Using Your Own Applications and Devices Policy	
Enabling Policy Statement; Executive Owner; Approval Route:	Our Data - Chief Operating Officer - Compliance Committee
Associated Policy Statements:	
Authorised Owner:	Head of Information Security
Authorised Co-ordinator:	Lead Information Security Assurance Specialist
Effective date:	13/07/2022
Due date for full review:	14/07/2024
Sub documentation:	Information Security Policy Framework Data Protection Policy Acceptable Use Policies Statement Terms of Reference: Compliance (Data) Committee

Approval History

Version	Reason for review	Approval Route	Date
1.0	First Draft – incomplete for ISSG discussion	James Newby	20/01/2015
2.0	Changes made following input from ISSG meeting	James Newby	09/03/2015
3.0	Changes made during final revisions by sub-group	James Newby	17/03/2015
4.0	To incorporate extension of provisions to cover personally acquired applications. Input from GW, AK and JN	JN/GW	01/08/2015
5.0	To explicitly reference removable media	GW	26/10/2015
6.0	Major redraft to reflect current reporting structures, supporting policy, procedure	Compliance (Data)	13/07/2022

1. Introduction and Purpose

This document sets out the University's policy on the use of personally-owned devices to process University data and forms part of the University's Information Security Policy.

Whilst it is recognised that staff use of personally-owned devices for work purposes brings benefits to the University, such devices pose a high security risk to the University as they are not managed by the University, may not be patched or running adequate anti-virus software, and are likely to be more vulnerable to unauthorised access.

Staff are also more likely to have admin rights on their personally-owned computer which increases the risks from malware. Copying University data to personally-owned devices also reduces the ability for the University to know where University data is stored, and makes it harder to comply with relevant legislation.

1.1. The University understands and acknowledges that most staff use their own devices and applications to access, store and transmit University data for legitimate work purposes which enhances their effectiveness and benefits the institution. This policy does not therefore seek to inhibit the use of these apps or devices, but to provide clear guidance for their use.

1.2. The aim of the policy is to ensure that the University complies with data protection legislation and that University information, particularly personal and sensitive information, is protected from unauthorised access, dissemination, alteration, or deletion. It complements and supports the existing Data Protection Policy.

1.3. The policy also aims to ensure that University data, which may be data about the University, its staff, students, clients, suppliers and other business connections; information that is confidential (including but not limited to that subject to contractual obligations to maintain confidentiality), proprietary or private information; and intellectual property owned by the University or in which the University has a legal interest, is properly protected.

2. Scope and Exceptions to the Policy

2.1. The policy covers all University staff and students with access to University IT networks, data and systems.

2.2. Devices and applications acquired by staff personally and only used for personal purposes (i.e. not used to access, store or transmit University data) fall outside the scope of this policy. Digital equipment, devices and apps come into scope when used to handle University data.

Exceptions:

2.3. Any individual who wishes to use a personally-owned app or device for purposes not allowed by this policy (for example, to access, store or transmit sensitive University information), must first seek formal risk-assessment of the proposed activity/technology, with ultimate review and oversight from Compliance (Data) Committee and Senior Information Risk Owner for any exceptions

3. Definitions and Terminology

Device	fixed or mobile computing equipment (e.g. server, desktop PC, laptop, tablet, smartphone) or any equipment capable of digital data storage (e.g. USB key/memory stick, disk drive, media player, CD/DVD, digital tape).
Application (app)	software used to perform a particular function that may be paid for, free-to-use, open-source or personally written. It may run locally and/or from a remote location and accessed as a web-service (Cloud/SaaS). The app may be available on one or more personal and/or corporate owned devices.
Information security	the preservation of the confidentiality, integrity and availability of information.
Information	data which has meaning.
Information asset	all data with meaning that can be exploited to advance the University's objectives

	or confer competitive advantage.
Sensitive data	data which includes elements requiring some form of restriction of its availability. This normally includes personal information or data with commercial value to the University.
System owner	Head of Unit (Department or Faculty) or their nominee with prime responsibility for managing and maintaining an information system, database or network; this includes the day to day operation
Handling data	the accessing, storing, processing or transmission of data. This includes accessing the public Internet via University networks.

4. Policy Principles

4.1. It is recommended that University data and services are accessed from University provided and managed devices. If this is not possible, then formally-adopted University-authorised services should be used in accordance with the Acceptable Use Policies Statement.

4.2. All staff using their own apps or devices to access, store and transmit University data are expected to be aware of basic information security good practice. As per the Acceptable Use Policies Statement, it is a requirement that staff have viewed the Information Security training content available at https://securitytraining.surrey.ac.uk and completed the UK Law, Privacy and Compliance online data protection training module available at: https://surreylearn.surrey.ac.uk/d2l/le/lessons/226042/lessons/2102878.

4.3. Do not use personal apps or devices for storing, accessing or transmitting personally-identifiable or commercially sensitive information. The benefits that arise from the convenience and productivity enhancements of being able to access personal calendars, emails, contacts and documents containing less-sensitive data do not extend to handling highly-sensitive or commercially-confidential data. Staff should therefore comply with the principle that the use of their own apps and devices is appropriate for activities that help them "keep in touch with the office" but not for the handling of sensitive information. If in doubt, staff should submit a Data Privacy Impact Assessment to the Information Compliance Unit team, as outlined in the Data Protection Policy.

4.4. Device functionality and information security threats are constantly changing, so the rules will be updated frequently. As technical requirements and solutions will change over time and new information security risks will emerge constantly, the requirements and criteria for the issuing and use of apps and devices will change frequently, and may be addressed in specific supplemental guidance

Procedures:

When using their own apps or devices to access, store, manipulate or transmit University data, all staff must comply with the following basic measures:

4.5. Configure smartphone and tablet devices to highest-available password setting. Four-digit passwords are not considered sufficiently secure and most devices will support passwords of at least six digits.

4.6. Staff-owned devices that are also used for personal purposes should not be used to download sensitive or commercially-sensitive University data.

4.7. Personal or commercially-sensitive University data should only be transmitted using University provided devices, and in an appropriately secure fashion.

4.8. Unauthorised applications, file stores and cloud-based data repositories must not be used to manipulate, transmit or store University data.

4.9. Any device or application procured at the University's expense must be acquired via the normal IT equipment/software purchasing processes.

4.10. Devices such as mobile phones and tablets that are used to synchronise with University email/calendar/contact accounts or access University data should not be shared with other non-University users (such as family members).

4.11. Staff must report the loss of any personally-owned device via the breach reporting mechanism at https://www.surrey.ac.uk/information-governance/report-data-breach if it is within the scope of this policy, so the risk of a data breach may be assessed.

Roles & Responsibility:

Information security remains the responsibility of all University staff, but the following specific responsibilities are assigned to these individuals and groups:

4.12. Overall responsibility for the University's strategic plans for information security rests with the Executive Board member serving as the Chair of Compliance (Data).

4.13. The Chief Information and Digital Officer is responsible for ensuring that the arrangements for governing the scoping, development, implementation and maintenance of University IT systems, networks and databases comply with the principles of good information security. This includes the development of network access controls to ensure that only appropriate access is available to those using their own devices.

4.14. Responsibility for the identification, treatment and remediation of information risk, including both those within the orbit of IT Services as well as those across the rest of the University resides with the Head of Information Security.

4.15. System owners are responsible for ensuring that IT systems they manage are configured appropriately and used effectively, in accordance with the IT Security Policy.

4.16. Information Asset Owners are accountable for ensuring that information assets within their realm of responsibility are managed in accordance with the Data Protection Policy, legislative context, and any contractual agreements involving third parties.

4.17. All staff who are users of information systems must manage the creation, storage, amendment, copying, archiving and disposal of information in a manner which safeguards and protects its confidentiality, integrity and availability. This includes the use of staff-owned devices to access, store or transmit University-owned data.

4.18. All staff are responsible for accessing and engaging with all information security training and guidance provided by the University.

5. Governance Requirements

Implementation: Communication Plan

5.1. This policy will be initially communicated to managers via a Leaders Alert. Further dissemination will then take place as part of the broader plan to use all available communication channels to raise information security awareness among all staff.

Review:

5.2. This policy will be reviewed biennially or as necessary.

Legislative Context and Higher Education Sector Guidance or Requirements:

5.3. The University is bound by the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (the DPA). The seventh principle of the DPA states that:

"appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data"

5.4. Loss of devices holding University data may cause damage and distress to those who entrust us to look after their data, damage the University's reputation and its relationship with its stakeholders (including research funders), and have significant legal and financial consequences. The Information Commissioner can impose serious monetary penalties on the University for breaches of the GDPR and DPA.

5.5. University data held on personally-owned devices is subject to the Freedom of Information Act and Data Subject Access rights under the GDPR and the DPA and must be provided to the University of Surrey Information Compliance Unit on request.

5.6. Loss of devices containing other University data may give rise to loss of rights in intellectual property, inability to register rights in intellectual property and breach of contractual and other obligations to third parties for disseminating or otherwise failing to protect confidential information.

6. Stakeholder Engagement and Equality Impact Assessment

6.1. Equality: The policy has been assessed to exert a low equality impact so a full equality assessment is not required and has not been undertaken.

6.2. Health & Safety: No health and safety implications arise from the implementation of this policy.