Acceptable Use Procedure	
Enabling Policy Statement; Executive Owner; Approval Route:	Our Data - Chief Operating Officer - Compliance Committee
Is the Procedure for internal use only (Non-disclosable) ?	Disclosable
Associated Policy Statements:	N/A
Authorised Owner:	Head of Information Security
Authorised Co-ordinator:	Data Protection Officer
Effective date:	September 2023
Due date for full review:	September 2026
Sub documentation:	N/A

Approval History

Version	**Reason for review**	**Approval Route**	**Date**
1.0	First draft of Acceptable Use Policies Statement	Executive Board	30/11/2020
1.1	Annual update and corrections	Compliance (Data) Committee	20/01/2022
1.2	Annual updates, corrections, and addition of content from now retired IT Acceptable Use Policy and Guidelines	Compliance (Data) Committee	01/08/2023

1. Purpose

This document sets out the responsibilities and required behaviours of all users of University of Surrey provided IT facilities and systems. It is intended to protect you, the University and its partners, and ensure University resources are used appropriately, lawfully and equitably.

2. Scope and Exceptions

2.1. This Procedure applies to:

- University of Surrey staff
- University of Surrey students
- Third party users authorised by the University of Surrey

2.2. This procedure applies to all IT facilities and systems owned, leased, hired or otherwise provided by the University of Surrey, connected directly or remotely to University infrastructure or used on University premises, including (but not limited to):

- IT hardware such as PCs, laptops, tablets, mobile phones and printers.
- Software that the University provides, such as operating systems, office applications, web browsers etc.
- Data that the University provides, or arranges access to. This might include online journals, datasets or citation databases.
- Online services arranged by the University, such as Office 365, email etc.
- Access to the network provided or arranged by the University. This covers, for example, network connections in halls of residence, on-campus Wi-Fi and connectivity to the internet from University PCs.

2.3. The principles of information security are underpinned by legislation and the consequences of a serious breach of information security are severe. Therefore, exceptions to the principles outlined in this procedure are not expected to be allowed. In highly-exceptional cases, and with a very high level of justification, any request to relax the normal information security requirements will be subject to a risk assessment. Approval for the exception must be authorised in writing by the Chief Information and Digital Officer or a delegate.

2.4. Violation of applicable laws or any of the provisions of this procedure may be subject to:

- Revocation of access to University systems.
- Withdrawal of services, fines or ultimately expulsion or termination of contract/employment for severe infringements leading to University misconduct.
- Where appropriate, breaches of the law may be reported to the authorities.

3. Definitions and Terminology

N/A

4. Procedure Principles

User Accounts/Identity

4.1. You must not use the IT facilities and systems without the permission of the Chief Information and Digital Officer or one of his/her delegates. Authority is granted by a variety of means:

- The issue of a username and password or other IT credentials.
- The explicit granting of access rights to a specific system or resource.
- The provision of a facility in an obviously open access setting, such as an Institutional website; a self-service kiosk in a public area; or an open Wi-Fi network on a campus.

4.2. You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of this procedure.

4.3. All access to University systems must be through authorised channels - locally or remotely - using an allocated unique ID tied to your name and authentication methods determined by the University (including a password that meets policy requirements and use of multi factor authentication).

4.4. Authorised users are assigned an account for their individual use, under the following conditions:

- This account may not be used by anyone other than the individual to whom it has been issued.
- You must not attempt to usurp, borrow, corrupt or destroy someone else's IT credentials.
- The assigned account password must be changed immediately and not divulged to anyone, including ITS staff, for any reason.
- This password must not be used as the password for any other account.
- Will, if there is any indication that an account has been compromised, change their password and contact the IT Service Desk immediately.
- You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.
- You must not use your University email account or IT credentials to demonstrate or infer that you are acting on University approved business when you are acting in a personal capacity.

Intended Use

4.5. The IT facilities and systems are provided for use in furtherance of the mission of the University of Surrey, for example to support a course of study, research or in connection with your employment by the institution.

4.6. Use of the IT facilities for non-institutional commercial purposes, or for personal gain is prohibited. Any such use requires the explicit approval of the Chief Information and Digital Officer or their delegated representative.

4.7. Whilst not exhaustive, the following activities are considered to be unacceptable uses of University of Surrey facilities:

- Any illegal activity or activity which knowingly breaches any University of Surrey policy or procedure.
- Any attempt to knowingly gain unauthorised access to facilities or information.
- Providing access to facilities or information to those who are not entitled to access.
- Any irresponsible or reckless handling or unauthorised use or modification of University data.
- Any use of University facilities to bully, harass, intimidate or otherwise cause alarm or distress to others.
- Sending unsolicited and unauthorised bulk email (spam).
- Creating, storing, accessing or transmitting pornographic, offensive, defamatory, or obscene material.
- Create or transmit material:
    - Which encourages terrorism or extremism.
    - With the intent to defraud.
    - Containing confidential information about the University, its employees or students unless in the proper course of your duties or studies.
    - Which is discriminatory, offensive, derogatory, or with the intent to cause fear, alarm, annoyance, inconvenience or anxiety.
- Deliberately or recklessly consume excessive IT resources such as processing power, bandwidth or consumables.

Infrastructure

4.8. You must not jeopardise the integrity of University of Surrey IT infrastructure and systems by, for example, doing any of the following without approval:

- Damaging, reconfiguring or moving equipment;
- Loading software on the University of Surrey's equipment 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;
- Deliberately or recklessly introducing malware;
- Attempting to disrupt or circumvent IT security measures;
- Port scanning or testing the effectiveness of security measures

Email

4.9. The University supports safe, fair and proper usage of email, and Users must adhere to the University's policies. Use of the University of Surrey's email systems is intended for business use. Personal use is permitted where such use does not affect the User's quality of work or that of their colleagues, is not detrimental to the University of Surrey in any way, not in breach of any term and condition of employment and does not place the individual or the University in breach of statutory or other legal obligations. Users are accountable for their actions on the email systems.

4.10. Email addresses assigned to individual users are for the sole use of the assignee and remain University of Surrey assets.

Software Licensing

4.11. The University has a legal responsibility to ensure that the software it is using has a valid licence and is being used only in accordance with the End User Licence Agreement (EULA). You must abide by software licensing terms and conditions.

Intellectual Property

4.12 You must not use any intellectual property in breach of its copyright or licence.

Handling University and Research Partner Data

4.13. All Users who handle data on behalf of the University of Surrey are responsible for ensuring that this is done in accordance with all University policy, partner and legal requirements.

Internet Usage

4.14. The University supports safe, fair and proper usage of the Internet. Users of the Internet from University equipment or connecting to the University network must adhere to the University's policies. Use of the University of Surrey's Internet systems is intended for business use. Personal use is permitted where such use does not affect the User's quality of work or that of their colleagues, is not detrimental to the University of Surrey in any way, not in breach of any term and condition of employment, and does not place the individual or the University in breach of statutory or other legal obligations. Users are accountable for their actions on Internet systems.

Social Media

4.15. You must ensure that you are aware of your obligations when using Social Media either personally or for work regardless if on University equipment or not, and the potential consequences of unacceptable use of social media. The full policy detail of the Social Media Policy is available at: https://www.surrey.ac.uk/about/policies-and-procedures

Monitoring

4.16. Subject to UK law, the University reserves the right to log, filter, survey, monitor and limit the use of all University computer and network resources, data and information (including without limitation Internet, email and all files and databases) by its users at any time without notice, for monitoring and record-keeping purposes, preventing or detecting crime, investigating or detecting the unauthorised use of the University's communication systems, or ascertaining and ensuring compliance with the University's practices or procedures. You should have no expectation that any information on University systems will be kept confidential from relevant officials of the University in the normal discharge of their duties. The University may disclose such information to others, inside or outside the University, at its sole discretion for legitimate business or legal reasons.

Corporate and User-Owned Mobile Devices

4.17 The use and support of University and personally-owned mobile devices to access University data is at the discretion of the IT department and such devices are subject to University policy and procedure. The full policy detail of the IT Equipment Provisioning Procedure is available at: https://www.surrey.ac.uk/about/policies-and-procedures

Office Area and Off-Site Security

4.18 You are obliged to ensure that computing devices and data are kept secure, during and after working hours, both on and off-site.

Leaving the University

4.19 On leaving the University your access to the University network and data will be discontinued immediately and you must return all University-provided equipment and any University data whether printed, stored on removable media, or stored on remote or non-University computing systems. You must not delete any University data without the permission of your line manager or tutor.

Training

4.20 Training is a key measure of the University’s provision of defensible cybersecurity, and it is the responsibility of the University to provide this, as well as for users to complete this training when requested.

5. Governance Requirements

5.1. Implementation: Communication Plan

5.1.1. All users in the University must comply with these policies. To ensure full coverage, all new users must sign the Acceptable Use Procedure as part of their induction. Agreement to these terms will be recorded and kept in electronic form.

5.1.2. The Welcome to the University of Surrey email from HR states that new starters must read and understand the Acceptable Use Procedure.

5.1.3. All Users should also be aware of the University’s Our Data Policy Statement available at: https://www.surrey.ac.uk/about/policies-and-procedures.

5.1.4. For any policy/procedure disputes, exceptions or questions please contact the Cyber Security Team at infosec@surrey.ac.uk in the first instance.

5.2. Implementation: Training Plan

5.2.1. Agreement to this procedure will be signed off annually thereafter as part of cyber awareness training for Users.

5.3. Review

The procedure will be reviewed every 3 years or as necessary following changes in the legislative context. Minor changes which do not change the meaning of the procedure, will be proposed to Compliance (Data) Committee before being implemented. Major changes that alter the meaning of the procedure or significant re-writes will be considered by Compliance (Data) Committee.

5.4. Legislative Context and Higher Education Sector Guidance or Requirements

Related legislation includes:

- Telecommunications Act 1984
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Counter Terrorism and Security Act 2015
- UK General Data Protection Regulation
- Data Protection Act 2018

5.5. Sustainability

This procedure has no impact on carbon emissions or on energy consumption.

6. Stakeholder Engagement and Equality Impact Assessment

6.1. An Equality Impact Assessment was completed on 04/08/2023 and is held by the Authorised Owner.

6.2. Stakeholder Consultation was completed, as follows:

Stakeholder	Nature of Engagement	Request EB Approval (Y/N)	Date	Name of Contact
Governance	Procedure review		05/09/23	Andrea Langley
H&S	Procedure review		06/07/23	Matthew Purcell
Sustainability	Procedure review		04/08/23	Martin Wiles