store files within Class Notebooks and Teams for College-related documents

6 Respect for Privacy

- 6.1 HRC users are expected to respect the privacy of others and not attempt to access or disclose personal or confidential information without proper authorisation. Use of HRC IT resources for harassment, bullying, or any form of malicious intent towards others is strictly prohibited. Additionally, HRC users must not share any confidential information belonging to the College.

7 Copyright and Intellectual Property

- 7.1 HRC users must respect copyright laws and intellectual property rights. Unauthorised distribution or sharing of copyrighted materials is not allowed. Software installation and use must comply with license agreements.

8 Communication Tools

- 8.1 Communication tools such as Teams, Outlook email, and telephone should be used for college-related communication. Users must not engage in spamming or any form of email or online abuse. HRC accounts must not be used for personal commercial activities or any other non-educational purposes.
- 8.2 Other collaboration tools such as Zoom may only be used with prior agreement from IT Services, and only if Teams cannot provide the required features or if the meeting is being organised by an external contact for the benefit of staff and students.
- 8.3 Do Not Use:
Personal email addresses, WhatsApp, Facebook, or other social media should not be shared to communicate privately on a one-to-one basis between staff and students.

9 Prevent

- 9.1 Under HRC's Prevent Duty, users access our systems with the clear understanding that they will not engage in any activities that contravene prevailing legislation, particularly the Terrorism Act (2006), which prohibits the online posting of material that encourages or endorses terrorist acts, including those committed in the past. The Act also establishes the potential for prosecution for those transmitting such material, including via electronic means. Visits to websites related to terrorism or the downloading of materials from such groups—regardless of whether the sites are open access—will be monitored by HRC and reported to the appropriate authorities.

10 Safeguarding and Online Safety

- 10.1 HRC is committed to fulfilling its safeguarding responsibilities in line with UK legislation and guidance, including *Keeping Children Safe in Education (KCSIE)*. All users of the College's IT systems and networks must comply with these safeguarding standards.
- 10.2 **Key Safeguarding Measures:**
- Monitoring and Filtering: All activity on the College's network is monitored and filtered in accordance with statutory safeguarding requirements. The following categories of websites are blocked to protect users from harmful, inappropriate, or illegal content:
 - Sexually explicit content
 - Drug abuse
 - Explicit violence
 - Extremist groups or radicalisation material
 - Illegal or unethical activities
 - Gambling
 - Sports hunting and war games
 - Weapons and weapon-related content
 - Peer-to-peer file sharing
 - Malicious websites
 - Phishing or SPAM-related URLs

All access attempts to blocked sites are logged. Authorised staff may investigate user activity, such as website access history, in the context of safeguarding concerns, disciplinary matters, or criminal investigations. However, any such requests must be formally submitted via the IT Helpdesk and will

only be actioned with approval from the Head of IT Services. In cases involving staff, access will only be granted with approval from the Director of HR and Corporate Development.

- 10.3 **Appropriate Use:** Users must not use HRC systems or personal devices on campus to access, store, or distribute material that is illegal, offensive, or harmful. This includes cyberbullying, extremist content, and any material that could cause harm or distress to others.
- 10.4 **Reporting Concerns:** Any safeguarding concerns—including inappropriate online behaviour, grooming attempts, or exposure to harmful content—must be reported immediately to a Designated Safeguarding Lead (DSL) in person or via their email safeguardingteam@hrc.ac.uk or directly any member of staff, anonymous reporting can be achieved through Whisper by texting HRC1 along with your message to 07860021323.
- 10.5 **Use of bring your own devices (BYOD):** Personally owned devices connected to the College network must also adhere to safeguarding expectations. The College reserves the right to restrict or monitor device use if there are concerns around safety or welfare.
- 10.6 **Staff Responsibilities:** Staff must model appropriate digital behaviour and are expected to guide students in the safe and responsible use of technology. They must also complete mandatory safeguarding and online safety training.

11 Data Protection and GDPR

- 11.1 HRC is committed to handling personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This includes ensuring the lawful, fair, and transparent processing of data, and safeguarding the rights and freedoms of individuals whose data is held or processed by the College.
- 11.2 While HRC implements appropriate technical and organisational measures to protect personal and other sensitive data against unauthorised access, alteration, disclosure, destruction, or accidental loss, it cannot and does not guarantee the absolute security, confidentiality, or integrity of such data. Users are reminded to exercise caution when handling or transmitting personal data via HRC systems.
- 11.3 Personal data—including students' names, addresses, photographs, status, email addresses, login credentials (e.g. username, alias), student identifiers, and related information—may be stored electronically. This data is used for administrative purposes, monitoring system usage, safeguarding, and for providing educational services, all in compliance with HRC's legal obligations under UK GDPR.
- 11.4 All users of HRC IT systems must ensure that any personal data they access, store, or transmit is handled lawfully and securely, and only for legitimate College-related purposes. Users must not share or disclose personal data unless authorised to do so and must report any data breaches or suspected breaches to the College's Data Protection Officer (DPO) immediately.
- 11.5 Access to personal data is restricted to authorised staff and is granted strictly on a need-to-know basis. Monitoring of system usage may occur where necessary for safeguarding, legal compliance, or policy enforcement. All monitoring is carried out in accordance with UK GDPR and College policy.

- 11.6 Students and staff have the right to access their personal data held by HRC and may request correction or deletion where appropriate. Requests should be made formally to the Data Protection Officer in accordance with HRC's Data Subject Rights procedures.

12 Bring Your Own Device (BYOD)

- 12.1 HRC does not officially support the use of personal devices (BYOD) to access HRC systems, applications, or data. While individuals may choose to use their own devices on campus, they do so entirely at their own risk and responsibility.
- 12.2 Personal devices—including mobile phones, laptops, and tablets—may connect to the internet via the HRC My Device Wi-Fi network. This connection allows access to the internet and to selected published HRC systems such as Moodle and ProSolutions, in accordance with the College's firewall and security protocols.
- 12.3 All personally owned electronic devices (e.g., tablets, laptops, iPads) brought onto HRC premises remain the sole responsibility of their owners. HRC accepts no liability for any loss, theft, or damage. Any misuse of such devices will be dealt with under the terms of this policy.
- 12.4 Students may bring mobile phones to HRC at their own risk. Phones must be used respectfully—restricted to break times or free periods—and set to silent mode during lessons unless the tutor grants permission. Within Technology Centres (TCs), mobile phones may be used for non-verbal purposes; however, headphones must be used when playing audio.
- 12.5 All personal devices used on campus are subject to the same rules and expectations as HRC-issued equipment and are covered by this policy.
- 12.6 Personal devices must be secured using a PIN, password, or biometric authentication. If a device is lost or stolen, it must be reported to the College without delay so that IT Services can take appropriate action.
- 12.7 It is strictly prohibited to connect any active networking hardware—such as network switches, hubs, wireless access points, or routers—to the HRC network. All IP address assignments are exclusively managed by HRC.
- 12.8 HRC reserves the right to monitor any activity conducted while connected to the HRC network or access any HRC resources, including internet usage, to ensure compliance with its IT and safeguarding policies.

13 General Conditions of the IT Acceptable User Policy

Use of IT resources for illegal activities, including but not limited to hacking, unauthorised access, or distribution of malicious software, is strictly prohibited. Examples of common activities that users must/must not undertake include the following (please note, this is not an exhaustive list):

13.1 **Students, Staff and visitors must:**

- adhere to this Acceptable Use Policy, the Jisc Acceptable Use Policy, and all relevant laws, regulations, and codes of practice when using HRC IT resources.
- use the HRC's IT resources (computers, software, networks, etc.) exclusively for academic purposes, research, or any other activities explicitly authorised by the College.
- immediately report any security concerns, such as phishing attempts, malware, or suspicious activity, to the Tech centre.
- use the HRC's network resources (e.g. internet access, email, internal systems) responsibly and avoid activities that might overload or damage the network, such as excessive downloading or hosting illegal content.
- maintain professionalism when communicating online or collaborating via digital platforms, treating others with respect and adhering to the HRC's conduct standards.
- use HRC email accounts for academic and professional communication and refrain from sending unsolicited or inappropriate messages (spam, offensive content, etc.).
- be aware that the HRC is not responsible for any emails sent by users, and their details may be passed to the appropriate authority if a complaint is received.
- only access their own folders on the network or within Office 365 or Team folders to which they have been granted permission.
- use the appropriate methods of communication with staff, and external contacts as outlined in the section below
- leave computing areas clean and tidy when finished.
- always remember to log off after using a shared computer.
- if leaving a PC unattended, it must be locked. To do this, press Ctrl + Alt + Delete and select 'Lock this computer', or press Windows + L to prevent unauthorised access.
- avoid using shared personal/ public devices to access HRC resources. If this is necessary, ensure the device complies with HRC security policies. Once finished using, sign out fully, close all browser windows, and ensure no passwords or HRC data are saved. Failure to comply, resulting in the compromise of HRC resources, may lead to restricted access and appropriate action being taken, depending on the circumstances.
- it is the responsibility of the user to ensure that the operating system (OS) on any personal device used to access organisational data is kept up to date with the latest security patches and updates. Failure to maintain an updated OS may result in a compromised security posture, and as such, the user may be restricted from accessing organisational systems and data.
- must be aware that in the event a personal device accessing HRC resources is found to be outdated or insecure due to failure to maintain an updated OS, HRC reserves the right to deny access to its systems and data. Additionally, any organisational data stored on such devices may be remotely wiped without prior notice to ensure the protection of sensitive information.
- 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
- when processing personal data, users must comply with the HRC College's Data Protection Policy and the General Data Protection Regulation (GDPR), ensuring that all data is processed (collected, used, shared, and disposed of) in full accordance with the principles set out in 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.

13.2 **Students, Staff and visitors must not:**

- share their login credentials, passwords, or any access keys with others, even if requested by peers or colleagues.
- access or share any confidential or sensitive information (including personal data or proprietary information) without proper authorisation or a legitimate academic need.
- must not install or use software on HRC devices or networks that have not been authorised by the IT department. This includes pirated software, personal applications, or any software that may compromise security
- attempt to access College IT resources or systems after their account has been revoked, suspended, or expired, or when they no longer have permission to use the system.
- engage in any activities that may harm or disrupt IT systems, such as introducing malware, viruses, or other harmful code, or using College IT resources to attack other systems (e.g., DoS attacks).
- attempt to bypass or disable any security controls, such as firewalls, antivirus software, permissions or filtering systems, put in place by the College to protect its IT systems and data.
- send or open unsolicited emails (spam) or engage in phishing attempts designed to deceive others into revealing sensitive information such as passwords, bank details, or personal data.
- eat or drink in computer areas to prevent damage to equipment and maintain a clean, safe environment.
- use HRC IT resources to engage in cyberbullying, including making abusive comments, sharing personal information or media without consent, posting content to harass or defame others, or engaging in blackmail. Any form of harassment, cyberbullying, or discriminatory behaviour against students, staff, or others associated with the College is strictly prohibited.
- 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
- 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

- introduce data-interception, password-detecting or similar software or devices to the network.
- attach USB drives or removable devices to any HRC resources without first scanning them to ensure they are free from malware and safe to use.
- engage in the creation or transmission of material designed or likely to cause annoyance, inconvenience, or needless anxiety.
- download, copy, or transmit the works of others to third parties without their permission. Written material, images, and software are protected by copyright laws.
- transmit unsolicited commercial material (spam or similar).
- place any material on the internet that incites, encourages, or enables others to gain unauthorised access to the HRC's systems.
- remove equipment from its location without authorisation.

14 Monitoring

14.1 HRC reserves the right, without notice, to access, listen to or read any communication you make or receive using HRC facilities. It will only do this for the following purposes:

- to establish the existence of facts
- to ascertain compliance with regulatory or self-regulatory practices and procedures
- to investigate or detect unauthorised use of systems.
- to prevent or detect crime.
- to provide practical help to prevent people from being drawn into terrorism and violent extremism.
- to intercept for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding e mails to correct destinations.
- to check electronic communications systems when you are on holiday or on sick leave

14.2 Monitoring will only be undertaken by authorised personnel who understand the College's obligations under prevailing Data Protection Regulations.

15 Artificial Intelligence (AI)

15.1 Artificial Intelligence (AI) encompasses technologies and techniques that enable computers to perform tasks that typically require human intelligence. These tasks include problem-solving, understanding natural language, recognising patterns, learning from experience, and adapting to changing circumstances. When using AI tools, the user must ensure they maintain ethical research and development, privacy, security, and lawful responsibilities. The following activities involving AI systems are strictly prohibited:

- Engaging in activities that compromise the security or integrity of AI systems.
- Using AI to perpetrate fraud, deception, or other forms of malicious behaviour.
- Discriminatory or biased use of AI that may harm individuals or communities.
- Creating or disseminating harmful content generated by AI, including deepfakes or misinformation. The College will regularly monitor and evaluate the performance and impact of AI systems to identify and address any issues that may arise over time.

16 Policy Compliance

- 16.1 Any misuse of IT facilities or breaches of this policy will be reported to the Head of IT, failure to adhere to this policy may result in formal action under the college's prevailing procedures, including access restrictions, and could lead to further legal consequences if security breaches occur due to noncompliance. If the misuse breaches current law or is reportable under relevant legislation the College reserves the right to inform the police or relevant authority.

17 Evaluation and Review

- 17.1 The effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.