Hereford College of Arts

IT ACCEPTABLE USE POLICY

Document Control	
Manager responsible	Tina Tupper, ILT Manager
Version number	4.0
Approved by	SLT
Approval date	07 October 2020
Review date	October 2021

IT ACCEPTABLE USE POLICY

Contents

1. PURPOSE

This policy provides a framework for the use of IT facilities (hardware, software, data, network access, third party services, online services and IT credentials) provided or arranged by Hereford College of Arts. This framework applies to anyone using the HCA IT facilities. It should be interpreted in the widest application, and takes into consideration the JANET Acceptable Use Policy.

2. GENERAL PRINCIPLES

- The privacy of others should be respected. Systems, data or passwords belonging to other users should not be sought out, intentionally copied, or modified. Another user's ID and Password should **not** be used.

- User ID and Passwords must not be divulged to anyone. Individuals are solely responsible for the security of their User ID and Password.

- The unauthorised copying of software is a violation of the College's Security Policy and the software copyright law.

- It is important that the College networks are free from viruses. The installation of unauthorised software and the downloading of unauthorised files is prohibited.

- Email is for communicating college information in a professional manner. The composition and sending of email must show the same respect and concern for others as exhibited in normal written correspondence.

3. ACTIONS AND RESPONSIBILITES

3.1 Internet

Students are offered access to the internet as part of the college's courses. Use of the internet enables students to access libraries, databases, bulletin boards and exchange messages with other Internet users. control and The aim of the college in offering access to the internet is to further educational goals. Staff and students should be aware that use of the internet is monitored by the College. The College will not permit the following activities:

- The creation, display, storage, production or transmission of offensive material
- Intrusion of privacy or theft of intellectual property which causes breaches of confidentiality
- Dissemination of unsolicited and unwanted, and possibly offensive and/or illegal material
- Destruction of information and/or temporary disabling of remote systems
- Misuse of the publicly funded resource for purposes which do not benefit the community and may be illegal in themselves
- The subscription to any services not authorised by the College
- Any breach off data protection legislation.
- Creation or transmission of material with the intent to defraud.
- Violating the privacy of other users

- The downloading of unauthorised files
- The use of any social online chat facility (e.g. social networking & dating sites) other than that providing a support service or within the HCA Network facility.
- The use of online gaming facilities other than those approved by the curriculum.
- The setting up of 3rd party E-Mail facilities on college equipment without prior authorisation

3.2 Email

Email is provided to enable College wide communications and world-wide communications via the Internet.

In using Email, the same values and principles should be applied as to other forms of communications on behalf of the College. It should not contain anything that you would not put in any other form of written communication.

The College will not permit the following use of the Internet and Email:

- Forgery (or attempted forgery) of Email messages.
- Reading, deleting, copying or modifying the Email of other users.
- The sending of harassing, obscene, or other threatening Emails.
- The sending of unsolicited junk mail or chain letters.
- Sending, displaying or downloading of offensive messages or pictures
- Using obscene language
- Violating copyright laws
- Excessive use of college email for purposes that are not directly related to college business.
- Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.
- Content considered a data protection risk.
- Other actions which may bring the Colleges name into disrepute

3.3 Internet Access

Freedom of network use entails that users accept a general duty of care to take all proper precautions to prevent misuse. Misuse of the college Network, VLE & website may have serious implications for other sites, and have financial implications for the College.

Use is regarded as a College service and may be withdrawn if abused or as part of a disciplinary procedure.

Students will only be given Internet access on acceptance of the IT Acceptable Use Policy and E-Safety Policy.

3.4 Wi-Fi

Students, Associate Members, and Staff are permitted to use the College Wi-Fi (EDUROAM) in order to access the Internet from personal Electronic Devices e.g. laptops.
Devices are only permitted to be connected to College electrical sockets after completion of the College PAT Test. The same restrictions as above apply for Internet usage. Individuals connect devices to HCA Wi-Fi and electrical sockets at their own risk and the College Accepts no responsibility for any damage that may happen as a result.

Only pre-configured devices owned by the college are allowed to connect to the Wi-Fi via HCAWap.

3.5 Restriction of Access

Individuals are solely responsible for the security of their User ID and Password, an individual's User ID and Password must not be divulged to anyone else. This applies to all computing facilities provided by any department of the College and should be read in conjunction with the HCA IT Security Policy. A serious breach of this policy may lead to disciplinary action. Individuals are not permitted to connect their personal devices to the Network using Network access points without Authorisation.

The Internet may not be used for any of the following:

- The accessing, creation or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
- The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- The creation or transmission of defamatory material or personal information
- The transmission of material such that this infringes the copyright of another person
- The transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks e.g. the sending of junk mail or other advertising material over the web
- Deliberate unauthorised access to facilities or services accessible via the Internet e.g. Trying to get into systems and files by "hacking"
- Using the Internet to incite racial hatred, radicalisation and/or acts of terrorism
- Accessing unsuitable material that may be in breach of the law and the college Safeguarding and Prevent Policy

Deliberate activities with any of the following characteristics:

- wasting staff effort or networked resources, including time on end systems accessible via the internet and the effort of staff involved in the support of those systems

- corrupting or destroying other users' data
- violating the privacy of other users
- disrupting the work of other users
- using the internet in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment)
- deliberately bypassing the proxy servers
- deliberately finding ways and means of avoiding the monitoring systems
- continuing to use an item of networking software or hardware after the college has requested that use cease because it is causing disruption to the correct functioning of the Internet
- other misuse of the Internet or networked resources, such as the introduction of viruses
- excessive use of college internet access for purposes that are not directly related to college business e.g. Facebook, Ebay, running a private business or online shopping
- Where the Internet is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the Internet

3.6 BYOD (Bring Your Own Device)

Staff and students are permitted to utilise their own mobile devices within the college. The devices must only connect using the Eduroam Wi-Fi provided logging on with the credentials given to individuals during the induction process.

Personal devices should not under any circumstance be connected directly to the HCA Network via cable to Network ports.

Staff and students must take full responsibility for the care of their devices and ensure that personal insurance policies cover the use of the device within the college campus.

Although every effort is made to support the wide variety of operating systems devices may use, the college is unable to guarantee connection of the device to the Wi-Fi facility.

IT staff are not able to support staff or students with any technical issues they may have with their personal devices. Individuals are advised to contact the vendor for after sales service.

4. Prevent Duty

This policy supports the College's statutory duty under the prevent guidance. Students and staff are not allowed to use the College IT facilities to incite racial hatred, radicalisation and/or acts of terrorism. As part of that duty the College has blocked access to websites that support and promote intolerance, hate, militancy and extremism. Please refer to the College's e-safety policy.

5. POLICY SUPERVISION

Any suspected breach of this policy should be reported to the ILT Manager who will instigate appropriate action. The ILT Manager will also take action when infringements or abuses are detected in the course of their normal duties.

6. SUMMARY

This policy will be reviewed annually by the ILT Manager, or sooner if there is a change in legislation or the college environment. SLT will review and approve the policy.

Any person found breaching the Acceptable Use Policy may be prohibited from using the network and may be subject to the college's disciplinary procedures. Certain activities made by persons not complying may lead to suspension or dismissal.