Policy Statement **Executive Owner** **Approval Route:**	Our Data Chief Operating Officer Compliance (Data) Committee
Authorised Co-Ordinator:	Compliance Manager OIA and Policy Framework
Effective date:	14 December 2022
Due date for full review:	January 2024

Approval History

Version	Reason for review	Date
1.0	Creation of Policy Statement	25/1/22
2.0	Policy Statement updated to include Information Security Policy and Data Protection Policy	14/12/22

Introduction

The **University Policy Framework** comprises 8 **Policy Statements** – Our Colleagues, Our Students, Our Education, Our Research and Innovation, Our Safety, Our Data, Our Partners and Reputation, Our Operations.

The 8 **Policy Statements** are high level documents which cover the University's mission, aims and business. **Policy Statements** are aligned to the University Strategy.

The **Policy Framework** is detailed in the Procedure of Policies and Procedures (POPP). POPP provides direction on, and standards for, the development and review of University **Policy Statements**, **Procedures** and related documentation.

Procedures are 'how to …' documents, each of which is owned by one **Policy Statement**. **Procedures** may also be associated with one or more other **Policy Statement(s)**. The Vice-Chancellor, as the principal Academic and Administrative Officer of the University, is accountable to Council for the good management of the University and for the matters set out in each **Policy Statement**. The Vice-Chancellor delegates responsibility for delivery to the Executive Owner of each **Policy Statement**.

This is the **Policy Statement** for: **Our Data**

1. Purpose and Scope

This document forms the University of Surrey's "Our Data Policy Statement". It incorporates the Information Security Policy and Data Protection Policy.

1.1. The University recognises that the data it manages must be appropriately secured for it to maintain its reputation for trustworthiness, to protect the institution from the consequences of breaches of confidentiality, failures of integrity or interruption to the availability of that data, and to comply with the law and contractual agreements.

1.2. Data is a corporately owned asset that requires clear governance processes to control its processing and retention.

1.3. The University has developed this Policy (approved by Executive Board) and supporting policies and procedures for information security and data protection (approved by the Executive Board sub-committee). They are published, communicated to employees and relevant external parties, and are in place to help protect our data assets against internal, external, deliberate or accidental threats and vulnerabilities.

1.4. This Policy applies to:

- All colleagues, students, contractors and visitors, or any other person or organisation having access to University of Surrey data
- All University of Surrey data including personal data
- The equipment, systems, credentials, etc. that are used to access and safeguard data

1.5. Failure to comply may lead to:

- Damage and distress being caused to those who entrust us to look after their data
- Reputational damage to the University and its relationship with stakeholders
- Damage caused by unavailability, inaccessibility or corruption of University Information Assets
- Significant legal and financial consequences
- Disciplinary action being taken against members of staff up to and including dismissal. In the

case of a breach of this policy by a contractor, colleague, student or volunteer, it may lead to the termination of the engagement or referral for action under other procedures

Information Security

1.6. Information Security is defined as the "preservation of confidentiality, integrity and availability of information". These can be summarised as:

- Confidentiality: Information is only available to authorised users
- Integrity: Information is accurate and complete
- Availability: Authorised users have access to Information when they need it

1.7. The level of Information Security applied in individual circumstances shall be driven primarily by the classification of the information concerned and the level of rigour proportionate to the risks involved.

1.8. University data will be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

1.9. The University shall prepare, test, and review protocols for responding to suspected Information Security breaches.

1.10. Information Security risks shall be managed via Risk Register/s. Significant residual risks will be escalated to the Compliance (Data) committee as required.

1.11. Mandatory information security and data protection training is provided to all staff.

Data Protection

1.12. Anyone who processes personal information within the University must comply with the principles of data protection. These Principles outlined below define how personal data can be legally processed.

a) processed lawfully, fairly and in a transparent manner in relation to the data subject

b) collected for specified, explicit and legitimate purposes

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

d) accurate and, where necessary, kept up to date

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

1.13. The University shall be responsible for and be able to demonstrate compliance with data protection legislation.

Data Subject Rights

1.14. The University will comply with all data subject rights as appropriate in relation to the processing it undertakes. These rights are:

- Transparency of processing
- Right of access to personal data (Also known as a Subject Access Request)
- Right of rectification of inaccurate personal data
- Right of erasure

- Right to restriction of processing
- Right to data portability
- Right to object to processing in certain circumstances
- Right to object to automated individual decision making, including profiling

Transparency of processing

1.15. Wherever personal data is collected for a new purpose, the Information Asset Owner responsible for that data will ensure a Privacy Notice is created or an existing one updated and shared with data subjects. The Privacy Notice will include:

- Name of data controller and contact details
- Contact details of the University Data Protection Officer
- Purposes of processing the data
- Legal basis of processing
- Any transfers outside the UK
- Length of time for which data will be retained
- Data subject rights in relation to the data
- Recipients of the data
- Statutory or contractual requirements to provide the data
- Any automated decision-making including profiling
- Right to complain to the Information Commissioner's Office (ICO) if data is not processed in accordance with data protection principles

Accountability Obligations

1.16. **Record keeping**
The University must keep full and accurate records of all its processing activities in accordance with the UK GDPR requirements.

1.17. **Data Protection Impact Assessments (DPIA)**
A DPIA is a key part of the University's accountability obligations under UK GDPR designed to systematically analyse, identify and minimise the data protection risks of a project or plan involving the processing of personal data likely to result in high risk to individuals. DPIAs are completed by the Information Asset Owners and signed off by the Data Protection Officer.

1.18. **Sharing Agreements**
An appropriate contract/Data Sharing Agreement should be put in place when sharing personal data outside the University; especially processing of personal data outside the UK.

2. Definitions

Acceptable Use Policy - Regulations for using University of Surrey IT facilities

Data - Information in all its forms which is under the control of the University

Data Classification - the process of organising data by relevant categories so that it may be used and protected more efficiently e.g. unrestricted, restricted and highly restricted

Data Controller - the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor - the entity which processes personal data under instructions from the Data Controller

Data Subject - a natural person whose personal data is processed by the University of Surrey or by an appointed data processor

Encryption - the process of encoding data, information or messages in a way that unauthorised persons cannot read it but those authorised (hold the key or password) can

Information - See "Data"

Information Asset - a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles

Information Asset Owner - member of staff who manages an information or data asset and who has the power to make decisions about how that information/data is managed

Information Security Breach - means any external act or internal act or omission that results in Information and/or Personal Data being disclosed incorrectly or unlawfully; altered, destroyed, or made otherwise unavailable

Information Governance Framework - ensures that information, particularly personal, special category, sensitive and confidential information, is effectively managed with accountability structures, governance processes, documented policies and procedures, staff training and appropriate resources

Personal data - any information that relates to an identified or identifiable living individual

Processing - any operation or set of operations which is performed on data, including personal data

Record - information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business

Records Management - controlling records within a comprehensive regime made up of policies, procedures, systems, processes and behaviours. Together they ensure that reliable evidence of actions and decisions is kept and remains available for reference and use when needed

Senior Information Risk Owner (SIRO) – A member of Senior Management who attends the Senior Management Board and provides assurance to that Board on the organisation's Information Governance Framework and data and cyber risk policy, act as champion for data compliance and cyber security on the Board.

Special Category Data - personal data which requires more protection because it is sensitive e.g. racial or ethnic origin, religious or philosophical beliefs, biometric, health and sexual orientation

3. Objectives

3.1. Ensure that data is appropriately controlled, classified and protected

3.2. Reduce the risk of data leakage by negligence or human error

3.3. Ensure confidentiality, integrity and availability of our data

3.4. Reduce the risk of security incidents including those involving third parties

3.5. Make data protection integral to the design and implementation of systems, services, products and business practices

3.6. Reduce the likelihood of a personal data breach that will affect our stakeholders

4. Legislative Context and Higher Education Sector Guidance or Requirements

- UK General Data Protection Regulation 2016/679
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Computer Misuse Act 1990

- The Counter Terrorism and Security Act 2015 (in particular the 'prevent duty')
- The Payment Card Industry Data Security Standard (PCI DSS)
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Surveillance Camera Code of Practice issued under the Protection of Freedoms Act (2012) (PoFA)
- Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003.
- Environmental Information Regulations 2004

5. Delivery Parameters

5.1. **Data is held in compliance with the University's regulatory obligations including data protection legislation** - Data is kept secure and personal data must only be processed under appropriate, usually limited, conditions in compliance with data protection legislation. Data subjects are able to exercise rights in respect of their own personal data.

5.2. **Identify and manage data risks** - We will have a culture of risk identification that applies to all of our colleagues, students, contractors, visitors, or any other person or organisation having access to University of Surrey data. Data risks will be identified at a local level and reported upwards to identify trends and mitigations with the Compliance (Data) Committee maintaining oversight of all out of appetite risks.

5.3. **Confidence in the reliability and quality of the data is maintained throughout its lifecycle** - The University holds timely, accurate and reliable data in order to manage its activities, support business change and meet internal and external requirements to enable it to demonstrate accountability through accurate reporting.

5.4. **Develop data aware culture** - Through developing appropriate behaviours for a more collaborative data aware culture where every colleague and student takes personal responsibility for the management of data under their control.

5.5. **Engage with our main stakeholders** - We will seek to engage with our contractors and key stakeholders to establish common principles and foster high standards.

5.6. **Report, investigate and take action** - Incidents will be investigated to ensure that, where necessary, appropriate action is taken to mitigate the consequences and prevent a repetition of similar incidents in the future.

5.7. **Develop our colleagues', students' and contractors' skills** - All colleagues, students and contractors will be given the skills and training needed to comply with this Policy appropriate to the role they are undertaking. It will be made clear to colleagues and students their roles and responsibilities and how the University's Process and Procedures support them in discharging these responsibilities.

6. Responsibilities (ownership)

6.1. **Council**

- Ultimate responsibility for data integrity and compliance rests with the University's governing body, the Council
- Council approves the University's Strategy and monitors progress against it
- The Council have delegated to the Vice Chancellor the executive accountability for cyber security and data compliance
- Promoting a culture of data awareness and compliance

6.2. **Vice Chancellor**

- Overall accountability for the University's performance
- Setting a culture of cyber awareness and data maturity

6.3. **Policy Owner - Chief Operating Officer (COO)**

- Responsible for formulating the resource allocation requests for data management (security

and governance)
- Responsible for the appointment of appropriate qualified senior personnel

6.4. **Executive Board**
- Accountable for applying the supporting documentation within their portfolios
- Responsible for resolving escalated risks and issues from the Compliance (Data) Committee
- Responsible for approving resource allocation requests in the context of the wider planning and prioritisation processes

6.5. **University Secretary and General Counsel (Senior Information Risk Owner)**
- Responsible for appointment of Data Protection Officer
- Chairs the Compliance (Data) Committee
- Overall responsibility for the University's strategic plans for information security and data compliance rests with the Senior Information Risk Owner serving as the Chair of Compliance (Data) Committee

6.6. **Compliance (Data) Committee**
- Approval of supporting Procedures
- Responsible for overseeing progress and delivery within the scope of the Information Governance framework
- Responsible for resolving issues and barriers to success
- Responsible for making the case for appropriate resource allocation
- Responsible for ensuring identified risks have been mitigated within the risk appetite

6.7. **Chief Information and Digital Officer (CIDO)**
- The CIDO is responsible for overseeing ITS resources to manage day-to-day information security activities
- To ensure that university systems, networks, databases and third-party arrangements are designed and installed with appropriate measures implemented to prevent information security breaches
- To provide adequate data retention capacity and technical security measures to enable staff to comply with published data retention schedules and other system specific information security requirements

6.8. **Head of Information Security**
- The Head of Information Security 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

6.9. **Data Protection Officer**
- The Data Protection Officer ensures that policies, procedures, and the Information Governance Framework and training are in place to address the obligations of the organisation to data subjects

6.10. **System Owners**
- System owners are responsible for ensuring that IT systems they manage are configured appropriately and used effectively to ensure that the risks of an Information Security incident are minimised. These owners are assumed to be responsible for the organisational and technical measures necessary to ensure that good Information Security practice is built into their system's day to day operation, addressing confidentiality, integrity and availability

6.11. **Information Asset Owners**
- To ensure that an appropriate security classification is applied to the information they are responsible for, and that encryption of high-risk data and sensitive information is applied where required
- To ensure that the business rules covering access rights to the service are defined and maintained, and that they are compatible with the security classification of the underlying

information

- To ensure that the Information Security risks for the service are identified, assessed and addressed prior to implementation, and reviewed at regular intervals thereafter
- To ensure that information assets are effectively managed in accordance with the data protection principles and the Our Data Policy
- To ensure adequate resourcing has been provided to carry out and maintain up to date data protection impact assessments (DPIA) and privacy notices for the activity/information assets

6.12. **Heads and Directors of Faculty Operation**

- Professional Services Department Heads and Directors of Faculty Operations shall ensure that adequate departmental business continuity arrangements are in place in their departments to prevent failures of data compliance, operational disruption or reputational damage following an Information Security incident
- Shall ensure that all equipment capable of storing or transmitting data is held securely and that the risk of theft or misuse is minimized

6.13. **Heads and line Managers**

- Responsible for ensuring there is a culture of data awareness and cyber security compliance within their teams
- Responsible for ensuring all staff are, at the earliest opportunity, appropriately trained
- Responsible for ensuring compliance with all relevant Procedures relating to Information governance and cyber security
- To ensure that the business processes and practices in their areas comply with the Information Security and Data Compliance Processes and Procedures

6.14. **University Staff**

- To comply with this Policy and supporting related documents from the policy framework, including the Acceptable Use Policy
- All staff shall follow University policies, procedures, and system instructions to ensure that no breaches of Information Security result from their actions
- To complete all required training and follow related policies and guidance, including mandatory information security training and data compliance training
- To inform IT Services, or the Information Compliance Unit (ICU), of any potential threats to Information Security as soon as possible
- All staff shall retain data in accordance with the Our Data Policy and the provisions of the Data Management Strategy or its successor. Particular consideration should be given to the classification of data classified as confidential or restricted and the consequent access granted to colleagues, students or third parties

7. Implementation and Communication

7.1. This Policy will be communicated to all staff, students and other relevant parties through the University's external web pages, MySurrey, Surrey Net and via internal newsletters.

7.2. The Executive Board will annually review the Policy Objectives and Delivery Parameters .

7.3. New Procedures will be brought to the attention of stakeholders via a range of media, including:

- SurreyAlert
- SurreyNet
- Induction Training
- Other bespoke training

8. Exceptions

The principles of Data Protection and Information Security are underpinned by legislation and the consequences of a serious breach 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 requirements may be subject to a risk assessment and must be authorised in writing by the Chair of Compliance (Data) committee.

Appendix 1 – Performance

Performance target dates, unless otherwise stated, align with the end of the strategy period 2023/24.

- Structured regular management review of conformity to policies and procedures
- Absence of significant data breaches or substantial complaints by Data Subjects which lead to ICO finding against the University
- Maintenance of accreditation of IG Toolkit, PCI-DSS and Cyber Essentials
- Cyber and ICU activities internal audit reports are categorised as effective/satisfactory