UNIVERSITY OF SURREY

Data Management Procedure	
Enabling Policy Statement	Our Data
Executive Owner	Chief Operating Officer
Approval Route	Compliance (Data) Committee
Is the procedure for internal use only	For internal use but it is disclosable
Associated Policy Statements	
Authorised Owner	University Secretary and General Counsel (University SIRO)
Authorised Co-ordinator	University Data Protection Officer
Effective Date	02/12/2024
Date for full review	02/12/2027
Sub-documentation	Information Sharing Procedure

Approval History

Version	Reason for review	Approval route	Date
1.0	This is the first Data Management Procedure. Previously there was a data management strategy and many of the key points of the strategy are now covered by the Our Data Policy Statement. This procedure provides high level instructions to staff about their obligations and signposts them to wider guidance.	Compliance (Data) Committee	12/10/2023
2.0	Various amendments following first year of operation.	Compliance (Data) Committee	02/12/2024

1. Purpose

This procedure provides you with the high level steps required when dealing with information, including personal data, on behalf of the University. It forms part of the wider Information Governance framework and should therefore be read in conjunction with the Our Data Policy Statement and with the toolkits, guidance and training as directed via the links included throughout. Adherence to this procedure supports the University in complying with its obligations under UK General Data Protection Regulation 2016/679 (UKGDPR) and Data Protection Act 2018.

2. Scope and Exceptions to the Procedure

This procedure is grouped into a number of categories which reflect toolkits and guidance themes on the Information Governance SurreyNet pages, including -

- information management (classification; records storage, retention and disposal);
- information privacy (data protection principles, data protection impact assessments and data breaches);
- information requests (data subject access requests, freedom of information requests, police requests).

Although information security is one of the data protection principles, this procedure does not cover the associated technical facilitation (i.e. pertaining to IT systems and devices), or the procedures governing how University systems can be accessed and utilised. These are managed by the Information Security team.

All staff are required to comply with this procedure, including Researchers in the normal course of their duties, however, there are some specific conditions which apply to research activity. These will be covered separately and are not included in this procedure.

This procedure covers those activities listed above but cannot detail every eventuality that might arise. Nor does it seek to provide instruction on every aspect of information governance or data protection as this would be over-whelming. In support of this procedure and your understanding, further guidance is provided on the Information Governance pages on SurreyNet. The University's Data Protection Officer and the Information Governance team are also available to provide further advice and assistance. They can be contacted at dataprotection@surrey.ac.uk

This Procedure applies to -

- people: all staff and colleagues who have a University of Surrey account;
- data: all data, including personal data collected, held or processed by or on behalf of the University whether digitally or in hard copy;
- systems and security: the equipment, systems, credentials, etc., that are used to access and safeguard data, including personal data.

3. Definitions and Terminology

Data Breach: 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.

Data Subject: A natural living person whose personal data is processed by the University of Surrey or by an appointed Processor.

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: A 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 Asset Register: A register created and maintained by Information Asset Owners to reflect how personal data is processed within their agreed remit.

Information Classification: The process of organising data by relevant categories so that it may be used and protected more efficiently.

Personal data: Any information that directly or indirectly relates to an identified or identifiable natural living individual.

Processing: Any operation or set of operations which is performed on data, including personal data (collecting, storing, amending, sharing, deleting, etc.).

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.

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.

4. Procedural Principles

4.1 All records that sit under the Procedure of Policies and Procedures Framework (POPP) should follow the requirements of that framework. This will include policies, procedures, codes of practice and other guidance documents

4.2 Your Obligations

Everyone

As outlined in the Our Data Policy Statement, **anyone who processes personal data within or on behalf of the University must comply with the principles of data protection**. Section 23 of the Staff Handbook, which forms part of the terms and conditions of employment, also states that **all staff are required to comply with applicable data protection legislation**.

This means that you are required to acquaint yourself with the Our Data Policy Statement; this Procedure; and the related guidance as outlined below, and to complete any related training mandated from time to time.

Everyone is required to follow any instructions, advice and guidance provided by the University's Data Protection Officer and the Information Governance team. In the same vein you are required to work in collaboration with the University's Information Asset Owners to ensure data protection remains embedded in your working practices.

Information Asset Owners

Information Asset Owners (IAOs) are members of staff who are responsible for ensuring that specific information assets are handled and managed appropriately. Their role is to understand what information is held, what is added and what is removed, how information is shared and who has access to the information and why. The key activities that IAOs perform are required by data protection legislation and include -

- Creating and maintaining Information Asset Registers for the data assets they "own". This enables the University to hold appropriate Records of Processing.
- Ensuring privacy notices are created and maintained.
- Reporting data breaches (although anyone can report a breach, IAOs should ensure that breaches pertaining to their own data assets are reported appropriately).
- Championing a culture of good practice in relation to data management and privacy.

4.3 Information Management

Information is a key asset of the University which needs to be organised effectively, held securely and processed in a compliant manner. To be a reliable asset means it needs to be accurate, up to date and retrievable. Information also has a life-cycle and retention plans should be put in place to ensure it is not held for longer than necessary and is disposed of in an appropriate manner.

Information Classification

In order to promote good practice for the handling of information, the University has adopted an information classification scheme. The classification scheme will help the University to protect information from being compromised, purposely or not; protect the interests of data subjects; meet its compliance obligations; and encourage good information management practice. All information will carry a security classification whether physically marked or not. It is important that you understand which classification applies to your information/documents so that it is stored and processed appropriately and the risk of data breach is minimised.

What you need to do

- It is recommended that you mark or label your files, documents or sets of data with the appropriate classification from the outset, so that it is clear whether any special management or technical protections have been applied to it.
- In any event, the Information Asset Owner must ensure the record of processing includes the appropriate classification.
- Where you are unsure of the classification of your information, you should consider it confidential until confirmed otherwise.

Records Storage, Retention and Disposal

Information is a key asset which must be managed appropriately through out its life-cycle from collection or creation through to disposal, to ensure security and availability, and to enable compliance with data protection legislation. Information which is not managed properly can create an administrative burden and become a compliance liability, exposing the University to the possibility of legislative penalties.

The University has adopted the JISC standard retention schedules which can be found here. Where information is not covered by the JISC schedules, a local process must be put in place.

The University has limited space which can be used for the storage of records that are required by law to be held for a long time; these stores are **not** for short term storage, overflow purposes or for information which needs to be referred to on a regular basis. The Information Governance team manages the store which is located at Manor Park.

What you need to do

- Understand the security classification of the information and ensure it is marked and stored appropriately.
- Store information on University approved systems only.
- Use logical and consistent naming conventions for folders, files and documents.
- Use version controls, preferably system applied (e.g. via a collaboration tool such as SharePoint) or manually applied using consistent sequential numbering
- Keep paper documents in a similarly logical and consistent manner, ensuring they are stored according to their security classification.
- Identify and apply the appropriate retention period to your information as defined in the JISC retention periods or your locally approved process
- Create an alert process for review and disposal, either via digital means (e.g. on SharePoint) or by manual process (ensuring this will be readily available, keeping in mind this might be several years in the future)
- Dispose of records in an appropriately secure manner
- If you are required to store information for an extended period and want to make use of the University store, you must complete a transfer form and return it to dataprotection@surrey.ac.uk who will manage the process.

4.4 Information Privacy and Information Sharing

Privacy principles and conditions of processing

Personal data’ means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, by that information. Special category is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person.

All personal data must be handled in compliance with the data protection principles and conditions of processing, and must comply with the specific conditions applicable to special category data BEFORE it can be processed.

What you need to do

- Be aware of the principles of the UK GDPR and Data Protection Act 2018.
- Ensure individuals are made aware of how you will use their personal data by providing them with a privacy notice.

- Ensure you understand the lawful purpose for processing the personal data you are handling and that this is recorded in your record of processing.
- Do **not** process special category personal data unless it meets the specific conditions set out under UK GDPR.

.2 Information Sharing

In order to support the University in complying with its legal obligations, as well being aware of the requirements of the UK GDPR and the Data Protection Act 2018, staff should understand the general principles around how to share information appropriately in their daily activities. Please refer to the Information Sharing Procedure which provides more detail.

.6 Email Auto-Forwarding

If you deal with personal data in your emails, or if there is any possibility that you will receive emails containing personal data, you **MUST NOT** set up email auto-forwarding from your Surrey account. Doing may constitute a breach of GDPR. It is highly likely that this requirement will apply to the majority of those holding Surrey accounts. If you are unsure about whether you will be receiving personal data in your emails, you should err on the side of caution and **MUST NOT** set up email auto-forwarding.

There might be cases when it is appropriate to auto-forward emails containing personal data to external third parties, however, this must only be done where appropriate contracts and assurances are in place, and not without prior approval from the Data Protection Officer.

In all cases, if you are unsure, please contact the Information Governance Team.

4.5 Data Protection Impact Assessment (DPIA)

It is a legal requirement for a DPIA to be undertaken for any processing of personal data which is likely to result in a high risk to individuals.

It is up to the University to determine what constitutes high risk but this is likely to be where -

- large volumes of personal data are being processed;
- particularly sensitive (special category) data are being processed;
- where new technology is being introduced which will or could potentially be used to process personal data. In any event, for all new technology, a reasonable consideration of the level of risk must be made and recorded.

DPIAs are completed using OneTrust. This will begin with an assessment which will determine whether further information is required.

What you need to do

- Carry out a DPIA prior to entering into any contractual arrangements.

4.6 Data Breaches (Personal Data)

A personal data breach is when personal data has been accessed, disclosed, lost, amended or destroyed, whether intentionally or not. The University must report serious breaches to the ICO within 72 hours, therefore it is important that **ALL breaches or suspected breaches** are reported as soon as possible. This procedure covers breaches which involve personal data. Breaches that do not involve personal data are handled by IT Security.

What you need to do

- As soon as a personal data breach is identified you must report it via the following link OneTrust.
- Do **not** discuss the breach with anyone not involved in the breach.
- Stop processing the data, until advised otherwise. E.g. do not continue an email chain which contains misdirected information.

4.7 Information Requests

Data Subject Access Requests (DSARs)

As outlined in the Our Data Policy Statement, under UK data protection legislation individuals have certain rights in relation to their own personal data. Although these cover a number of different rights (e.g. access, rectification, erasure, etc.), they are collectively referred to within the University as Data Subject Access Requests or DSARs.

UK GDPR sets the deadline for responding to DSARs as one calendar month. This is only extendable by a maximum of two months (i.e. three months in total) in circumstances where the request is complex. Failure to comply with a DSAR has the potential to result in serious consequences for the University, including regulatory enforcement notices, significant financial penalties and reputational damage.

DSARs may be requested via any means but for ease it is useful to think of them in terms of "formal" and "informal". An informal request is likely to be a simple task and must be something which falls within the normal duties of a role, for example, a member of staff requesting that HR update their home address.

A formal request is likely to be more complicated and could involve a large volume of information, for example an individual requests a copy of all their personal data held by the University. Formal requests are managed by the Information Governance team and there are specific channels through which such requests must be directed. These are by emailing dataprotection@surrey.ac.uk or by completing the web form on the University's web site.

What you need to do

- Make yourself familiar with data subject rights and have a general understanding of the University's compliance obligations in relation to DSARs.
- If received, direct any formal DSARs to the University's DSAR channels (as above).
- Contact dataprotection@surrey.ac.uk without delay if you are unsure and comply with any instructions (including deadlines) given by the Information Governance team.

.7 Freedom of Information Requests (FoI)

The University has adopted the model publication scheme for Universities. This sets out information that it routinely makes publicly available, or that it intends to publish.

The University must respond to an FOI request within twenty working days. It will operate in the spirit of transparency but will apply exemptions in appropriate circumstances.

FoI requests will normally be about information which is not personal data. If there is a DSAR element contained within an FoI request, it will be split out from the FoI request and dealt with separately under the DSAR process and timescales.

What you need to do

- All FoI requests must be carried out by the Information Governance Team. All staff and others authorised to handle personal data on behalf of the University who believe they have received an FoI request must direct requestors to submit their request at freedomofinformation@surrey.ac.uk or to the web form on the University's web site.
- If you are asked to provide information by the Information Governance Team in relation to an FoI, you must endeavour to do so in the timescales stated in their correspondence with you.

.8 Information Requests from the Police

This process applies to circumstances when the University receives requests from law enforcement agencies (known under data protection law as "competent authorities") for personal data about students, staff or other individuals whose information is held by the University. Exemptions under law allow personal data to be disclosed to law enforcement agencies **without** the consent of the individual who is the subject of the data and regardless of the purpose for which the data was originally collected. Personal data may be released if:

- the information is required for safeguarding national security;
- failure to provide the data would prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty.

Although there is not an automatic right of access to the information, the University seeks to co-operate with the police and other agencies in the prevention and detection of crime so that the campus is safe and secure for everyone, including the wider community.

Requests will be dealt with by the Information Governance Team and/or Campus Safety in consultation with relevant University colleagues and will assess whether the information can or cannot be released.

What you need to do

- Immediately upon receipt, all police requests, including accompanying documentation, must be forwarded to dataprotection@surrey.ac.uk.
- In Emergency Situations or Out of Hours the request must be sent to campussafety@surrey.ac.uk with a copy to dataprotection@surrey.ac.uk.
- Following assessment by Information Governance team and/or Campus Safety in consultation with relevant University colleagues, if the information is to be released, they will liaise with the colleague nominated to respond with instructions. The information **must** be shared securely, preferably using an external sharing standalone SharePoint Site.
- Any request for an exemption (i.e. not disclosing the information requested) must be justified and sent in writing to the University Secretary & General Counsel and the DPO. They will make the decision on a case by case basis and will record their decision. If it is agreed that the information cannot be released, the University Secretary/DPO will reply to the requestor.
- In an Emergency where providing the information is time-critical, the Head of Campus Safety or nominated deputy is authorised to provide the information requested. A confirmation email must be sent to DPO.

5. Governance Requirements

5.1 Implementation: Communication Plan

This Procedure will be communicated -

- via Leader's Alert and management cascade;
- in the list of University procedures;
- on the Information Governance SurreyNet pages
- in recommending reading along with the new starter UK Law module.

5.2 Implementation: Training Plan

The training requirements relating to this Procedure will utilise a number of channels, including –

- series of in person/Teams training sessions for groups of staff to be put in place by summer 2024
- additional online training provision – initial phase by summer 2024.

5.3 Review

Initial review to be one year from effective date. Thereafter, every three years unless there are changes to relevant legislation before the review date.

5.4 Legislative Context and Higher Education Sector Guidance or Requirements

- the UK General Data Protection Regulation 2016/679
- the Data Protection Act 2018
- the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
- the Information Commissioner's Office;
- the Freedom of Information Act 2000.

5.5 Sustainability

This procedure has no impact on carbon emissions or on energy consumption.

6. Stakeholder Engagement and Equality Impact Assessment

6.1 An Equality Impact Assessment has been completed on and is held by the Authorised Coordinator.

6.2 Stakeholder consultation was completed as follows –

Stakeholder	**Nature of Engagement**	**Request EB Approval Y/N**	**Date**	**Name of Co**
Chief Information Security Officer	Consultation			Tom Brown
Equality and Diversity Advisor	Consultation			Michael Has
Archives and Special Collections Manager	Consultation			Helen Rober
Head of Governance Services	Consultation		01/11/2024	Ros Allen
Head of Sustainability	Consultation			Martin Wile
Director of Health and Safety	Consultation		07/11/2024	Matthew Pu
Academic Freedom / Freedom of Speech	Consultation		22/11/2024	Abigail Brad
GRA [POPP]	Consultation		21/11/2024	Kelley Padle