UNIVERSITY OF SUFFOLK

DATA SECURITY POLICY

Purpose

1. This Data Security Policy outlines the procedures and guidelines for safeguarding, managing, and storing sensitive information at The University of Suffolk. Its primary aim is to ensure the confidentiality, integrity, and availability of data, in compliance with all relevant laws and regulations.

Scope

2. This policy applies to all faculty, staff, students, contractors, and any individual or entity accessing or handling university data, systems, or networks.

Data Classification

3. Data is classified as the following:

- Sensitive Data: Information classified as sensitive includes, but is not limited to, personally identifiable data (PID), financial data, health records, research data, intellectual property, and any data covered under legal, contractual, or regulatory requirements.
- Internal Data: Information not publicly available but not classified as sensitive.
- Public Data: Information that can be freely shared without restrictions.

Responsibilities

4. Responsibilities for data security:

- University Administration: Responsible for overseeing the implementation, compliance, and regular review of this policy.
- Data Owners: Academic or department heads responsible for defining data classifications, access levels, and ensuring appropriate protection measures.
- Digital & IT Team: Responsible for maintaining secure systems, networks, providing technical support, and enforcing security measures.
- Users: Required to adhere to this policy, including securing access credentials, reporting security incidents, and following best practices for data protection.

Data Security Measures

5. Data security measures used are:

- Access Control: Grant access to data on a need-to-know basis. Use strong authentication methods, including passwords, multi-factor authentication (MFA), and least privilege principles.
- Encryption: Encrypt sensitive data in transit and at rest using industry-standard encryption algorithms.
- Data Handling: Ensure secure handling, transmission, and storage of sensitive information. Ensure no storing of sensitive data on personal devices unless encrypted and authorised.
- Security Awareness Training: Regularly train and educate staff, students, and relevant parties on data security best practices and policies.
- Incident Response Plan: Develop and maintain a comprehensive incident response plan to address data breaches, including reporting procedures, containment, and recovery.
- Regular Audits and Assessments: Conduct periodic security audits, risk assessments, and vulnerability scans to identify and mitigate potential threats.

Compliance and Legal Obligations

6. Compliance and legal obligations include:

- Adhere to all relevant data protection laws and regulations, including the General Data Protection Regulation (GDPR), Data Protection Act, and any other applicable legislation.
- Obtain necessary consents and permissions before collecting, processing, or sharing personal data.

Reporting Security Incidents

7. All security incidents must be reported:

- Promptly report any suspected or actual data security incidents, breaches, or violations to the Data governance team who will liaise with the Digital & IT Team and the designated authorities.

Individuals Rights

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

i. The right to be informed about how their personal data may be processed
ii. The right of access to their personal data held by the University
iii. The right to rectification if their personal data is inaccurate or incomplete
iv. The right to request deletion or removal of personal data where there is no compelling reason for its continued processing

v. The right to restrict processing in certain circumstances

vi. The right to data portability which allows individuals to obtain and reuse their personal data for their own purposes across different services

vii. The right to object to processing in certain circumstances

viii. Rights in relation to automated decision making and profiling

9. 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).

10. 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 Governance Team (datagovernance@uos.ac.uk) immediately. Similarly, staff must prioritise requests from the Data Governance Team to assist with processing a Data Subject request, to ensure compliance with Data Protection Laws.

Data Breach Management

11. Everyone is responsible for ensuring that data security breaches are avoided; where one does occur, you should report it immediately to datagovernance@uos.ac.uk, via the online reporting form or 01473 33824.

12. 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

13. Some types of breach must be reported to the ICO by the University’s Data Protection Officer or Data Governance Team 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.

14. The Data Governance Team 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.

15. 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

16. It is the responsibility of the Data Governance Team 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.

17. 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

18. The Data Protection Officer (DPO) 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

19. 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 Governance Team in the first instance.

20. 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

21. 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 DPO (Academic Registrar (AR)) and Head of Data Governance
Initial investigation and management of data security breaches	Academic Registrar (DPO) 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 awareness of data protection across the University, and the provision of training and information for staff and students	Academic Registrar (DPO)
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	Quality Committee
Personal data to be handled in line with the University of Suffolk Data Management Policy, best practice, and data protection legislation	Staff and students handling personal data