Regulations governing the use of Computing facilities

Purpose and Context

The aim of these regulations is to ensure that the University computing facilities are used safely, lawfully, and equitably.

Scope

These regulations apply to anyone using the University of Huddersfield computing facilities.

Introduction

The issues covered by these regulations are important and you are strongly urged to read the regulations in detail. Any user still in doubt regarding their use of the University computing facilities must seek further advice from IT Support before proceeding (Contact IT Support).

Definitions used in these regulations

Appropriate authority refers to the Director of Digital Information, the relevant system owner, or any person nominated by them.

Computing facilities, or *University computing facilities* includes:

- IT hardware that the University provides, such as PCs, servers, storage, laptops, tablets, smart phones, and printers;
- Software that the University provides, such as operating systems, office application software, web browsers, online services (SaaS), etc. It also includes software that the institution has arranged for you to have access to;
- Data that the University provides or arranges access to. This might include online journals, data sets, or citation databases;
- Access to the network provided or arranged by the University. This would cover, for example, network connections on-campus, WiFi including eduroam and govroam, VPN connections, or connectivity to the internet from University PCs, access to networks from other providers, access to the Health and Social Care Network (HSCN), and remote working solutions provided by the University;
- Online services arranged by the University such as Microsoft 365, or any online learning resources; and
- IT credentials.

IT refers to 'information technology', the common term used to refer to anything related to computing technology, such as hardware, software, networking, the internet, or corresponding services and support.

IT credentials means the use of your University login, or any other token (email address, smartcard, dongle) issued by the University to identify yourself when using the University computing facilities or any other computing facility. For example, you may be able to use drop-in facilities or WiFi connectivity at other institutions using your usual username and password through the eduroam system.

1. Availability

Every effort is made to ensure that University computing facilities are available in accordance with times published. In general, services like e-mail and web access are always available. However, the means of delivery might not be, depending on opening hours and the reliability of hardware and software. Occasionally, University computing facilities are unavailable because of system maintenance and upgrades; in such cases users will be informed in advance whenever possible at https://hud.ac/it-status.

Unless specific arrangements have been made data is periodically removed under standard procedures carried out by system managers such as at the end of a University session. Users must make themselves familiar with the arrangements in force regarding any data they store on University computing facilities.

Except as may be required by law, the University accepts no liability for any direct, indirect or consequential loss, including loss of profits, damage, costs or expenses arising from, or relating to, acts or omissions of users of the University computing facilities, their guests, members of the public or intruders; neither does the University accepts any liability for any consequences arising out of the unavailability of University computing facilities and related services, or loss of data, no matter how caused.

2 Governance

When using University computing facilities, you remain subject to the same laws and regulations as in the physical world.

It is expected that your conduct will be lawful. Furthermore, ignorance of the law is not considered to be an adequate defence for unlawful conduct.

When accessing services from another jurisdiction, you must abide by all relevant local laws, as well as those applicable to the location of the service. Where local law conflicts with UK law or with these regulations, you should not use University computing facilities unless explicitly authorised.

You are bound by the University's general policies and regulations when using the University computing facilities, available at https://www.hud.ac.uk/policies/

You must abide by the regulations applicable to any other organisation whose services you access such as Janet and Jisc Cloud (formerly Eduserv), or when using the eduroam network at another organisation, or when using the HSCN. You are bound by the regulations put in place by other providers when using their facilities, such as for example when using a placement provider's computers or networks whilst on placement. Where such regulations conflict with UK law or with these regulations, you should not use University computing facilities unless explicitly authorised.

Some software licences procured by the University will set out obligations for the user – these should be adhered to. If you use any software or resources covered by a Combined Higher Education Software Team (Chest) agreement, you are deemed to have accepted the Jisc User Acknowledgement of Third Party Rights. See What are Chest Agreements for more information.

Breach of any applicable law or third-party regulation will be regarded as a breach of these computing regulations.

3 Authority

Authority relating to computing facilities lies with the Director of Digital Information or any person they nominate. These people are responsible for the interpretation and enforcement of these regulations.

You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of these regulations. If you feel that any such instructions are unreasonable or are not in support of these regulations, you may appeal using the Complaints Procedure.

Persons who are not students or employees of the University may be authorised to use University computing facilities at the absolute and sole discretion of the appropriate authority. Those who arrange access on behalf of persons who are not students or employees must ensure that they are made aware of these regulations prior to access being authorised and that they can be individually identified.

4 Intended Use

The University computing facilities are provided for use in furtherance of the business of the University (“valid use”); for example to support a course of study, research or in connection with employment by the University.

Use of the University computing facilities for personal activities (if it does not infringe any of the regulations and does not interfere with others’ valid use) is permitted, but this is a privilege that may be withdrawn at any point.

Use of the University computing facilities for non-institutional commercial purposes or for personal gain requires the explicit approval of the appropriate authority and can be revoked at any time. The University reserves the right to levy charges in accordance with University policies. Individuals using the University computing facilities for commercial purposes do so at their own risk.

Use of certain software licences is only permitted for academic use and, where applicable, in accordance with the user obligations published by the Chest team https://www.chest.ac.uk/user-obligations/. See the accompanying guidance for further details. You must only use University-provided software for its licensed purposes.

The University is under a duty to prevent extremism under the Counter-Terrorism and Security Act 2015. It has a zero-tolerance approach to acts which could incite or promote terrorist activity including, but not limited to, accessing websites that might be associated with extreme or terrorist organisations and which could attract criminal liability. For any research related activities, the University follows guidance provided by Universities UK for the handling of data related to security sensitive research.

5 Identity

You must take all reasonable precautions to safeguard any IT credentials (for example a username and password, email address, smart card or other identity hardware) issued to you. You must not allow anyone else to use your IT credentials. No-one has the authority to ask you for your password, and you must not disclose it to anyone.

Where using multi-factor authentication, you must never reveal your secondary authentication code to anybody, nor enter it into any website or system other than the University’s.

You must not attempt to obtain or use anyone else’s credentials.

You must not impersonate someone else or otherwise disguise your identity when using the computing facilities.

You must be prepared to identify yourself to members of staff on duty to help protect the integrity of the University computing facilities. Campus cards must be always carried when using the University computing facilities.

Access to University computing facilities is managed in accordance with and subject to the provisions of the Identity and IT Access Management Policy.

6 Infrastructure

You must not do anything to jeopardise the integrity of the IT infrastructure by, for example, doing any of the following without approval by the appropriate Authority, or unless following approved practices:

- Damaging, reconfiguring, or moving equipment;
- Loading software on the University's equipment;
- Reconfiguring or connecting equipment to the network;
- Setting up servers or services on the network;
- Deliberately or recklessly introducing malware;
- Attempting to disrupt or circumvent IT security measures.

7 Information

If you handle personal, confidential, or sensitive information, you must take all reasonable steps to safeguard it and must observe the University's Data Protection and Information Security policies and guidance available at https://www.hud.ac.uk/informationgovernance/

You should be aware of the particular risks around use of online cloud storage, removable media, mobile devices, and privately owned devices and ensure your use is in line with policy and guidance. When using a personally-owned device to access University networks or information, you must adhere to the University's Using Your Own Device Policy.

Sensitive or confidential information should only be kept in a cloud storage service that has been approved by the University and has a Privacy Impact Assessment in place.

You must not infringe copyright or break the terms of licences for software or other material.

You must not attempt to access, delete, modify, or disclose information belonging to other people without their permission, or without the explicit approval from the appropriate authority.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening, or discriminatory. The University has procedures to approve and manage valid activities involving such material; please refer to the relevant school committee.

You must abide by any University guidelines when using the University computing facilities to publish information.

8 Behaviour

Real world standards of behaviour apply online and on social networking platforms, such as Facebook, Instagram, and X (formerly Twitter).

You must not cause needless offence, concern, or annoyance to others.

You should also adhere to the University's social media policy. Guidance for students is available at https://www.hud.ac.uk/media/policydocuments/Student-Social-Media-and-Communications-Policy.pdf and guidance for staff is available at https://www.hud.ac.uk/media/policydocuments/Staff-Use-Of-Social-Media.pdf.

You must not send spam (unsolicited bulk email).

You must not recklessly consume excessive IT resources such as processing power, bandwidth, or consumables.

You must not use the University computing facilities in a way that interferes with others' valid use of them.

You must abide by any local regulations concerning eating or drinking in open access University computing facilities.

IT equipment purchased by the University must be returned for updates, rebuilding, or redeployment upon demand by an appropriate Authority.

IT equipment or software purchased by the University remains the property of the University and must be returned to the University upon request or at the end of employment, research, or studies unless transfer of ownership is agreed by an appropriate Authority and allowable under licensing terms.

9 Monitoring

The University monitors and records the use of the University computing facilities including for the purposes of:

- The effective and efficient planning and operation of the University computing facilities;
- Detection and prevention of infringement of these regulations;
- Investigation of alleged misconduct.

Such monitoring may occasionally detect personal use of University facilities, and you should be mindful that browser tabs opened on a personal device elsewhere may automatically refresh upon connection to the University network and fall into scope of monitoring.

The University will comply with lawful requests for information from government and law enforcement agencies.

You must not attempt to monitor the use of the computing facilities without explicit approval from the appropriate authority.

10 Infringement

Infringing these regulations may result in sanctions under the University's disciplinary procedures. Penalties may include withdrawal of services and/or fines. Offending material will be taken down.

Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.

The University reserves the right to recover from you any costs incurred as a result of your infringement.

You must inform the appropriate authority or a member of staff in Computing and Library Services if you become aware of any infringement of these regulations.

POLICY SIGN-OFF AND OWNERSHIP DETAILS	
Document name:	Computing Regulations
Version Number:	1.7
Equality Impact Assessment:	April 2022
Approved by:	University Teaching and Learning Committee
Effective from:	May 2024
Date for Review:	May 2025
Author:	Deputy Director and Head of IT
Owner (if different from above):	Director of Digital Information
Document Location:	https://www.hud.ac.uk/media/policydocuments/Computing-Regulations.pdf
Compliance Checks:	Monitoring of annual statistics on breaches of the Regulations handled under the respective student or staff University disciplinary processes.
Related Policies/Procedures:	IT Security Policy IT Security Procedure Manual Using Your Own Device Policy Identity and IT Access Management Policy

REVISION HISTORY

Version	**Date**	**Revision description/Summary of changes**	**Author**
V1.0	April 2017	First draft using Policy Framework. Minor drafting updates.	Head of Business Quality and Planning
V1.1	February/March 2018	Inclusion of GDPR. Minor drafting updates.	Head of Business Quality and Planning
V1.2	April 2019	Minor drafting updates.	Head of Business Quality and Planning
V1.3	May 2020	Minor drafting updates.	Business and Finance Manager

V1.4	May 2021	Minor updates for currency, URLs; inclusion of MFA instructions	Deputy Director and Head of IT
V1.5	May 2022	Typographic updates and clarifications	Deputy Director and Head of IT
V1.6	May 2023	Fixed links to other materials, minor wording changes for clarity	Deputy Director and Head of IT
V1.7	May 2024	Addition of references to HSCN; clarity on asset ownership responsibilities; clarity that all IT is under the auspices of CLS; reference to Identity policy.	Deputy Director and Head of IT