Acceptable Use Policies Statement

Operational Owner:	Head of Information Security
Executive Owner:	Chief Operating Officer
Effective date:	20/01/2022
Review date:	20/01/2023
Related documents:	IT Acceptable Use Policy and Guidelines Data Protection Policy Social Media Policy Monitoring Policy Information Security Policy Sustainability Policy

Approval History

Version	Reviewed by	Reason for review	Approved by	Date
1.0	Nicola Orpin	First draft of Acceptable Use Policies Statement	Executive Board	30/11/2020
1.1	Ambrose Neville	Annual update and corrections	Compliance(Data) committee	20/01/2022

1 Introduction

1.1 Purpose

1.1.1 The Acceptable Use Policies (AUPs) are intended to protect you as well as the University and its partners and to ensure the University of Surrey's resources are used appropriately, lawfully and equitably.

You will also be required to participate in periodic awareness training. Violation of applicable laws or any of the provisions of this policy may be subject to disciplinary action, up to and including termination and legal proceedings.

The issues and regulations covered by this policy are complex and therefore each section of this policy statement has a link to more detailed information of this policy's requirements.

1.2 Scope

1.2.1 The Acceptable Use Policies (AUPs) are mandatory for all Users that use any sort of computing across the university.

These regulations apply to anyone using the IT facilities (hardware, software, data, network access, third party services, online services or IT credentials) provided or arranged by the University of Surrey.

1.3 Definitions

1.3.1 **User(s)** - all University staff and students, temporary staff, contractors, consultants, vendors, service providers, partners, affiliates, third parties or any other person or entity authorised to utilise the University's information resources.

University Systems – any hardware, software, data, network access, third party services or online services provided or arranged by the University of Surrey.

2 Policy Principles

2.1 **Access to University Systems**

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. You must adhere to the University's password and multi-factor authentication policies.

The full policy detail of the IT Acceptable Use Policy and Guidelines is available at https://www.surrey.ac.uk/about/policies

2.2 **Infrastructure**

You must not jeopardise the integrity of the University IT infrastructure.

The full policy detail of the IT Acceptable Use Policy and Guidelines is available at https://www.surrey.ac.uk/about/policies

2.3 **Software Licensing**

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.

The full policy detail of the IT Acceptable Use Policy and Guidelines is available at https://www.surrey.ac.uk/about/policies

2.4 **Intellectual property**

You must not use any intellectual property in breach of its copyright or licence.
The full policy detail of the IT Acceptable Use Policy and Guidelines is available at https://www.surrey.ac.uk/about/policies

2.5 **Handling University and Research Partner Data**

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.
The full policy detail of the IT Acceptable Use Policy and Guidelines and the Data Protection Policy is available at https://www.surrey.ac.uk/about/policies

2.6 **Non-university related private data**

Subject to UK law, non-University related personal data such as private files, photos or messages are kept on University equipment, media and services at the User's risk. The University has no liability for erasure or destruction of any such information.
The full policy detail of the IT Acceptable Use Policy and Guidelines is available at https://www.surrey.ac.uk/about/policies

2.7 **Internet Usage**

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.
The full policy detail of the IT Acceptable Use Policy and Guidelines is available at https://www.surrey.ac.uk/about/policies

2.8 **Social Media**

Social media forms a large part of our communications and the University actively encourages the use of these tools. 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

2.9 **Email**

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. The full policy detail of the IT Acceptable Use Policy and Guidelines is available at https://www.surrey.ac.uk/about/policies

2.10 **Online Conferencing and Communications Applications**

Online conferencing applications are an important part of our communications. You should be aware of what constitutes appropriate usage of online conferencing applications and the potential consequences of inappropriate usage.
The full policy detail of the IT Acceptable Use Policy and Guidelines is available at https://www.surrey.ac.uk/about/policies

2.11 **Monitoring**

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.

The full policy detail of the IT Acceptable Use Policy and Guidelines and the Monitoring Policy is available at https://www.surrey.ac.uk/about/policies

2.12 **Reporting Incidents**

You must be aware of what constitutes a reportable incident, and how you should report them. Guidance is available via the staff intranet, and the full policy detail of the Information Security Policy is available at https://www.surrey.ac.uk/about/policies

2.13 **Corporate and User-Owned Mobile Devices**

Mobile devices such as tablets and smartphones need to be protected to the same extent as computers. The use and support of University and personally-owned mobile devices to access University data are at the discretion of the IT department and such devices are subject to University policy.

The full policy detail of the Mobile Phone Policy and the Using Your Own Devices Policy is available at https://www.surrey.ac.uk/about/policies

2.14 **Office Area and Off-Site Security**

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

The full policy detail of the IT Acceptable Use Policy and Guidelines is available at https://www.surrey.ac.uk/about/policies

2.15 **Sustainability**

Users should follow the University's established sustainability initiatives where possible.

The full policy detail of the Sustainability Policy is available at https://www.surrey.ac.uk/about/policies

2.16 **Leaving the University**

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.

The full policy detail of the IT Acceptable Use Policy and Guidelines is available at https://www.surrey.ac.uk/about/policies

2.17 **Training**

All Users are obliged to periodically undertake the University's Security and Privacy Awareness training courses. 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 appropriate training.

The full policy detail of the IT Acceptable Use Policy and Guidelines and the Information Security Policy is available at https://www.surrey.ac.uk/about/policies

Additional information on Security and Privacy at work and home can be found on SurreyNet.

3 Governance Requirements

3.1 Responsibility

3.1.1 The Acceptable Use Policies Statement and supporting policy content are subject to approval by the Data and Infosec Steering Committee (DISC).

Line managers are responsible for ensuring that staff in their areas are aware of and have access to appropriate guidance and equipment to enable them to comply with the Acceptable Use Policies Statement and supporting policies.

All individuals who use University IT equipment must comply with the Acceptable Use Policies Statement and supporting policies.

3.2 Implementation / Communication Plan

3.2.1 All users in the University must comply with these policies. To ensure full coverage, all new users must sign the AUPs as part of their induction. Agreement to these terms will be recorded and kept in electronic form. Agreement to the AUP will be signed off annually thereafter as part of cyber awareness training for Users. All Users should also be aware of the University's IT Security policy available at https://www.surrey.ac.uk/about/policies. For any policy disputes, exceptions or questions please contact the Cyber Security Team at infosec@surrey.ac.uk in the first instance.

3.3 Exceptions to this Policy

3.3.1 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 policy 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 Security Officer or a delegate.

3.4 Review and Change Requests

3.4.1 The policy will be reviewed annually or as necessary following changes in the legislative context.

Minor changes which do not change the meaning of the policy, will be proposed to the Data and Infosec Steering Committee (DISC) before being implemented.

Major changes that alter the meaning of the policy or significant re-writes will be considered by the Data and Infosec Steering Committee (DISC)

3.5 Legislative context

3.5.1 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 Regulations
- Data Protection Act 2018

3.6 Stakeholder Statements

3.6.1 Equality: The University is strongly committed to equality of opportunity and the promotion of diversity for the benefit of all members of the University community. The University's approach is to promote equality across the full range of its activities, in employment, teaching and learning and as a partner working with and within local, national and international communities. Equality Analysis is a process which examines how the impact of the policy has been considered on the diverse characteristics and needs of everyone it affects. This policy has been reviewed and no negative impact on equality has been identified.

3.6.2 Health & Safety: No new health and safety implications arise from the implementation of this policy. Therefore, the principles set out within the University Health and Safety Policies will be seen to apply in this respect

3.6.3 Other: n/a