

## ICT Acceptable Use Policy

<b>Classification:</b>	Policy
<b>Version Number:</b>	2.00
<b>Status:</b>	Approved
<b>Approved by (Board):</b>	University Leadership Team
<b>Approval Date:</b>	20 July 2021
<b>Effective from:</b>	20 July 2021
<b>Next Review Date:</b>	Biennial
<b>Document Authors:</b>	Steph Jones, Stewart Doyle
<b>Document Owner:</b>	Security and Architecture Manager, ICT (Steph Jones)
<b>Department/Contact:</b>	support.hull.ac.uk
<b>Summary:</b>	This document details the policies that apply to anyone using ICT provisioned systems and services to ensure that they are used safely, lawfully, and equitably.
<b>Scope:</b>	All University members and third-parties using University owned or provisioned systems and services.
<b>Collaborative provision:</b>	Not applicable
<b>Assessment: (where relevant)</b>	Not applicable
<b>Consultation: (where relevant)</b>	Not applicable
<b>Relevant legal frameworks:</b>	See relevant section of overarching Information Governance and Assurance Policy
<b>Related documents:</b>	To be read in conjunction with ICT Acceptable Use Policy (Guidance)
<b>Published locations:</b>	Public website ( <a href="http://www.hull.ac.uk">www.hull.ac.uk</a> )
<b>Document Communication and Implementation Plan:</b>	Available upon request.

All printed versions of this document are classified as uncontrolled.  
A controlled version is available from the university website.

# ICT Acceptable Use Policy

## 1. Introduction

- 1.1 This document details the policies that apply to anyone using ICT provisioned systems and services to ensure that they are used safely, lawfully, and equitably.
- 1.2 This policy should be read in conjunction with the accompanying [ICT Acceptable Use Policy \(Guidance\)](#) and overarching [Information Governance and Assurance Policy](#).

## 2. Scope

- 2.1. This policy applies to all University members and third-parties using both University owned and provisioned systems and services, including but not limited to, desktop workstations, laptops, tablets, servers, mobile phones, wireless devices, specialised equipment, data, network access, user accounts, on-premise and cloud-hosted services.

## 3. Compliance

- 3.1. When using ICT systems and services, you remain subject to the same laws and regulations as in the physical world.
- 3.2. It is expected that your conduct is lawful. In the UK ignorance of the law is not a defence for unlawful conduct.
- 3.3. When accessing services located in a different country than where you reside, you must abide by the local laws of the country where you reside, as well as the laws applicable in any country where the service or part of it is located.
- 3.4. You are bound by the University's general regulations and policies when using the ICT systems and services, available at [www.hull.ac.uk/policies](http://www.hull.ac.uk/policies).
- 3.5. You must abide by the terms and conditions of use published by any other organisation whose services you access such as Janet and Jisc Collections.
- 3.6. When using services via Eduroam (the roaming access service for international research and education institutions), you are subject to both the regulations and policies of this University and the institution where you are accessing services.
- 3.7. Software licences procured by the University will set out terms and conditions for the user – these should be adhered to. If you use any software or resources covered by a Chest (Combined Higher Education Software Team) agreement, or Microsoft Licensing, you are deemed to have accepted their respective terms and conditions of use.
- 3.8. Breach of any applicable law or third party terms and conditions of use will be regarded as a breach of these ICT acceptable use policies.

## **4. Authority**

- 4.1. The acceptable use policies are issued under the authority of the University Leadership Team. The Director of ICT is responsible for their interpretation and enforcement, and may also delegate such authority to other people.
- 4.2. You must not use ICT services and systems without due authority. This is usually granted through the issuance of a user ID and password or other ICT credentials.
- 4.3. You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of these policies. If you feel that any such instructions are unreasonable or are not in support of these policies, you may appeal to the Director of ICT or through the University complaints procedures.

## **5. Intended use**

- 5.1. ICT systems and services are provided for use in furtherance of the mission of the University of Hull, for example to support a course of study, research or in connection with your employment by the institution.
- 5.2. Use of ICT systems and services for personal activities (provided that it does not infringe any of the policies, and does not interfere with others' valid use) is permitted, but this is a privilege that may be withdrawn at any point. Use of ICT systems and services for non-institutional commercial purposes, or for personal gain, requires the explicit approval of the Director of ICT.
- 5.3. Use of certain licences is only permitted for academic or administrative use and may be subject to the terms and conditions laid out by the licensing authority.

## **6. Identity**

- 6.1. You must take all reasonable precautions to safeguard any ICT credentials (for example, a user ID and password, email address, smart card or other identity hardware) issued to you.
- 6.2. You must not allow anyone else to use your ICT credentials.
- 6.3. Nobody has the authority to ask you for your password and you must not disclose it to anyone.
- 6.4. You must not attempt to obtain or use anyone else's credentials.
- 6.5. You must not impersonate someone else or otherwise disguise your identity when using ICT systems and services.

## **7. Infrastructure**

- 7.1. The ICT infrastructure is all the underlying systems and services that constitutes the ICT function. You must not do anything to jeopardise the integrity of the ICT infrastructure by, for example, doing any of the following without approval:
  - Damaging, reconfiguring or moving equipment;
  - Installing software on the ICT systems other than in approved circumstances;
  - Reconfiguring or connecting equipment to the network other than by approved methods;

- Setting up servers or services on the network without the express approval of ICT;
- Deliberately or recklessly introducing malware;
- Attempting to disrupt or circumvent ICT security measures;
- Attempting to impair the operation of University, or external, ICT system and services through, for example, a denial of service (DOS) attack.

## **8. Information**

- 8.1. 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 policy and information governance and assurance guidelines, available at [www.hull.ac.uk/policies](http://www.hull.ac.uk/policies).
- 8.2. You must observe the University's Information Governance Assurance Policy and associated sub-policies and guidance, available at [www.hull.ac.uk/policies](http://www.hull.ac.uk/policies).
- 8.3. You must not infringe copyright, or break the terms of licences for software or other material.
- 8.4. You must not attempt to access, delete, modify or disclose information belonging to other people without their permission, or explicit approval from the University.
- 8.5. You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist without the explicit approval from the University. The University of Hull has procedures to approve and manage valid activities involving such material.

## **9. Conduct**

- 9.1. Appropriate conduct when using ICT systems and services, extending to online activity including social networking platforms, are subject to University policies and regulations available at [www.hull.ac.uk/policies](http://www.hull.ac.uk/policies) and [share.hull.ac.uk](http://share.hull.ac.uk).
- 9.2. You must not send spam (unsolicited bulk email).
- 9.3. You must not deliberately or recklessly consume excessive ICT resources, such as processing power, bandwidth or consumables.
- 9.4. You must not use ICT systems or services in a way that interferes with others' valid use of them.

## **10. Monitoring**

- 10.1. The University of Hull monitors and records the use of ICT systems and services for the purposes of:
  - The effective and efficient planning and operation of ICT systems and services and the University;
  - Detection and prevention of infringement of University regulations;
  - Investigation of alleged misconduct;
  - The University of Hull will comply with lawful requests for information from government and law enforcement agencies.

- You must not attempt to monitor the use of ICT systems and services without explicit authority.

## **11. Infringement**

- 11.1. Infringing these policies may result in the withdrawal of services or sanctions under the institution's disciplinary processes. Offending material will be taken down.
- 11.2. Remedial action (e.g. ensuring ICT systems and services are free from malware) and/or training may be required before access is restored.
- 11.3. Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.
- 11.4. The University of Hull reserves the right to recover from you any costs incurred as a result of your infringement.
- 11.5. You must inform the Director of ICT if you become aware of any infringement of these policies.