5. his also applies to Partnership staff or others working with or on behalf of the University of Suffolk, accessing University of Suffolk systems, with responsibilities and expectations set out in the relevant Partnerships Agreement.

6. 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.

7. The University has processes 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.

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

9. 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 seek advice from the Data Governance Team (contact details below).

Training

10. All staff must complete the University's online Data Protection training, which is available via the University of Suffolk Online Training portal. Most staff are required to complete the module every three years. Some staff are 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

Legal basis for processing

20. Whenever the University processes personal data there must be a valid lawful basis for

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

25. 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.

26. 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. Information pertaining to the University DPIA process can be found by staff on The Hub.

27. 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.

28. A DPIA should:

- Provide a description of the nature, scope, context and purposes of the processing
-

Appendix 1: University Policies

Data Security Policy

Code of Practice for Managing Freedom of Information Requests

Digital & IT: Acceptable Use of IT Policy

Digital & IT: Mobile Device Use Policy

Employees and Other Workers Privacy Notice

Research Governance

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 tien-GBSL11(ep

Appendix 3: Legal bases for processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
    a. The Data Subject has given **consent** to the processing of his or her personal data for one or more specific purposes.
    b. 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.
    c. Processing is necessary for compliance with a **legal obligation** to which the Data Controller is subject.
    d. Processing is necessary in order to protect the **vital interests** of the Data Subject or of another natural person.
    e. 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.
    f. 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).

2. There are 10 legal bases on which Special Category Personal Data may be processed:
    a. The Data Subject has given **explicit consent** to the processing of those personal data for one or more specified purposes.
    b. Processing is necessary for the purposes of **carrying out the obligations and rights** of

e. Processing relates to **personal data which are manifestly made public** by the Data Subject.
f. Processing is **necessary for the establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity.
g. 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.
h. 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.
i. 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.
j. 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
datagovernance@uos.ac.uk
01473 338240

Data Protection Resources:

- University online training module University of Suffolk Online Training
- University information regarding data governance UoS Data Governance
- Digital & IT Acceptable Use Policy
- University Data Breach information UoS Data Breach Reporting
- ICO resources https://ico.org.uk/