Policy title	Data Management Policy
Version number	
Effective from date	December 2021
Applicable to	Data Users, including staff, students and others who have access to and use Personal Data on behalf of the University
Owner	Academic Registrar
Date EIA completed	
Approving Committee(s)	Executive
Date of approval	
Review date	April 2022

University of Suffolk

Data Management Policy

Purpose

This document explains the University of Suffolk's policy on data protection and data security and is based on the following principles:

- The University will comply with all relevant legislation, particularly the Data Protection Act 2018 and the EU General Data Protection Regulations 2016 ("GDPR").
- Ensuring compliance is a corporate responsibility of the University requiring the active involvement of, and appreciation by, all staff at all levels of the organisation, including honorary staff/associates, contractors, hourly paid lecturers and any students or interns carrying out work on behalf of the University.
- The University will provide support and services to enable staff handling personal data to remain compliant with the legislation and the University's requirements in respect of data security.

About the Policy

At the University data is collected and used about a wide range of individuals, for example staff, students, applicants, visitors and people taking part in our research. Maintaining the security and privacy of their personal data is essential. This policy sets out the University's requirements as Data Controller when processing Personal Data which includes the collection, analysis, sharing, transferring, storing or deleting of such data in any media or format.

This Policy has been approved by the University's Executive and is subject to review every four years in line with the University's review schedule of policies and procedures. Review will take place earlier where changes in legislation require such review.

All University of Suffolk Data Users must comply with this Policy when processing Personal Data on behalf of the University recognising that they have a role to play in ensuring that the University maintains the trust and confidence of the individuals about whom the University processes personal data (including its own staff), complying with legal obligations and protecting the University's reputation. Disciplinary action can be taken against those who do not comply, particularly in cases when there has been deliberate, wilful or negligent disregard of the Policy and University requirements.

The University has policies in place, including this Policy, which are designed to protect the accuracy, integrity and confidentiality of personal data and to ensure that individuals are able to exercise their rights. Appendix 1 provides more information about these other policies.

Key words are defined in the Glossary of Terms in Appendix 2.

If you do not feel confident in your knowledge or understanding of this Policy, or you have concerns regarding the implementation of this Policy, you should raise this with the Data Protection Officer to seek advice (contact details below).

Training

Whilst some staff will receive elements of data protection training as part of their research requirements, all staff must complete the University's online Data Protection training, which is available (University of Suffolk Online Training). Most staff will be required to complete the module every two years, but some staff may be required to complete it annually because of the nature of their work (e.g. if they work with NHS patient data). New members of staff must complete this module as part of their induction. It is the responsibility of managers to ensure that their staff complete the required training, including any additional training required (for example, for researchers), both as part of their induction and biennially thereafter, recording completion in the individual's Actus appraisal record.

It is the responsibility of the Pro Vice-Chancellor of Research and for each supervisor of Postgraduate Research Students to decide whether students must complete the University's online data protection training, or any additional data protection training modules identified as appropriate, at the outset of their programme or annually, and for ensuring completion. More generally the module can be made available to those students undertaking research which involves the use of personal data, as required.

Data Protection Principles

The GDPR sets out principles that the University must observe and comply with when processing Personal Data. The GDPR requires that personal data shall:

1) be processed lawfully, fairly and in a transparent manner
2) be collected only for specified, explicit and legitimate purposes
3) be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed
4) be accurate and, where necessary, kept up to date
5) not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed
6) be processed in a manner than ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accident loss, destruction or damage
7) not be transferred to a country outside of the European Economic Area (EEA) without appropriate safeguards being in place

Further information on the Data Protection Principles can be found on the Information Commissioner's website (ICO - Data Protection Principles).

The University and its staff who process or use personal data must be able to demonstrate compliance with all of the above principles.

Accountability and Governance

The University is responsible for, and must be able to demonstrate, compliance with the GDPR and data protection.

There are a number of actions the University, and its Data Users, can and, in some cases, must take in order to meet this data protection principle, including:

- Implementation of Data Management Policy
- Taking a 'data protection by design and default' approach
- Ensuring that written contracts are in place with organisations that process personal data on the University's behalf
- Maintaining documentation of all University processing activities
- Implementing appropriate security measures
- Recording and, where required, reporting personal data breaches
- Carrying out data protection impact assessments (DPIAs) where the use of personal data is likely to result in a high risk to individuals' interests
- Appointment of a Data Protection Officer
- Adherence to relevant codes of conduct and signing up to certification schemes

Registering with the Information Commissioner's Office (ICO) as a Data Controller

As an organisation that processes personal and special category data, the University is required to register with the ICO. The ICO publishes contact details for the University and the University's Data Protection Officer, fee information, any trading names used by the University and the data protection registration number given by the ICO (Z9376827).

Data Protection Officer

The University's Data Protection Officer advises the University on data protection law, monitors compliance, provides advice to Data Users, and ensures that guidance, training and resources are available to Data Users. The Data Protection Officer is the point of contact for individuals wishing to exercise their rights in relation to their data, and for any contact with the ICO. Contact details for the Data Protection Officer and their team who deal with general queries and Subject Access Requests are as follows:

Data Protection Officer
dataprotection@uos.ac.uk
01473 338000

Legal basis for processing

Whenever the University processes personal data there must be a valid lawful basis for that processing. There are six potentially applicable lawful bases for general processing of Personal Data and ten lawful bases for processing Special Category Data. If Special Category Data is being processed, both a lawful basis for general processing and an additional condition for processing this type of data must be identified. These are listed in full in Appendix 4.

Further sources of advice and guidance are set out in Appendix 5.

In practice, for many of the University's activities it will rely on the legal basis that the 'processing is necessary for the performance of a task carried out in the public interest' as this covers our work as a university in teaching and research. However sometimes the University will need to rely on alternative bases.

Profiling and Automated Decision Making

The ICO has produced guidance (Automated decision-making and profiling) on Profiling and Automated Decision Making which is available on its website and should be taken into account before considering any activity or task which involves Profiling or Automated Decision Making.

Before starting a task or activity which involves Profiling or Automated Decision Making, the following steps must be carried out:

1. A Data Protection Impact Assessment (DPIA) must be carried out. The Data Protection Officer must be informed and consulted as part of that exercise

2. A Privacy Notice must inform individuals if their data will be used for solely automated decision-making processes with legal or similarly significant effects. This must explicitly set out the Data Subject's rights. The Privacy Notice should be approved by the Data Protection Officer

3. The DPIA must be kept under regular review, and records of those reviews must be retained

Data Protection by Design and Data Privacy Impact Assessments (DPIAs)

An aspect of the accountability and governance data protection principle, the University must ensure that consideration is given to the protection of data from design through the life cycle of the process or system.

It is therefore the responsibility of any University member introducing or designing a new process or system, to take account of the data protection principles and ensure that data protection laws are complied with and can be demonstrated.

A DPIA enables Data Users to identify and minimise the data protection risks of a project. A DPIA must be completed for any data processing that is **likely to result in a high risk** to individuals. It is also good practice to complete a DPIA for major projects which will require the processing of personal data.

A DPIA should:

- Provide a description of the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify additional measures required to mitigate the risks

Further information about DPIAs is available on the ICO website (ICO - Data Protection Impact Assessments).

DPIAs should be shared with the Data Protection Officer (dataprotection@uos.ac.uk) prior to sign-off and commencement of the project.

Security

The following data security and management requirements are in place at an organisational level:

1) Each of the corporate systems including MS365 at the University of Suffolk has built-in security, backed up by secure storage.

2) Firewalls limit external access to the University of Suffolk network. Only a very small number of trained network administrators have access to the network. Access for enrolled students, staff and trusted visitors is provided through university log-ins.

3) Server rooms are strictly controlled access areas.

4) The University login gives access to the University of Suffolk network. Staff passwords expire after a defined period and must be changed by the user. Student passwords do not expire; however, students are advised to change them regularly. Both staff and students are required to change their passwords immediately if they believe their details have been compromised.

5) Although workstations automatically lock if left inactive for a specific period, users should always lock their workstations when moving away from their desk.

6) All staff data should be stored on O365 (whether OneDrive, SharePoint or Teams) and is backed up every night. Data stored on legacy network drives are backed up each night

The following should be applied to specialist databases, which contain varying levels of personal and sensitive information, as good practice:

- Each database should be held in a separate directory on the main University of Suffolk network drive and be password restricted to an authorised individual or group.

- The database itself should be password protected by the system administrator.

- All other personal or sensitive data that may be held in local, small-scale documents, for example spreadsheets and word documents, must be password protected and restricted to essential users.

- Personal or sensitive data should never be copied to a lap-top computer for local processing without the express permission of the system owner and only in exceptional circumstances. Whilst University laptops are password protected, they can be vulnerable to a determined hacker. Equally, personal or sensitive data should not be stored on flash-drives, CD-ROM or other external devices.

- Data at the University of Suffolk are retained and disposed of according to need. The overarching principle is that data should only be retained and stored for as long as such data have a legitimate purpose, and thereafter they should be disposed of securely. Each School and Professional Service area of the Institution holds a Data Retention Schedule which specifies the nature of the data retained, the retention period, the reason for

retention, and the action to be taken at the end of the retention period, including how the data are to be disposed of.

- At the end of the retention period, data should be disposed of and/or destroyed. Manual files should be shredded and disposed of in designated confidential waste sacks if appropriate. Electronic data should be deleted from central systems by the individual responsible for the data after liaising with the Digital & IT team.

Individuals Rights

In accordance with the GDPR and the Data Protection Act 2018 every Data Subject has the following rights:

1) The right to be informed about how their personal data may be processed
2) The right of access to their personal data held by the University
3) The right to rectification if their personal data is inaccurate or incomplete
4) The right to request deletion or removal of personal data where there is no compelling reason for its continued processing
5) The right to restrict processing in certain circumstances
6) The right to data portability which allows individuals to obtain and reuse their personal data for their own purposes across different services
7) The right to object to processing in certain circumstances
8) Rights in relation to automated decision making and profiling

More information about the rights of individuals can be found on the ICO website (ICO - Individual Rights). Information about Subject Access Requests can be found on the University website (Subject Access Request Form).

The University must respond to any requests from Data Subjects wishing to exercise these rights within strict time limits. Therefore, all requests from individuals wishing to exercise rights must be forwarded to the Data Protection Officer (dataprotection@uos.ac.uk) immediately. Similarly, staff must prioritise requests from the Data Protection Officer and their team to assist with processing a Data Subject request, to ensure compliance with Data Protection Laws.

Data Breach Management

Everyone is responsible for ensuring that data security breaches are avoided; where one does occur, you should report it immediately to dataprotection@uos.ac.uk or 01473 338000 and ask to be put through to the Data Protection Team.

Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission

- Loss of availability of personal data

Some types of breach must be reported to the ICO by the University's Data Protection Officer within 72 hours. The sooner the breach is reported, the sooner action can be taken and the greater the opportunity to limit any potential damage which might be caused by the incident.

The Data Protection Officer will determine whether it is necessary to report the personal data breach to either the ICO for the affected Data Subjects, or necessary third parties.

The general procedure in the case of a data security breach will follow ICO guidelines and focus on the completion of the four stages of breach management:

- Containment and recovery
- Assessment of on-going risk
- Notification of breach
- Evaluation and response

It is the responsibility of the Data Protection Officer to ensure that a record of all breaches, regardless of whether they are required to be reported to the ICO is retained and that the Registrar and Secretary is informed of reportable instances.

The Data Protection Officer has direct access to the Vice-Chancellor, Chair of Audit & Risk Committee and Chair of the University Board for reporting breaches as required.

Annual Reporting

The Data Protection Officer will provide an annual report on information compliance and governance to the Registrar and Secretary for the information of Executive, Audit and Risk Committee and the University Board.

Queries, Concerns and Complaints

Any queries, concerns, or complaints about the processing of Personal Data by or on behalf of the University or in relation to the exercise of any Data Subject rights should be directed to the Data Protection Officer in the first instance.

Any person who is not satisfied with the way the University has handled Personal Data or a request to exercise Data Subject rights may complain to the ICO (ICO).

Responsibilities

Within this policy, the following post-holders have these responsibilities:

Responsibility	Owner
Administration of subject access requests, response to data protection enquiries from staff and students	Academic Registrar's PA supported by Academic Registrar and Head of Data Governance
Initial investigation and management of data security breaches	Academic Registrar and Head of Data Governance
Overall responsibility for Data Management Policy, authorisation of actions related to data security breaches, management and oversight of the Head of Data Governance and PA to the Academic Registrar, raising	Academic Registrar

awareness of data protection across the University, and the provision of training and information for staff and students	
Overall responsibility for those aspects of data security relating to University of Suffolk information technology systems	Director of Digital
Strategic liaison regarding data protection and data security with the Executive, Audit & Risk Committee and University of Suffolk Board	Chief Operating Officer
Institutional approval of Data Protection Policy	Executive
Personal data to be handled in line with the University of Suffolk Data Protection Policy, best practice and data protection legislation	Staff and students handling personal data

APPENDICES

Appendix 1: University Policies

Data Management Policy

Digital & IT: Acceptable Use of IT

Digital & IT: Secure use of mobile devices

Research Code of Practice

University of Suffolk Code of Practice for Managing Freedom of Information Requests

Appendix 2: Glossary of Terms

Automated Decision-Making	A decision made by automated means without any human involvement
Consent	Agreement which is freely given, specific, informed and unambiguous
Criminal Offences Data	Data relating to criminal convictions and offences or related security measures.
Data Breach	The destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data
Data Controller	The person or organisation that determines when, why and how to process personal data
Data Privacy Impact Assessment	A standard assessment used to identify and reduce risks of a data processing activity
Data Processor	Any person, company or organisation (other than an employee of the data controller) who processes personal data on behalf of a Data Controller
Data Protection Officer (DPO)	An internal, statutory role, required to monitor and promote compliance with data protection legislation
Data Protection Laws	Any law which relates to the protection of individuals with regards to the processing of Personal Data including Regulation (EU) 2016/679 (known as the General Data Protection Regulation or GDPR), the Data Protection Act 2018 and all legislation enacted in the UK in respect of the protection of personal data, and any code of practice or guidance published by the Information Commissioner's Office.
Data Retention	Data retention principles are set out in the University's privacy notices on the website.
Data Subject	Any living, identified or identifiable individual about whom we hold Personal Data
Data Users	Staff, students and others who have access to and use Personal Data on behalf of the University
Individuals Rights	The rights granted to Data Subjects by the applicable data protection legislation, including the right of access to their Personal Data, the right to correct it, and the right to deletion
Personal Data	Any information identifying a Data Subject or from which we could identify a Data Subject. Personal Data includes 'Special Categories' of sensitive personal data and Pseudonymised Data but not anonymised data (data where any identifying elements have been removed)
Special Categories of Personal Data	A subset of Personal Data, being any information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life or

	sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions
Processing or Process	Any activity that involve the use of Personal Data, whether manual or electronic, including obtaining, recording or holding the data, organising, amending, transferring, retrieving, using, disclosing, erasing or destroying it
Privacy Notices	Separate notices setting out information that may be provided to Data Subjects when the University collects information about them. These notices may apply to a specific group of individuals, for example employees or they may cover a specific purpose, for example filming on campus
Pseudonymised Data	Data which has been modified to replace information that directly or indirectly identifies an individual with artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is kept separately and secure
Third Party	Anyone other than the Data Subject and the Data Controller

Appendix 3: Legal bases for processing

Processing shall be lawful only if and to the extent that at least one of the following applies:

1) The Data Subject has given **consent** to the processing of his or her personal data for one or more specific purposes.

2) Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.

3) Processing is necessary for compliance with a **legal obligation** to which the Data Controller is subject.

4) Processing is necessary in order to protect the **vital interests** of the Data Subject or of another natural person.

5) Processing is necessary for the performance of a task carried out in **the public interest** or in the exercise of official authority vested in the Data Controller.

6) Processing is necessary for the purposes of the **legitimate interests** pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child. (This does not apply to processing carried out by public authorities, such as Universities, in the performance of their public tasks).

There are 10 legal bases on which Special Category Personal Data may be processed:

1) The Data Subject has given explicit consent to the processing of those personal data for one or more specified purposes.

2) Processing is necessary for the purposes of carrying out the obligations and rights of the Data Controller or of the Data Subject in the field of employment and social security (subject to the Data Protection Act 2018).

3) Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the data subject is physically or legally incapable of giving consent.

4) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the Data Subjects; 12 Revised Data Protection Policy 27.06.2018.

5) Processing relates to personal data which are manifestly made public by the Data Subject.

6) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

7) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

8) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to safeguards.

9) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy; L 119/38 EN Official Journal of the European Union 4.5.2016.

10) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

Appendix 4: Sources of information, guidance and advice

Data Protection Officer, Head of Data Governance and Professional Assistant to the Academic Registrar

Data Protection Officer
dataprotection@uos.ac.uk
01473 338000

Data Protection Resources:

- ICO resources (https://ico.org.uk/)
- University online training module (University of Suffolk Online Training)
- University information regarding data privacy [https://www.uos.ac.uk/content/data-privacy]
- University IT Security Information (Data Management Policy)
- University Digital & IT Guidance on the use of IT Facilities (ITS Guidance on the use of IT Facilities)