Staff Regulations for the Use of University IT Facilities

The aim of these regulations is to ensure that Durham University's IT Facilities can be used safely, lawfully and equitably. Further information and guidance on specific issues covered by these regulations are available at https://durhamuniversity.sharepoint.com/sites/MyDigitalDurham/SitePages/Information-and-Cyber-Security.aspx. All applicable policies and standards can be found on the University's Policy Zone at https://durhamuniversity.sharepoint.com/sites/ph.

1. Scope

1.1. These regulations apply to all members of Durham University's staff and other individuals and organisations who connect to or use the **University IT Facilities** (including hardware, software, data, network access, third party services, online services or IT credentials) provided or arranged by the University. Regulations applicable to Durham University students are available at https://durhamuniversity.sharepoint.com/sites/ph.

2. Intended use

2.1. You may use a University IT Facility provided that:

a) you are an **Authorised User**, having been assigned a Durham University IT Account or been given, in accordance with University processes, express permission to use University IT Facilities;

b) you have not been required to cease use of the University IT Facility or of activities involving University IT Facilities by an **Authorised Representative**; and

c) you comply with the IT Regulations set out below.

2.2. The **University IT Facilities** are only to be used by authorised users in support of academic work and normal University duties in the course of their employment and education, or for other recognised roles or activities for which access to these facilities is granted.

2.3. You must not use the University IT Facilities for any unsanctioned commercial activity. Any use of University IT Facilities for non-institutional commercial activity requires express written permission from the Chief Information Officer. If you wish to undertake consultancy work please refer to Research & Innovation Services with regard to the approval process.

2.4. University IT Facilities may be used for personal activities, subject to certain conditions. Such personal use may include, but is not limited to, browsing the internet, printing and making personal telephone calls. Personal use is a privilege and not a right and must not be overused or abused. You should avoid using university email accounts for personal use. The University reserves the right to withdraw permission at any time, or to restrict access at the University's discretion or any other action identified in Clause 8 – Breach of these Regulations. Personal use must meet the following conditions:

a) It must be minimal and is expected to take place during personal time (that is, during a lunch break, and before or after work). Exceptions to this are where University IT

Facilities are provided in conjunction with University residential accommodation, whereby reasonable use is allowed.

b) Personal use of University IT Facilities should be clearly identified as private, for example in the title and/or filing of material in a folder marked as such;

c) It must not affect an employee's work or interfere with University business; and

d) It must not breach any of these regulations or interfere with others' valid use.

For the avoidance of doubt, inappropriate use or accessing inappropriate material, including, but not limited to, pornography or any other material that falls within the definition of Sections 6 or 7 of the Regulations, is strictly not permitted in the workplace or using any University IT Facilities either during work or personal time. Such activity may constitute gross misconduct which could lead to the termination of employment, as detailed in Section 8 of these Regulations. For procedures relating to research involving such material, see clause 6.5.

2.5. Charges are payable by users for some University IT Facilities, such as printing and replacement of lost campus cards. For current charges please see My Digital Durham.

3. Governance

3.1. Your use of the University IT Facilities must comply with the law. Ignorance of the law is not considered a valid excuse for any acts in contravention of the law, and it is your responsibility to ensure you are complying with the relevant laws.

3.2. When accessing or using University IT Facilities while in another country you are responsible for familiarising yourself with and adhering to the laws applicable in that country, and must also comply with UK law.

3.3. You are bound by the Statutes and **General Regulations of the University** when using the University IT Facilities, available at https://www.dur.ac.uk/about-us/governance/governance-documentation/statutes-and-regulations/general-regulations/. You must also adhere to the University's published policies, standards, procedures and guidance relevant to the use of University IT Facilities, available at https://durhamuniversity.sharepoint.com/sites/ph.

3.4. You must abide by the end user terms published by any other organisation whose services you access, including but not limited to **Jisc** and **Eduserv**. See definitions for further information.

3.5. You must adhere to the terms and conditions of all service and licence agreements relating to the University IT Facilities that you use including websites, software, equipment or any other service used. In the event that you have any questions regarding the terms of any software or third party service provided to authorised users, you should contact the IT Service Desk or the department which provided access to the software or service.

3.6. When using **Eduroam**, you are subject to both the IT Regulations of Durham University and the institution where you are accessing services.

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

3.8. The University is under a duty to prevent extremism in accordance with the Counter-Terrorism and Security Act 2015. You must not engage in any activity which could incite or promote terrorist activity including, but not limited to, accessing websites or social media content that might be associated with extreme or terrorist organisations and which could attract criminal liability. For procedures relating to research involving such material, see clause 6.5.

3.9. The University has a responsibility to safeguard children and vulnerable adults who are on its premises or in contact with its staff/students, and it recognises the risks presented by online activity. As such, everyone has a duty to be vigilant and report any behaviour online which would indicate a risk to vulnerable parties. Such behaviour includes, but is not limited to, accessing or distributing abusive imagery of children. For procedures relating to research involving such material, see clause 6.5.

4. Identity

4.1. You must take all reasonable precautions to safeguard any IT credentials (for example, a username and password, campus card or other tokens for authentication) issued to you. You must not allow anyone else to use your IT credentials, including your campus card. Nobody has the authority to ask you for your password and you must not disclose it to anyone. There may be exceptional circumstances in which shared passwords are required for business continuity reasons. See the Password and Credential Standard on the Policy Zone for further information.

4.2. You must not use your University password on non-University websites and systems.

4.3. You must not attempt to obtain or use anyone else's credentials, including their campus card.

4.4. You must not impersonate someone else or actively disguise your identity in order to undertake any wrongful act when using the University IT Facilities, or such that activities carried out on University IT Facilities cannot be audited.

4.5. You must not log on to a University IT Facility and leave it unattended such that it could be used by another person.

4.6. In the event that you wilfully or negligently allow your IT credentials to be used by another individual, for example by sharing your password or leaving an IT facility logged in and unattended, you may be liable for activity carried out using your account.

5. Infrastructure and Equipment

5.1. You must not knowingly do anything to jeopardise the integrity of the University IT Facilities or expose the University to risk, including, but not limited to, doing any of the following without authorisation:

- Damaging or reconfiguring equipment;
- Deliberately or recklessly introducing or transmitting malware, for example by browsing websites or downloading or opening files that could reasonably be considered likely to pose a risk of infection;
- Scanning University IT Facilities or other networks and attached devices for vulnerabilities, or attempting to exploit vulnerabilities;
- Operating a service that redistributes access or any other University resource to others. This includes connecting to the university network any equipment that routes, bridges,

switches or repeats traffic from other devices or networks, including but not limited to network hubs, switches, routers, firewalls and wireless access points (WAPs), or any device (such as a PC or server) that has been configured to perform these functions;

- Connecting to the University network any device offering a service to others, including but not limited to file, print, media, gaming and peer-to-peer servers;
- Attempting to disable access or gain unauthorised access;
- Attempting to disrupt or circumvent IT security measures.

5.2. You must immediately cease using an item of software or hardware connected to University IT Facilities in the event that the University or its Authorised Representative has requested that you do so.

5.3. You must follow advice from CIS to install, reconfigure or upgrade software and hardware where necessary to ensure security.

5.4. You must comply with the University's IT Device Standard on the Policy Zone when connecting an IT device to the University IT Facilities.

5.5. You must comply with the Information Security Classification and Handling Standard to prevent unauthorised access to and/or theft of IT equipment provided to you by the University. The level of physical security should be appropriate to the type and location of the equipment, its use and the sensitivity of any data stored.

5.6. Your device must not be used to provide access to any unauthorised users, for example by allowing a friend or relative who has not been authorised to use University IT Facilities to use your device while connected to the University network.

5.7. Devices should be logged out, locked or preferably powered off when not in use or left unattended.

5.8. You must not attempt to monitor the use of the University IT Facilities without explicit authority (see the Monitoring and Interception Policy on the Policy Zone for further information).

5.9. You must return all University IT Facilities at the end of your employment, contract or period of work, unless you have been granted an explicit exception.

6. Information

6.1. You must take all reasonable steps to ensure the security of information, in particular personal or commercially confidential information of the University in accordance with the Information Security Classification and Handling Standard. You are responsible for complying with all relevant laws, regulations or commercial contracts that govern the collection, use, storage, transmission and deletion of such information. You must observe the University's Data Protection and Information Security policies, available on the Policy Zone.

6.2. You must report any information security breach or weakness of which you become aware, including loss of equipment or suspected compromise of a device or system. Guidance on how to do this is provided on My Digital Durham.

6.3. You must not attempt to violate the privacy of others or access, delete, modify or disclose other users' information without their permission, or without explicit approval in accordance with the University's Monitoring and Interception Policy on the Policy Zone.

6.4. You must not breach copyright legislation or infringe the intellectual property rights of another person or organisation, for example use of software without an appropriate licence. You must also observe the University's Intellectual Property regulations.

6.5. You must not access, create, download, store or transmit unlawful material, or data that contain (or are capable of being resolved into) indecent, offensive, obscene, defamatory, threatening or discriminatory content. This includes material that might be subject to provisions of the Counter-Terrorism and Security Act 2015. If you wish to undertake any research or scholarly activity involving such material you must observe the appropriate University procedures to gain written approval before commencing such activity and should speak to the Chair of your Departmental Ethics Committee and / or your Head of Department as appropriate for advice in the first instance.

6.6. You must not create or transmit material with the intent to defraud.

6.7. You must not process, store or transmit any payment card data unless authorised to do so. This does not include use of your own personal payment cards.

6.8. You must ensure University information is appropriately backed up, for example by storing a copy of it in official University online storage facilities.

6.9. You must return, and not retain copies of, all information belonging to the University at the end of your employment, contract or period of work, except where an explicit exemption has been granted for you to retain it. This includes all personal data for which the University is identified as the Data Controller under data protection legislation and any data not classified as Public.

7. Behaviour

7.1. In using the University IT Facilities, you must not:

a) Do so in such a way as could reasonably be considered likely to cause any needless offence, concern or annoyance to others, or to perform any act which could reasonably be considered likely to amount to causing any individual or group any form of harassment, alarm or distress.

b) Act in a way that could reasonably be considered likely to jeopardise the University's institutional integrity or to bring the University into disrepute.

c) Present any statement or representation as the view or opinion of the University unless you have been explicitly authorised to do so. Any statement or opinion piece given must make clear that the views are that of the individual and not of the University.

7.2. You must adhere to the University's guidelines regarding social media, available on the Policy Zone.

7.3. You must not send spam (unsolicited bulk email). Internal bulk emails, to staff and/or student groups, may be sent only in relation to sanctioned University business. For communications regarding research activities, you must ensure you have gained approval from any relevant parties before proceeding, including ethical approval where required.

7.4. You must not consume IT resources such as processing power, storage, bandwidth or consumables, to an extent that could reasonably be considered excessive or that wastes the University's or another organisation's resources to investigate or resolve.

7.5. You must not use the IT Facilities in a way that interferes with or disrupts others' valid use of them. This includes, but is not limited to, corrupting or destroying other users' data and denying service to other users.

7.6. You must not breach the terms of use of any services accessed via the University IT Facilities. Any deliberate or persistent breach of such terms will be regarded as a breach of these Regulations.

7.7. You must complete all Required Learning in relation to IT, information security and data protection, as described in the Required Learning Policy on the Policy Zone.

8. Breach of These Regulations

8.1. If you are found to have breached these regulations, the University reserves the right to:

- Suspend access to University IT Facilities to enable a disciplinary investigation to take place;
- Refer your case to the relevant University representatives, to be dealt with in accordance with University Disciplinary Regulation. Consequences may extend to dismissal from the University for gross misconduct, as defined in the University's staff discipline regulations available on the Policy Zone.

8.2. Where a penalty is imposed as a consequence of a disciplinary hearing arising from a breach of these regulations, you will have the right of appeal.

8.3. Material found to be in breach of these regulations will be removed from University IT Facilities. If you have posted such material elsewhere, you may be required to do as much as is in your power to remove it.

8.4. You may be liable for any direct costs incurred as a result of a breach of these regulations for which you are responsible.

8.5. In the event that the University has reason to believe that you are participating in illegal activities using University IT Facilities, information will be passed to appropriate law enforcement agencies.

8.6. If you become aware that you or anyone else has breached these regulations, whether intentionally or otherwise, you must report this via the IT Service Desk.

9. Monitoring and Interception, and Provision of Information

9.1. Durham University reserves the right to monitor and record the use of its IT Facilities, including but not limited to email and internet use, for the purposes set out in the University's Monitoring and Interception policy on the Policy Zone. Use of University IT Facilities constitutes consent by the user to monitoring and interception in accordance with this policy.

9.2. Durham University uses a range of tools and techniques to detect potential threats to or compromises of IT Facilities. In the event that potential indicators of compromise are detected, your IT account, device or connection could be temporarily suspended for investigation, in order to protect the University, its systems, staff, students and visitors.

9.3. Durham University will comply with lawful requests for information including for example requests made under Freedom of Information or Data Protection laws or from government and law enforcement agencies.

10. Glossary

Term	Definition
Authorised representative	A person or persons that have been authorised by a relevant authority (for example the CIO with regards to IT) to deliver notices or require actions within a relevant scope.
Authorised user	Any individual who has been assigned a Durham University User Account; or any other individual to whom express permission to use University IT Facilities has been given (and not withdrawn temporarily or permanently) in accordance with University processes.
Bandwidth	Throughput of a computer network.
Credential	Typically a username and password used to authenticate to an IT system to gain access to resources.
Eduroam	eduroam (education roaming) is a service which enables students, researchers and staff to securely access the internet whilst visiting other participating institutions, using the username and password credentials provided by their home organisation.
Eduserve	An organisation that has negotiated many deals for software and online resources on behalf of the UK higher education community, under the common banner of Chest agreements. These agreements have certain restrictions that may be summarised as: non-academic use is not permitted; copyright must be respected; privileges granted under Chest agreements must not be passed on to third parties; and users must accept the User Acknowledgement of Third Party Rights.
Firewall	A network device which controls network traffic based on a set of rules to allow or deny certain connections between defined endpoints.
General Regulations of the University	The rules laid down by Senate and Council for the conduct of members of the University under the authority accorded to those bodies by the Statutes of the University. They are subject to alteration from time to time by those bodies. They are published in the University Calendar Volume I available on the web via www.dur.ac.uk/university.calendar/volumei/
Jisc	The network that connects all UK higher education and research institutions together and to the internet. When connecting to any site outside the University via the University's network you will be subject to Jisc's acceptable use policy.
Malware	Malicious software including harmful or unwanted software.
Peer-to-peer	A system that partitions tasks or workloads between peers, often used for sharing data (including torrents of copyright protected material) over networks.
Router	A router is a networking device that forwards data packets between computer networks.
Scanning	Identifying software versions and vulnerabilities in software and hardware.
Server	A device connected to a *network* which provides services to other devices – for example a file server delivers file storage services and a print server delivers access to network attached printers.
Switch	A networking device that connects devices together on a computer network by using packet switching.

University IT Facilities	All IT Facilities provided by Durham University, whether owned or hired by the University, or provided by other organisations as a result of a contract or other arrangement with the University. This includes IT Facilities purchased through research grants or other funding obtained under the auspices of the University.
University Network	See Data network.
Wireless Access Point (WAP)	A network-attached device which provides wireless connectivity to devices such as laptops, tablets and smartphones.

Document Administration

Version: 2.4
Classification: Public
Publication date: xxx
Owner: Chief Information Officer
Review date: xxx