Acceptable Use Policy

Document Control Table	
Manager Responsible	Operations Manager
Version number	1
Approved by	Senior Leadership Team
Approval date	October 2023
Review date	October 2026

1 Purpose

1.1 Hereford College of Arts ('the College') depends heavily on its Information Technology (IT) services for its teaching and administrative activities. These services are funded on condition they are used for legitimate, authorised purposes, and the College may be required from time to time to demonstrate to external auditing bodies that it has mechanisms in place to manage, regulate and control them. The main purpose of these regulations is to define what constitutes acceptable use which is:

1.1.1 To encourage the responsible use of facilities

1.1.2 To maximise the availability of resources (equipment, infrastructure and staff) for legitimate purposes

1.1.3 To minimize the risk of misuse from inside or outside College.

1.2 This Policy incorporate the Acceptable Use Policy of our service provider, Joint Information Systems Committee (JISC), which manages network connections between Universities and Colleges and the Internet. Their policy can be found at: https://community.jisc.ac.uk/library/acceptable-use-policy. There are also various national and European Union laws and directives that govern the use of IT, and others that make explicit reference to IT.

1.3 The College has a duty to bring these to the attention of its staff and students. If you are not sure whether something you are planning to do might contravene these regulations, check first with your Line Manager (in the case of staff) or Tutor (in the case of students), before proceeding. Advice is also available from the IT Helpdesk.

1.4 This Policy should be read in conjunction with other College Information Technology

Policies and its use, these are available on

1.5 **Scope –** This Policy covers the use of all IT services and facilities provided by the College or by third parties on behalf of the College. For the purposes of clarification, these include, but are not limited to:

1.5.1 All devices irrespective of ownership when connected to the College network.
1.5.2 All Services run by the College's IT Department.
1.5.3 Any application that runs over the College network.
1.5.4 Facilities and systems operated by Departments for academic research, teaching and administration.
1.5.5 Content hosted on the College's IT systems which are accessible via the internet by members of the public.
1.5.6 Services operated by third parties.
1.5.7 Software obtained under an educational licence agreement may also be subject to the terms of this Policy.

2 Authorised Use and Personal Use

2.1 In this Policy "authorised use" is defined as:

2.1.1 For students use properly associated with the College programme of study or course for which a student is registered and reasonable personal use.
2.1.2 For employees, use in the course of or properly and directly associated with their employment and reasonable personal use.
2.1.3 For users who are neither staff nor students, use is restricted to those purposes specified in the case made for registration.

2.2 In this Policy "Reasonable personal use" is defined as:

2.2.1 Incidental and occasional use which does not disrupt or distract the individual from the efficient conduct of College business. (i.e. due to volume, frequency, time expended or time of day used)

2.3 Any use that falls outside of the definitions for acceptable use or personal use is prohibited and may lead to the College's disciplinary procedures being invoked, with penalties that could include suspension from the use of all College computing facilities for extended periods. Serious cases may lead to disciplinary action, up to and including dismissal without notice and may expose you to court proceedings attracting both criminal and civil liability.

2.4 You will be held responsible for any claims brought against the College and any legal action to which the College is, or might be, exposed as a result of your unauthorised use.

3 Regulations and Policy

3.1 **IT users MUST**:

3.1.1 Respect the copyright of all materials and software that are made available by College service providers and third parties for authorised use.
3.1.2 Familiarise themselves with and comply with the requirements of the Data Protection Act 2018 and College Policy, most especially the obligation to notify the College's Data Protection Officer (DPO) of any relevant data holdings.
3.1.3 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. Hacking is defined as the unauthorised 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.

3.1.4 Have the written approval of their Head of Department where activities which might be subject to legislation are carried out in pursuit of legitimate, approved academic research (for example, work involving the use of images which may be considered obscene or indecent, or research into computer intrusion techniques)

3.1.5 Take all reasonable precautions to prevent the introduction of any virus, worm, trojan horse or other harmful program to any computer, file or software.

3.1.6 Only download data or datasets where they are explicitly permitted to do so. All users must abide by:-

3.1.6.1 The User Acknowledgement of Third Party Rights - http://www.eduserv.org.uk/services/Chest-Agreements/about-our-licences/userobligations,

3.1.6.2 The terms and conditions of JISC Model Licenses - (http://www.jisccollections.ac.uk/Help-and-information/How-Model-Licences-work/Guide-toModel-Licence/,

3.1.6.3 Copyright Law (Copyright, Designs and Patents Act 1988)

3.1.6.4 Any specific conditions of use imposed by the owners or suppliers of software or data. In particular users should be aware that, unless otherwise stated, software and datasets provided by College should only be used for College educational purposes.

3.2 **IT users MUST NOT**:

3.2.1 Use material or programs in a way which is unlawful, defamatory or invasive of another's privacy.

3.2.2 Use the IT services and facilities in such a way as to risk or to cause loss, damage or destruction of data or breaches of confidentiality of data.

3.2.3 Use the IT services and facilities in a way which infringes any patent, trademark, trade secret, copyright, moral right, confidential information or other proprietary right of any third party.

3.2.4 Users must not make, run or use unlicensed copies of software or data.

3.2.5 Put at risk the provision of services (for example by inappropriate use of bulk e-mail, or by recreational use that deprives other users of resources).

3.2.6 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, obscene, indecent or unlawful under the following Acts and Regulations:-

3.2.6.1 The Obscene Publications Act 1959.

3.2.6.2 The Sex Discrimination Act 1975.

3.2.6.3 The Race Relations Act 1976.

3.2.6.4 Disability Discrimination Act 1995.

3.2.6.5 Part-Time Workers (Prevention of Less Favourable Treatment)

Regulations 2000.

3.2.6.6 Fixed-Term Employees (Prevention of Less Favourable Treatment) Regulations 2002.

3.2.6.7 Employment Equality (Sexual Orientation) Regulations 2003.

3.2.6.8 Employment Equality (Religion or Belief) Regulations 2003.

3.2.6.9 Harassment Act 1997.

3.2.6.10 Employment Equality (Age) Regulations 2006.

3.2.6.11 The Protection of Children Act 1978.

3.2.6.12 The Public Order Act 1986.

3.2.6.13 The Criminal Justice and Public Order Act 1994.

3.2.6.14 Terrorism Act 2006.

3.2.6.15 The Counter Terrorism and Security Act 2015.

3.2.7 Use IT facilities in a way that brings or could bring College into disrepute. This includes associating College with external facilities such as Web sites that could bring the College into disrepute by association, for example by embedding College email addresses in such sites, or by providing hyperlinks from the College web sites to such sites.

3.2.8 Disclose or share credentials e.g. a password to others, or use accounts or passwords belonging to others, or otherwise to circumvent registration procedures. The term “password” is taken to refer to any authentication credential issued by College, and includes both hardware tokens and cryptographic keys. Users will be held personally liable and may be subject to disciplinary proceedings for any misuse of their user account resulting from the disclosure of passwords to others.

3.2.9 Access or attempt to access any data processing systems or services at the College or elsewhere for which permission has not been granted, or facilitate such unauthorised access by others.

3.2.10 Attempt to circumvent any firewall or software designed to protect systems against harm.

3.2.11 Interfere or attempt to interfere with or destroy systems or software set up on public facilities (this includes loading or attempting to load unauthorised software on to any College IT facilities).

3.2.12 Interfere with, disconnect, damage or remove without authority any equipment made available for use in conjunction with any College IT facilities.

3.2.13 Set up equipment to provide services that they are not competent to administer, especially if such services result in security vulnerability or exposure to misuse.

3.3 The College does not tolerate discrimination or harassment in any form whatsoever. This principle extends to any information distributed via any College IT system or via the Internet. You may not store on or transmit from any system any material which discriminates or encourages discrimination or harassment on racial or ethnic grounds or on grounds of gender, sexual orientation, marital status, age, ethnic origin, colour, nationality, race, religion, belief or disability. Breaches of this policy will lead to disciplinary action.

3.4 In the event that you receive or become aware of obscene, indecent, offensive, inflammatory, discriminatory or socially offensive material, you should notify the relevant person set out in paragraph 5.2.

3.5 Failure to comply with these regulations may lead to disciplinary action, up to and including dismissal from the College without notice and may expose you to court proceedings attracting both criminal and civil liability.

3.6 You will be held responsible for any claims brought against College and any legal action to which College is, or might be, exposed as a result of your unauthorised use.

4 Conditions of Use

4.1 Use of College IT facilities is subject to the following conditions. Additional conditions may apply to locally managed systems it is the responsibility of those managing such systems to make their users aware of any local regulations.

4.1.1 The facilities (including software) are provided entirely at the risk of the user. The College will not be liable for loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), damage (including damage to hardware, software or data) or inconvenience arising directly or indirectly from the use of the facilities, except where statutory health or safety matters are involved.

4.1.2 Whilst the College's Information Security Policy requires providers of computing facilities to employ appropriate security measures to prevent unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data, the College cannot and does not give any warranties or undertakings to the user about security, confidentiality or integrity of data, personal or other. The same applies to any other electronic material submitted to or processed on facilities provided or managed by College or otherwise deposited at or left on its premises.

4.1.3 The College accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or the invalidation of any warranty agreement) to equipment not owned by College as a consequence of any work carried out on such equipment by members of staff (or students acting in the capacity of members of staff), whether authorised or not.

4.1.4 The College accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or invalidation of any warranty agreement) to equipment not owned by College as a consequence of direct or indirect connection, whether authorised or not, to College networks. The user shall indemnify College for any loss or damage, whether direct or indirect, malicious or inadvertent, suffered or incurred as a consequence of the interconnection of any hardware or software not owned by or under the control of College with any IT system, hardware, software or data owned or controlled by College.

4.1.5 The College reserves the right to inspect, monitor, copy and/or remove user data in order to investigate operational problems or for the detection and investigation of suspected misuse. This includes the authorised interception and monitoring of communications as provided for by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under the Regulation of Investigatory Powers Act 2000.

4.1.6 Any monitoring of systems or networks may be carried out only in accordance with the College Policy on Monitoring Computer and Network Use. For the avoidance of doubt, this does not preclude third parties who operate services on behalf of College from carrying out lawful monitoring and disclosure on their systems and networks. It is important to be aware that communications on or through College's 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 College has reason to believe that its computer facilities were being misused to send unsolicited commercial e-mail.

4.1.7 The College reserves the right to check for insecure and vulnerable systems and to block access to systems and /or services which place at risk the integrity of its network or services, or which may pose a threat to third parties.

4.1.8 The College reserves the right to disconnect poorly managed equipment from the departmental local area network (LAN), or in extreme cases disconnect the departmental LAN from the College network until the offending machine is disconnected or shown to be configured correctly.

4.1.9 Any form of electronic communication may be construed in law as a publication and College publishing guidelines will apply. Users must be aware of the implications with respect to Intellectual Property Rights of publishing information in any electronic form

5 Procedures for Dealing with Misuse or suspected Security Violations

5.1 In the event of suspected misuse of IT facilities the College reserves the right to suspend user accounts and to inspect, monitor, copy or remove users' files if necessary. The College may also disconnect network services in any part of any building and prevent access to the facilities without notice while investigations proceed.

5.2 Cases of misuse or abuse should be reported to, and will be taken up in the first instance by the appropriate authority shown below:

5.2.1 Misuse by student - Report to Head of Further Education or Higher Education.

5.2.2 Misuse by staff – Report to IT & Digital Resources Manager

5.2.3 Misuse by managing staff, Head of Department etc. – report to Principle.

5.2.4 Misuse by anyone not included in the categories above report to IT & Digital Resources Manager.

5.3 The Head of Department and College authorities, may be informed and will deal with the incident under the appropriate disciplinary procedures for students and staff. In some cases legal action may be taken and law enforcement informed. The College reserves the right to disclose data or information about an individual's use of College's computing facilities to any appropriate or authorised third party (including law enforcement) to assist in any further investigation.

5.4 If websites containing material that may be illegal are discovered, particularly material relating to children or the exploitation of children, the College encourages its staff and students to make a report to the authorities named above or to the Internet Watch Foundation (IWF) hotline (http://www.iwf.org.uk). The normal course of events is that the IWF will request that the Internet Service Providers (ISPs) in the UK will block that site. If this does not happen the IWF will inform the Police who may investigate the matter further.

5.5 Actual or suspected security violations should be reported immediately to the College Information Security Group e-mail (isg@ucl.ac.uk).

5.6 No attempt should be made to investigate security vulnerabilities or breaches of the Policy unless or until appropriate authority has been obtained.

6 Further Information

6.1 The enrolment form signed by students explicitly binds them to abide by College Policies, of which this document forms a part. College staff are also obliged to abide by these regulations as a condition of employment.

6.2 Users of IT services who are neither staff nor students are required to complete a registration form which binds them to abide by these regulations.

6.3 In all cases the act of registering as a user of the College's IT facilities or making use of any of the IT facilities implies acceptance of conditions of use and compliance with all regulations and Policies, relevant Acts of Parliament and European Union law and directives.

6.4 From time to time College may issue good practice guidelines and reserves the right to withdraw network services to systems or services that are not operated in accordance with those guidelines.

7 Summary

7.1 Hereford College of Arts is committed to providing a safe and managed environment for students, staff and visitors to any part of the campus, by embedding this Policy and ensuring the College complies with all aspects of relevant Regulation and Law all users of IT facilities across the College will understand and be aware of what the College IT facilities can and cannot be used for.

7.2 Everyone working across the campus has a responsibility to follow all guidance as detailed in this Policy, should any person require clarification, guidance or advice then they should contact the IT & Digital Resources Manager.