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 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 dataassets.

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.

A Data Managementstrategy 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 and 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. - Breaches are dealt with in an effective and timely fashion to ensure regulatory obligations are met -

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 maximization of funding opportunities

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	- 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. - Records, and the data in them, can be efficiently retrieved by those with a legitimate right of access for as long as the records are held by the University - 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 application of information governance procedures are regularly monitored against agreed indicators and action taken to improve standards as necessary. - Changes to the processing of personal data will follow the Data Protection Impact Assessment process.

Principle 7	**All data will be ultimately governed by the Executive Board with guidance from the designated overseeing committee**
Background	Governance structures for data are now in place with an appropriate designated overseeing committee.
Objectives	- The designated overseeing committee 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 rigor 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. - Data protection risks are managed appropriately.

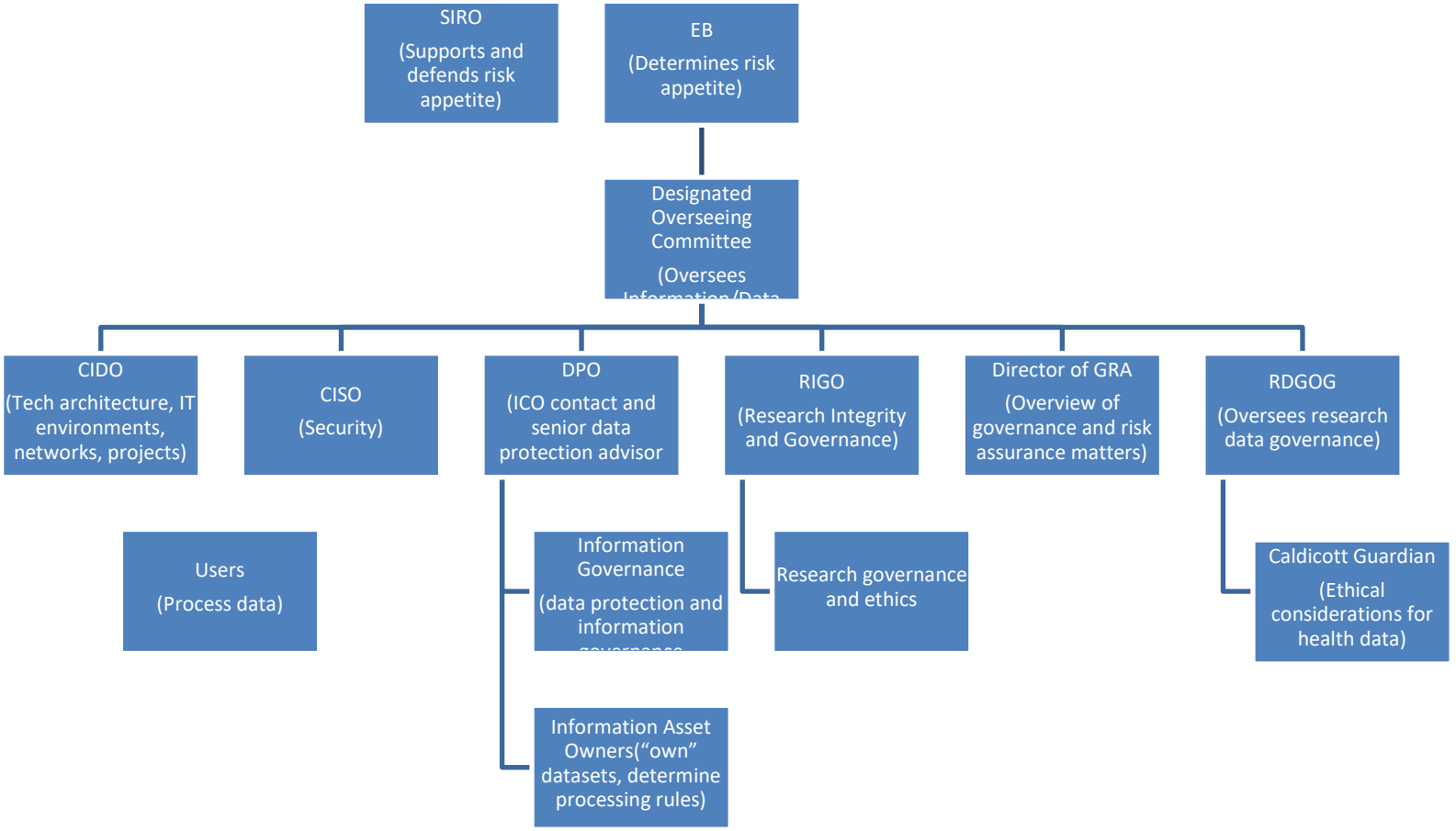
6 Relevant law, key policies & guidance

1. Glossary of Terms at Appendix 3.
2. Data Protection Legislation (currently the GDPR, UK GDPR, Data Protection Act 2018 and applicable e-privacy legislation)
3. Information Assurance Strategy
4. Data Protection Policy
5. Information Governance Guidelines
6. Information Security Policy
7. IT Acceptable Use policy
8. Monitoring and Filtering Policy
9. HR policies at: https://surreynet.surrey.ac.uk/hr-policies-and-forms
10. Other relevant policies at: https://www.surrey.ac.uk/about/policies
11. 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
1.8	F. Berkhout S. Mereweather	Inclusion of aspects required by DSP Toolkit/ Confidential Research Data governance	June 2021

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 the Designated Overseeing Committee 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.

Designated Overseeing Committee:

1. **Main purpose:**

   (a) The Designated Overseeing Committee 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.

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 the Designated Overseeing Committee.

(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 alltimes.

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 Line Managers, where appropriate;

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

(f) To attend available training;

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

(h) 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;

(i) In consultation with HoD, provide an annual assurance to the University's DPO 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– Data Management Strategy Delivery

Principle 1	Data, in all forms, is recognised as a University asset	
Objective	**Action**	**Planned outcome**
There exists a benefit to or link through the use of data and the achievement of the University's goals and strategy	The University has clearly defined goals and Strategy and has identified key data requirements and assurance arrangements	- Approved strategies - Formally document a GDPR compliance plan, including an element of testing and audits of key risk areas
	Provide guidance regarding the interpretation of the University's Strategy and goals in terms of data management.	- Check that Guidance/ Commitment statement reflects the DMS and other University strategy - Guidance to be written and disseminated to IAOs
	Ensure project and procurement processes include data related gateways such as DPIA, data models etc	- University project pathway incorporates required documentation (DPIA, Vendor Management etc) - Project staff have understanding of gateway requirements
	Understand the University's goals and strategy when using data or initiating projects and have guidance available	- Project processes include reference to University goals/values/strategy
There is an understanding of data usage, flows against purposes, and the data lifecycle is managed	Technical advantages of the University's privacy management system are fully exploited with data assets, flows, DPIA's and breaches managed within the system.	- IAOs have sufficient knowledge and guidance through best practice guidelines and training to use the system appropriately Privacy management software purchased and implemented: **(a)** Data assets are fully mapped within the system **(b)** DPIAs are completed within the system and a connection exists between data assets and DPIAs **(c)** Personal Data Breaches are managed through the system **(d)** Data subject rights requests are managed through the system
	Architecture diagrams for network produced (over time) to a consistent template, with responsibilities agreed for maintenance of these technical documents	- Templates for network and system diagrams to be approved by designated overseeing committee - Architecture documents available for validation by designated overseeing committee and maintained as appropriate by ITS or devolved system owners

Accurate management data is provided to enable effective University decision making	DPIA process identifies risks which are reflected in the University's risk registers as appropriate	- Level 1 and 2 risk registers reflect accurate data management risks
The IT Data Security Strategy is embedded	IT Data Security Strategy is complete, approved by the relevant committee and clear measures for implementation are created	- IT Data Security Strategy is approved by the appropriate committee and implementation is reviewed as appropriate

Principle 2	Data is held in compliance with the University's regulatory obligations including Data Protection Legislation	
Objective	**Action**	**Planned outcome**
The University is compliant with all current and emerging information compliance rules including the GDPR, UK GDPR and DPA 2018 and e-privacy legislation	All staff are aware of the principles of data protection legislation and how this relates to their information management responsibilities	- Review areas of e-learning non completion - Creation and management of generic and role specific training and guidance. Where significant new systems are introduces, tailored training are in place to guide staff through the process of change - Establish process to roll out mandatory refresher training
	Data Protection related policies to be kept up to date	- Data protection policy and data management strategy published on website up to date
	Provide guidance for compliance with the Data Protection Privacy Principles (and the Caldicott Principles when processing health data.)	- Appropriate guidance for target audience to be written and disseminated to IAOs and research community
	Staff adhere to University policies in particular the Data Protection Policy, relating to data protection, confidentiality and the security of personal information	- Creation and management of generic and role specific training and guidance. - Collation of known data processor relationships into central register - Identify contracts pre-dating GDPR and update, including updating processor agreements where data is shared with EU to contain EU clauses - Identify current use of RCGP datasets - Bring Clinical Informatics NHS data governance process into University owned Highly Confidential Research Data governance process.

	Annual reviews of departmental maturity for compliance with data protection policies and procedures ensure that all areas of the University continue to consistently adhere to data protection principles	- Annual self assessment assurance process created and rolled out to all departments
	Attend role appropriate training	- All new IAOs to attend IAO training - All staff who handle personal data to attend DP training - All staff to complete e-learning module with appropriate refresher cycle
Categories of access to data are defined on a least privileged/need to know basis	Classifications for access permissions are in place	- Security Classification labels are agreed and embedded within data handling systems such as O365 - Guidance for use of classification labels is available
	All University systems have security arrangements in place to ensure appropriate levels of access to data by individual Users	- outcomes of IT Security Strategy are in place - role based access requirements are defined and in place
	Advice and guidance are provided to Users on access permissions	- IT Security and devolved system owners provide guidance to users on access permissions and access to data
	Users are aware of and adhere to IT access policies and ICU advice and best practice guidance.	- Information Governance to ensure relevant policies are available to all staff and are disseminated in the best way for different groups to find relevant guidance and advice - Awareness of policies to be included in Annual self assessment assurance process created and rolled out to all departments
Data rights are able to be successfully fulfilled.	Data subject rights are effectively managed, and requests responded to within appropriate timescales	- Clearer privacy notices in place, combining relevant areas together (ie student support) - simplifying privacy notices for vulnerable groups - University systems holding personal data can fulfil a request to be forgotten - OneTrust can provide relevant information about DP legislation in countries of origin for staff/students - Processes in place to manage requests within the Privacy Management System
	Staff recognize when a right is being exercised and take appropriate action in adherence to University policies and guidance	- Info Gov to ensure guidance available to all staff; included in relevant training
	Maintenance of appropriate documentation to assist with responding to data subject rights request	- IAO “checklist” documentation and asset register maintained to identify location and flow of data

Breaches are dealt with in an effective and timely fashion to ensure regulatory obligations are met.	A process is in place to identify and respond to Personal data breaches and security incidents and breaches	- Processes to manage breaches include all main stakeholders - Processes are in place to manage breaches - All requests are handled within appropriate timescales
	The University's privacy software has capability to successfully fulfill rights	- Process is in place to manage breaches through the privacy management system
	The risk of information security breaches are minimized through the implementation of technical and organisational measures	- outcomes of IT Security Strategy are in place
	Lessons learnt procedures are in place for breaches	- Analysis of breaches is possible through privacy management system - Reporting of breaches through appropriate committee
The University is compliant with data protection legislation in that the personal data it holds is accurate and inaccurate data is rectified or erased without delay.	Systems support erasure and amendments to data	- Purchase of systems includes assessment of erasure and amendment capabilities
	There is an understanding of data flows so that amendments and erasure of data within a system does not inadvertently affect the integrity of data within dependent systems	- IT architecture information and ROPA will contain accurate information regarding data flows

Principle 3	Confidence in the reliability and quality of the data is maintained throughout its lifecycle	
Objective	**Action**	**Planned outcome**
The University is compliant with data protection legislation in that the personal data it holds is accurate and inaccurate data is rectified or erased without delay.	Systems support erasure and amendments to data	- Purchase of systems includes assessment of erasure and amendment capabilities
	There is an understanding of data flows so that amendments and erasure of data within a system does not inadvertently affect the integrity of data within dependent systems	- IT architecture information and ROPA will contain accurate information regarding data flows

Accurate external returns are submitted to ensure maximization of funding opportunities and research grant requirements from private and public funders are met	The quality of data submitted to the Higher Education Statistics Agency (HESA), Office for Students, Research England, and other funding bodies is assured.	- Systems support efficient extraction and analysis of statutory returns - Relevant staff are able to ensure efficient extraction and analysis of data from systems - Provision of accurate data to private and public funders
	Records are secure from unauthorized or inadvertent alteration or erasure.	- Access is controlled through role-based permissions - Systems will include audit trails to track all use and changes as appropriate - Records will be held in a robust format which remains accessible and readable for as long as required

Principle 4	Data will be governed appropriately throughout its lifecycle in relation to its purpose	
Objective	**Action**	**Planned outcome**
A community of clearly defined Data Management roles has been established and are maintained	Appointments to statutory roles are made and Information Asset owners/data champions in place across the University	- Take measures to manage IAO gaps, including reporting to EB as required
	Processes are in place to develop the IAO community on an ongoing basis and ensure they are supported	- IAOs attend Info Gov led regular sessions to address areas of knowledge relevant to them and to support one another
The community of IAOs ensure that enterprise data and other strategically important data held locally is managed for strategic and not local purposes	University project processes ensure IAO involvement so that review of existing data forms part of projects and data is not recreated unnecessarily	- Involvement of relevant IAOs in appropriate projects
	Enterprise data and other strategically important data held locally is managed for strategic purposes	- IAOs are aware of the purposes for which their data is collected and maintained and record this in an effective data management system
	All records (whether on network storage, cloud provision, databases etc) are stored in a way that supports their retrieval	- Purchase of systems includes assessment of storage and retrieval capabilities via tender and/or DPIA questions - Guidance is available to users of University provided storage locations to ensure they effectively store and manage their data
The role and responsibilities of the IAOs are defined	Roles and Responsibilities of IAOs are defined within the Data Management Strategy	- The role of IAO is defined and provided to all IAOs

Data will be managed appropriately	Records are secure from unauthorized or inadvertent alteration or erasure.	- Access is controlled through role-based permissions - Systems will include audit trails to track all use and changes as appropriate - Records will be held in a robust format which remains accessible and readable for as long as required
	The application of information governance procedures are regularly monitored against agreed indicators and action taken to improve standards as necessary	- Annual self assessment assurance process created and rolled out to all departments
	Retention periods are applied by automated means wherever this is supported by the system in which they reside	- All O365 filestores include automated retention and disposal of records in line with published retention schedules
	The management of data retention and governance will be automated wherever possible	- Assign responsibility for retention labelling in O365 and plan for addressing retention labelling - Office 365 capability for automated retention and disposal is used to its fullest potential -
	Data will be disposed of appropriately	- Retention schedule gap analysis completion - Update and publish overarching retention schedules - Clear strategies for data storage and archiving from systems are in place with appropriate retrieval and security - All IAOs are aware of appropriate retention periods for data under their control and apply them appropriately - All IAOs are aware of how data under their control should be disposed of and are able to dispose of data appropriately
	The University has in place appropriate security arrangements to ensure that data is held securely, is protected from unauthorized access from outside the University and is accessed appropriately from within the University	- IT Security policies are in place and outcomes of these are in place - The University has met appropriate security accreditations - IT Security policies are in place and outcomes of these are in place - The University has met appropriate security accreditations
	Retention periods are applied by automated means wherever this is supported by the system in which they reside	- Other systems holding large amounts of data will explore the possibility of automated retention and disposal of records

		- New systems being procured will seek to allow for automated retention and disposal of records.
Records, and the data in them can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held by the University	systems support efficient storage and retrieval of records and data stored within them	- Purchase of systems includes assessment of storage and retrieval capabilities via tender and/or DPIA questions
	All records (whether on network storage, cloud provision, databases etc) are stored in a way that supports their retrieval	- Guidance is available to users of University provided storage locations to ensure they effectively store and manage their data
Guidance for IAOs on how to manage the data within their areas has been developed	IAOs are aware of retention requirements relevant to them and can disseminate knowledge to ensure that retention periods are adhered to by all teams.	- IAOs are trained in the requirements of retention schedules that apply to them
	IAOs are aware of data classification labels and can apply them appropriate to their records held electronically and in other formats	- IAOs are trained in the requirements of data classification -
	IAOs are aware of best practice for handling data and records and can apply this to the data and information held in their areas	- IAOs are trained in basic information governance matters around storage of records and data

Principle 5	All data should be identifiable	
Objective	**Action**	**Planned outcome**
Data held within University systems and other networked locations has been identified and highlighted where personal data is stored	Data will be recorded alongside the purposes for which it is used	- Datasets, processing activities, data sharing, risks and retention will be recorded to form the ROPA in a fully implemented asset management system - IAOs have sufficient knowledge and training to keep data updated in the ROPA
Data that the University holds, and its use is automatically identified and discoverable	Technologies will be in place to ensure data is identifiable and discoverable	- All data held electronically will be discoverable via O365 capabilities - Technologies will be in place to ensure data shared outside the University can be identified
There is an understanding of data usage, flows against purposes and the data lifecycle is managed	All data held on University systems and networked drives is identified and data flows mapped	- Knowledge of data flows is recorded and accessible to appropriate members of the University

Interfaces, data flows, data modelling of systems and architecture support identification and management of data	The University has a fully mapped architecture and an understanding of data flows	- As systems are implemented or upgraded, sufficient information is mapped to contribute towards full identification of the supporting architecture, including data flows via interfaces and other forms of data sharing
Data will be classified according to the data risk categories	Effective data classifications will be established and clearly explained to the University	- Data Classifications available and applied systematically where possible
The management of data retention and governance is automated where appropriate	There are consistent and documented retention and disposal procedures which identify records that must be retained permanently or temporarily due to legal requirements or to meet operational need and which provide for the routine and timely disposal of documents which have reached the end of their retention period.	- Published retention schedules are up to date and align with retention periods recorded in the ROPA for personal data. The University Archive has identified records needed for permanent preservation. - Any amalgamation of retention periods to meet the needs of particular systems is based on the published retention schedules and align with their requirements
	IAOs are aware of retention requirements relevant to them and can disseminate knowledge to ensure that retention periods are adhered to by all teams.	- IAOs are trained in the requirements of retention schedules that apply to them
	Retention periods are applied by automated means wherever this is supported by the system in which they reside	- All O365 filestores include automated retention and disposal of records in line with published retention schedules
	There are consistent and documented retention and disposal procedures which identify records that must be retained permanently or temporarily due to legal requirements or to meet operational need and which provide for the routine and timely disposal of documents which have reached the end of their retention period.	- Any amalgamation of retention periods to meet the needs of particular systems is based on the published retention schedules and align with their requirements
Data is disposed of appropriately	Data with long term historical interest is identified and transferred to the Archive at the appropriate time	- Retention schedules will include disposition details to show when records should be sent to the archive - IAOs will transfer records to the archive at the appropriate time
	All data has an appropriate retention period assigned to it and is disposed of at the appropriate time	- IAOs are aware of the retention periods for their data and dispose of it appropriately

	Confidential destruction methods are used where appropriate	- Shredding is available for confidential paper records, and secure methods of disposal for hardware.
	All data is appropriately classified and disposed of using the method appropriate to that classification	- Data Classifications are defined and applied systematically

Principle 6	All data processing changes are subject to control	
Objective	**Action**	**Planned outcome**
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.	Development of operational technologies and application development follow the principles in the Information Assurance Strategy, Data Management Strategy, IT Security strategies and other relevant strategies that relate to these	- Staff responsible for application development and development of operational technologies as well as all project management and business analysis staff are aware of the relevant strategies and how they relate to their sphere of operations
	The criteria for managing and risk assessing changes to the way data is handled and processed are developed and embedded in relevant project and procurement processes	- Heads of Technologies and project managers/leads in the University are aware of the DPIA process and include completion of DPIA as a required step where appropriate
The application of information governance procedures are regularly monitored against agreed indicators and action taken to improve standards as necessary	Annual self assessment assurance process created and rolled out to all departments	- Annual self assessment assurance process in use as regular means of assessing maturity throughout professional and academic departments.
Changes to the way personal data is processed will follow the Data Protection Impact Assessment process	The DPIA process is regularly included in change projects and procurement processes.	- All IAOs are aware of the process and able to support completion of DPIA - Info Gov train on regular basis on how to complete DPIAs
	Outstanding risks following completion of DPIA will be followed up and reviewed as appropriate	- All DPIAs will be reviewed at an appropriate time period following their approval.

Principle 7	All data will be ultimately governed by the Executive Board with guidance from the designated overseeing committee	
The Designated overseeing committee will oversee the design and implementation of the overarching Information Assurance strategy and supporting strategies including IT Security strategies, Data Management strategy and any underlying policies	IT Security strategies, Data Management strategy and any underlying polices are scrutinized and signed off by the designated overseeing committee	- All relevant strategies and policies brought to designated overseeing committee for approval
	The designated overseeing committee will ensure the completion of any outcomes from IT Security strategies, Data Management strategy and any underlying policies to ensure delivery of those strategies and policies	- designated overseeing committee reviews completion of outcome tasks from relevant strategies

Principle 8	The level of rigor is proportionate to the risk	
Data risk categories are clearly defined	Data risk classification is defined and in place	- Classification of risk is defined within privacy management software and understood by relevant users - Risks are reported appropriately
Data is automatically and appropriate classified, tagged and protected according to its risk category	Data risk classification is automated and rolled out across University data stores wherever possible	- Data Classifications are defined and applied systematically
Data Protection risks are managed appropriately	Data Protection Impact Assessment process identifies residual privacy risks	- Document where LIA is appropriate to use - Identify where LIA are required, where they have been completed and where outstanding - Review completed DPIAs to assess where LIA is required and plan for their completion - Complete outstanding LIAs - Complete LIA for processing of children's data - work with IT Security to establish Info Gov aspects of vendor management process and ensure it fully addresses GDPR requirements - Data handling classification is defined, included in relevant strategy and embedded in relevant systems such as O365. Where data classifications are not embedded, IAOs and other relevant information handlers are aware of them and how to use them.

	SIRO signs off on any unmitigated residual risks	- All DPIAs document residual risks, with SIRO sign off on high risks unmitigated residual risk

Appendix 3 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 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.