Executive Board
23 April 2020
Item 13
20/EXB/055

Data Management Strategy

1 Introduction

1. The University acquires, creates and retains data in a variety of digital and non- digital formats. It also holds Personal Data and Special Category (sensitive) Data about data subjects including patients so must comply with the provisions of current Data Protection Legislation.

2. The University grapples with the challenge of managing its data. There is always a need for more information, insight, analysis, benchmarking and more efficient business processes which requires the effective management and processing of the University's data assets.

3. It recognises that there needs to be a balance between its:

   3.1 Public accountability and transparency in its governance;

   3.2 Compliance with regulatory obligations including the Data Protection Legislation; and

   3.3 Need to protect both the personal and commercially sensitive confidential information it holds.

4. A Data Management strategy is required to ensure that data is collected, created and processed in a compliant manner in the best interests of the wider University, supports its organisational strategy and informs the design and development of its technical architecture and business processes.

2 Scope

This strategy applies to University of Surrey staff, students, agency staff, visitors, contractors and third parties who are processing University data.

3 Aims

The aim of this strategy is to support the overarching Information Assurance Strategy in conjunction with the IT Data Security Strategy so as to enable data planning and governance to effectively manage University data as an asset, ensuring that data is collected, created and processed in a compliant manner that is also in the best interests of the wider University.

4 Roles and Responsibilities

See Appendix 1 for more information about University Data Governance Roles.

5 Data Strategy Guiding Principles & Objectives

This strategy is underpinned by the following 8 guiding principles and the objectives that the University has set:

Principle 1	**Data, in all forms, is recognised as a University asset**
Background	Data is managed as a corporately owned asset with clear governance processes to control its processing and retention.
Objectives	- University data, is managed as an increasingly important corporate asset and potential source of competitive advantage and is better protected and exploited. - There exists a benefit to or link through the use of data and the achievement of the University's goals and strategy. - There is an understanding of data usage, flows against purposes and the data lifecycle is managed. - Accurate management data is provided to enable effective University's decision making. - The IT Data Security Strategy is embedded.

Principle 2	**Data is held in compliance with the University's regulatory obligations including Data Protection Legislation.**
Background	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.
Objectives	- The University is compliant with all current and emerging information compliance rules including the data protection legislation; - Categories of access to data are defined on a least privileged/need to know basis. - Data rights are able to be successfully fulfilled.

Principle 3	**Confidence in the reliability and quality of the data is maintained throughout its lifecycle.**
Background	The University holds timely, accurate and reliable data in order to manage activities and meet internal and external requirements to enable it to demonstrate accountability through accurate reporting.
Objectives	- The University is compliant with the Data Protection Legislation in that the personal data it holds is accurate and that inaccurate data is

	rectified or erased without delay. - Accurate external returns are submitted to ensure maximisation of funding opportunities - The funding requirements for the Office for Students and research grant requirements from private and public funders are met.

Principle 4	**Data will be governed appropriately throughout its lifecycle in relation to its purpose**
Background	Data is assigned to a designated information asset owner (IAO). It must be kept secure and personal data must only be processed under appropriate, usually limited, conditions in compliance with Data Protection Legislation.
Objectives	- The University culture will become more data driven with generally enhanced Data Management capability across the organisation with an increase in the number of data specialists in key areas. - A community of clearly defined Data Management roles has been established and are maintained. - The community of appropriately trained and supported IAOs ensure that enterprise data and other strategically important data held locally is managed for strategic, not local purposes. - The role and responsibilities of the IAOs are defined. - Data will be managed appropriately. - Guidance for IAOs on how to manage the data within their areas has been developed. - Appropriate resourcing, training and organisational conditions are in place to ensure that they can operate effectively. - Gaps in current resource and necessary University support to address them have been identified.

Principle 5	**All data should be identifiable**
Background	Data is identified, findable and managed in a structured manner and labelled and recorded in a consistent and logical fashion.
Objectives	- Data held within University systems and other networked locations has been identified and highlighted where Personal Data is stored. - Data that the University holds and its use is automatically identified and discoverable. - There is an understanding of data usage, flows against purposes and the data lifecycle is managed. - Interfaces, data flows, data modelling of systems and architecture support identification and management of data - Data will be classified according to the data risk categories. - The management of data retention and governance is automated where appropriate. - Data is disposed of/archived appropriately.

Principle 6	**All data processing changes are subject to control**
Background	Implementing and codifying the measures to be taken when making changes to the processing of data is vital to ensuring that the significant remedial work

	required to establish the right conditions for success does not have to be repeated in the future. Change control is a vital component of effective Data Management.
Objectives	- The University's plans for the development of its technical architecture is driven by the Information Assurance and IT Data Security strategies and any changes will be properly controlled to reduce data compliance risk. - The criteria for managing and risk assessing change to the way data is handled and processed is developed and embedded. - Changes to the processing of way personal data will follow the Privacy Impact Assessment/Data Protection Impact Assessment process.

Principle 7	**All data will be ultimately governed by the Executive Board with guidance from DISC**
Background	Governance structures for data are now in place with an appropriate Data Information Security Steering committee (DISC).
Objectives	- DISC will oversee the design and implementation of the overarching Information Assurance strategy, this strategy, IT Data Security Strategy and any subsequent Data Management

Principle 8	**The level of rigour is proportionate to the risk**
Background	The University's Information Assurance Strategy will inform data requirements. This Data Management Strategy will ensure that the data collection, processing and sharing meets the needs of the University and effectively supports its mission.
Objectives	- Data risk categories are clearly defined. - Data is automatically and appropriately classified, tagged and protected according to its risk category.

6 Relevant law, key policies & guidance

1. Glossary of Terms at Appendix 2.
2. Data Protection Legislation (currently the GDPR and Data Protection Act 2018)
3. Information Assurance Strategy
4. Data Protection Policy
5. Information Governance Policy
6. IT Data Security Strategy
7. Information Security Policy

8. IT Acceptable Use policy

9. Monitoring and Filtering Policy

10. HR policies at: https://surreynet.surrey.ac.uk/hr-policies-and-forms

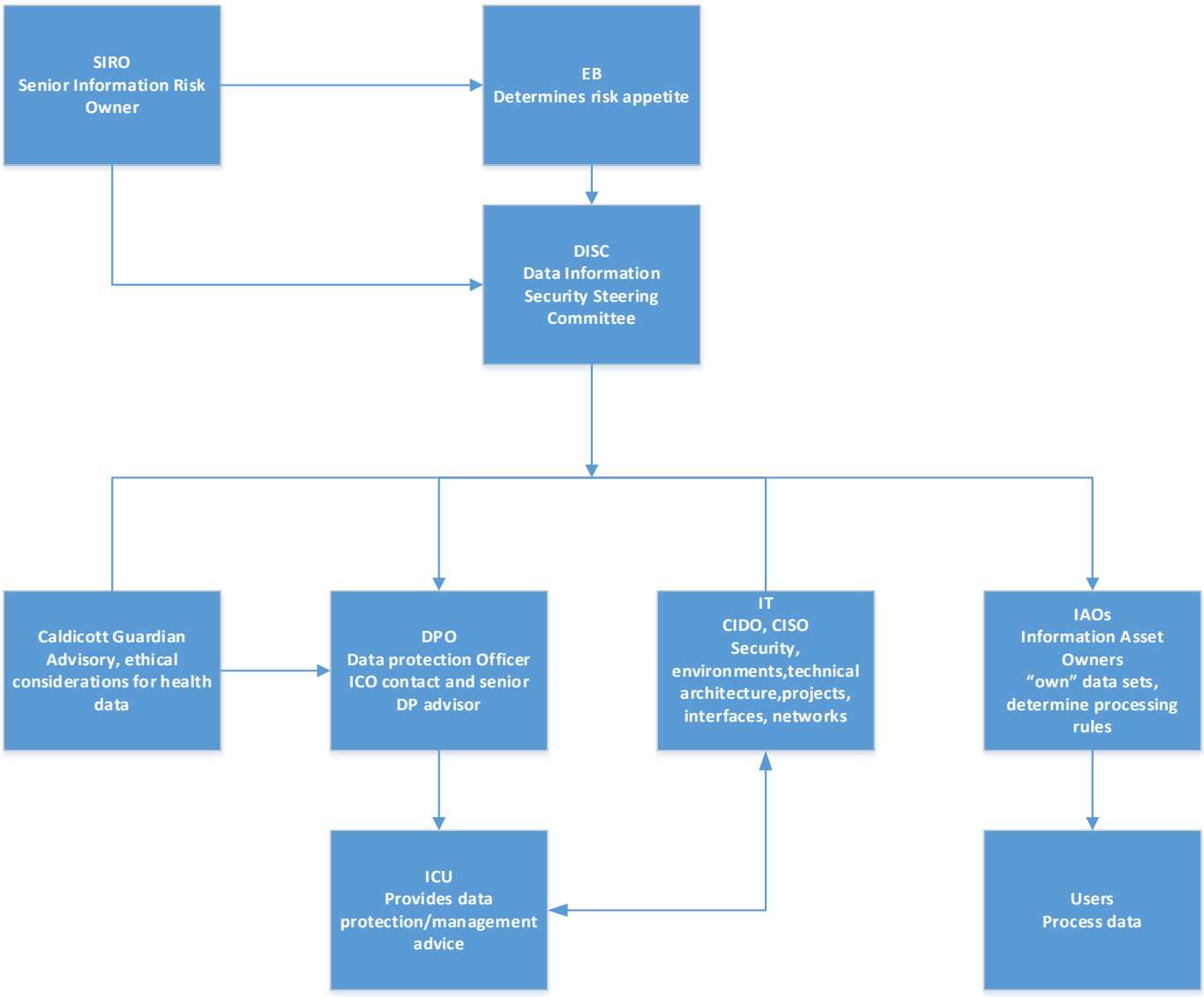
11. Other relevant policies at: https://www.surrey.ac.uk/about/policies

12. Key guidance can be found at: https://surreynet.surrey.ac.uk/staff-services/information-privacy-security/information-management-toolkit

7 Version Control

Version	Author	Changes	Date
1.1	J. Newby	First draft	December 2016
1.2	J. Newby	Incorporating contributions from S. Mereweather (sections 4 and 5)	December 2016
1.3	J. Newby	Further changes to section 3	January 2017
1.4	J. Newby	Addition of glossary	January 2017
1.5	J.Newby	Incorporating ITS resource requirements in Resource and Readiness Assessment section	March 2017
1.6	S.Mereweather, F.Berkhout, E.Donald	Incorporating updates post GDPR implementation and roles	October 2019
1.7	S. Litchfield F. Berkhout	Roles and terms of reference	January 2020

Appendix 1 - Data Community –Roles & Responsibilities



Senior Information Risk Officer

1. Main purpose of the role:

To act as the senior University officer taking responsibility for the institution's information risk policy and approach. To act as an advocate for information security and risk management on the University's Executive Board and to provide advice, guidance and assurances to the Vice-Chancellor, EB and DISSC on information risk. The role will include the supervision of the University's appointed Data Protection Officer and the community of Information Asset Owners (IAOs).

2. **Main Duties:**

(a) To create and authorise, with support from the DPO and IAOs, the University's information management policies and processes.

(b) To ensure that the University has in place, a fully tested and robust process for responding to information security or processing compliance breaches and to report any incidents to ISAGG and EB.

(c) To ensure that information risks are appropriately understood and that proportionate measures to mitigate them are incorporated into University strategies and plans. This will include strategic projects and larger IT projects, especially those involving changes to data holding enterprise systems.

Data Information Security Steering Committee:

1. **Main purpose:**

(a) The Data and Information Security Steering Committee (DISC) exists to oversee, on behalf of Executive Board (EB), the development, approval, implementation and review of Information Security and data management strategies as well as organisational and technical measures to manage, and protect the University's key corporate data assets, and to ensure that the University has the necessary data security capability in place to meet its statutory and regulatory obligations as well as deliver its strategic objectives. As such it shall:

Data Protection Officer

1. **Main purpose of the role:** To act as the University's senior advisor and assessor on Data Protection and GDPR issues, manager of the ICU team and the main point of liaison for external organisations and regulators for issues relating to Data Protection and the GDPR. To monitor compliance with data protection requirements and ensure that the University is appropriately prepared to meet its DPA and GDPR obligations.

2. **Main duties:**

(a) To inform and advise the University and its employees about their obligations to comply with the GDPR and other data protection requirements and to provide training.

(b) To monitor compliance with data protection requirements and report any findings to the SIRO and DISSC.

(c) To support the SIRO in developing and implementing appropriate risk management policies and procedures.

(d) To act as first point of contact for regulatory authorities and other external organisations for all enquiries relating to data protection.

(e) To act as the first point of contact for data subjects and to oversee any data subject access requests and complaints.

Caldicott Guardian

1. Main purpose of the role:

To act as the guardian of data subjects' interests and the "conscience" of the University in relation to the retention and processing of health and patient data. The post holder will act as an advisor to the University and the staff involved in processing health and patient data and will liaise closely with the SIRO and DPO on health and patient related data matters.

2. Main duties:

(a) To respond to researcher questions and requests for advice about the processing of health and social care data.

(b) To provide guidance to those dealing with patient data on appropriate processing arrangements consistent with the Caldicott principles.

(c) Advise the SIRO, DPO and Executive Board on the ethical implications of their data processing, management and security policies and procedure.

Chief Information and Digital Officer

1. Main purpose and duties of the role:

(a) Effective management and security of IT resources, for example, infrastructure and equipment.

(b) The formulation and implementation of IT related policies and the creation of supporting procedures, and ensuring these are embedded within the service developing, implementing and managing robust IT security arrangements in line with best industry practice.

(c) Developing and implementing a robust IT Business Continuity Plan.

(d) Ensuring the maintenance of all firewalls and secure access servers are in place at all times.

Chief Information Security Officer

1. **Main purpose and duties of the role:**

(a) Act as the IAO for the IT infrastructure with specific accountability for computer and telephone equipment and services that are operated by the University's corporate and clinical work force.

(b) Maintain a lead role by identifying risks, maintaining risk treatment plans and providing written or oral summaries on residual levels of risk and the status of corrective actions to IT management or the appropriate University oversight group.

(c) Conduct investigation, analysis and review following security control breaches, and manage security incidents. Recommend appropriate control improvements, involving other professionals as required.

(d) Monitor the application and compliance of security operations procedures, and report on non-compliance.

Information Asset Owners

1. **Main purpose and responsibilities:**

(a) Leading and promoting a culture that values and protects data;

(b) Knowing what data you manage and why;

(c) Knowing who has access to the data whilst you are responsible for it and why;

(d) Understanding and addressing risks to the data whilst you are responsible for it;

(e) Ensuring the data is used efficiently and effectively to achieve your department's and the University's vision;

(f) Acting as the nominated "owner" of an assigned data asset(s) on behalf of your department and the University;

(g) Ensuring that the data is processed for purposes consistent with the strategic objectives of your department;

(h) Determining how the data is collected, processed, retained and disposed of within your department in line with the overarching framework of the University; and

(i) Working with other IAOs to collaborate on internal data sharing arrangements.

2. Main duties:

(a) Review, at least annually (more frequently for higher risk information or assets with greater sensitivity), the data processing purposes for the data to ensure that it is kept up to date;

(b) Ensure that all University data processing and information security policies and any University best practice guidance are followed;

(c) Risk assess (if required) and log any changes to the processing of the data;

(d) Report any known, suspected or potential data security or processing breaches to the Data Protection Officer in consultation with your Line Manager, where appropriate;

(e) Report regularly on information risk in your department and on any significant new processing changes or risks to the Data Protection Officer in consultation with your Line Manager, where appropriate;

(f) To attend available training;

(g) Keep a log of any new requests for access to the data;

Work closely with other IAOs within the organisation to ensure that there remains a clear and documented framework of data asset ownership and a clear understanding of responsibilities and accountabilities – particularly in cases where data sets are transferred between IAOs; and Provide an annual assurance to the University's Data Protection Officer that the data for which you are responsible is appropriately secure and has been used only for its stated purpose.

User

1. Responsibilities

(a) Adhere to the principles of this strategy and relevant legislation, supporting policies, procedures and guidance.

(b) To only access information where they have a legitimate access right.

Appendix 2– Glossary of Terms

Data or Information Assets: Sets of data held created and maintained by Information Asset Owners as part of their responsibility to keep records of the data they hold.

Data Management: The development and execution of architectures, policies, practices and procedures in order to manage the information lifecycle needs of an enterprise in an effective manner.

Data Protection Legislation: means (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 1998 (to the extent that it remains in force), the Data Protection Act 2018, the GDPR and all legislation enacted in the UK in respect of the protection of Personal Data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time;

Data Protection Officer: Named individual responsible for providing DPA advice and for acting as main liaison point with regulators.

Personal Data: Data which relates to a living individual who can be identified from the data, or from that data in combination with other data held by an organisation

Senior Information Risk Owner (SIRO): Senior officer responsible to EB for the management of DPA risk and a key advisor to the Executive Board on data compliance and risk issues.

Special Category (sensitive) Data: Data which relates to a living individual of a sensitive nature, particularly concerning their racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offence.