UNIVERSITY OF SUSSEX

General Counsel, Governance and Compliance

INFORMATION CLASSIFICATION AND HANDLING POLICY

1. OVERVIEW AND PURPOSE

1.1 The University needs to safeguard its information and, where that information is personal data, also has a duty to comply with data protection legislation.

1.2 The Information Classification and Handling Policy sits alongside the University's Information Security policies and Data Protection Policy and is in place to ensure that all information – whether personal data or not – is handled by the University with appropriate care and security at all times.

1.3 This policy outlines how information should be classified based on its sensitivity or value, and any risks associated with inappropriate disclosure, and provides guidance on the protective measures that must be used when handling different types of information.

1.4 The Information Classification & Handling Policy ensures a consistent approach to classifying and handling information across the University and reduces the risk of information security and personal data breaches.

2. SCOPE

2.1 This policy applies to all information handled by the University, including information created by members of the University or originating elsewhere, i.e. received from third parties. The policy relates to information whether it is held electronically or physically.

2.2 This policy applies to all staff and others handling University information, either remunerated or not, including:

- Senior managers, officers, and directors;
- Employees (whether permanent, fixed-term, temporary, or casual);
- Contract, seconded, and agency staff;
- Volunteers, apprentices, and interns; and
- Others associated with the University, i.e. performing services for or on behalf of the University, such as agents and consultants.

2.3 Except where a student is also an employee of the University, or handling information on behalf of the University (e.g. as part of research work), this policy does not apply directly to students.

3. RESPONSIBILITIES

3.1 University Executive Group ('UEG')

3.1.1 UEG is responsible for ensuring appropriate technical and organisational measures are in place to safeguard any information that is handled as part of the University's day to day functioning.

3.1.2 UEG is responsible for ensuring the University complies with all legislative, regulatory and other requirements relating to information management, such as data protection and information security.

3.2 Heads of Schools and Professional Services Directors

3.2.1 Heads of Schools and Professional Services Directors have responsibility for ensuring that their staff are familiar with this policy and that classification and handling of information throughout the School or Division complies with this policy.

3.3 The Senior Information Risk Owner ('SIRO')[1]

3.3.1 The SIRO is the named individual responsible for leading a culture of good information management and governance within the University, including the appropriate classification and handling of information.

3.3.2 The SIRO ensures that information assets and risks within the University are managed appropriately and effectively via consistent organisational processes, and that policies and procedures are in place to facilitate this.

3.3.3 The SIRO will delegate responsibility for ensuring compliance with this policy in terms of information technologies used by the University to the Chief Digital Transformation Officer.

3.4 Chief Digital Transformation Officer[2]

3.4.1 The Chief Digital Transformation Officer is responsible for ensuring that information technologies used by the University facilitate and enable compliance with this policy.

3.5 All Staff

3.5.1 All staff (see 2.2) are responsible for familiarising themselves with this policy and complying with it.

3.5.2 All staff must ensure that information they handle is appropriately classified and handled in accordance with this policy and any associated guidance.

4. POLICY

4.1 Classification of information

4.1.1 Consideration should always be given to the sensitivity and value of the information being handled. Where there is a risk that inappropriate disclosure or dissemination of the information (either internally or externally) would cause financial or

[1] See Governance and Compliance : Governance and Compliance : University of Sussex
[2] See Governance and Compliance : Governance and Compliance : University of Sussex

reputational damage to the University, breach legal or regulatory requirements, or cause harm to or impact negatively on individuals, information should be classified as ***'Sensitive'***.

4.1.2 Additionally, careful consideration needs to be given to who information should be shared with. Staff should think carefully before sharing information and limit it to appropriate and necessary recipients. Staff should also be particularly conscious of whether information should be shared externally.

4.1.3 Examples of *'Sensitive'* information include valuable commercial information, research data, special categories of personal data, or information relating to contractual or legal obligations.

4.1.4 Having considered if information needs classifying, appropriate classification markings must be put in place, whether the information is in paper or electronic format, so that individuals are clear as to how the information should be handled.

4.1.5 Information should be classified as follows:

Classification	**Description**
Sensitive	The information may be shared or used internally or externally as appropriate, but appropriate safeguards should be in place to protect the information.
No classification	The information can be shared or used internally and externally, without any safeguards in place, such as information on our external webpages. However, as with all information, it should only be shared with appropriate and necessary recipients.

Where information has been classified as *'Sensitive'*, this classification should be made clear – for example, added to the email subject heading, included in the file name, or as a watermark on a paper document.

4.2 **Handling of information**

4.2.1 Information must be handled according to its classification, with the appropriate safeguards and measures put into place to protect the information.

4.2.2 '*Sensitive*' information requires an appropriate degree of security. Technical and organisational measures should be in place to protect against unauthorised or unlawful access, disclosure, or use of information, and against accidental loss, destruction or damage. Such measures should reflect the sensitivity or value of the information and may include appropriate access controls, information security measures such as password protection or encryption, and use of secure storage. Additional guidance can be found in IT's Information Security policies.

4.2.3 Particular care should be taken when sharing '*Sensitive'* information externally, as there is an additional risk inherent in transferring data outside of the University physically and/or outside of its systems and electronic storage solutions.

4.2.4 All information, regardless of classification, should only be held for as long as is necessary and must be retained and destroyed in accordance with the University's Records Management Policy and Master Records Retention Schedule. Information

classified as '*Sensitive*' must always be securely disposed of e.g. using secure shredding, confidential waste disposal or IT-supported deletion.

4.2.5 All IT equipment which holds information, such as laptops and mobile telephones, must be disposed of in a secure manner in accordance with the IT Asset Management Policy and the Workstation Disposal Policy.

4.3 Compliance

4.3.1 Where there is non-compliance with this policy resulting in a personal data breach, any breach must be reported to the University's Data Protection Officer under the Personal Data Breach Reporting Process.

4.3.2 Where there is evidence of a potential or actual systems/security breach affecting University information, this should be reported to IT Services, in accordance with the IT Security Policy.

4.3.3 Where there is deliberate misconduct or behaviour amounting to a wilful breach of this policy, or gross negligence causing a breach of the policy, the matter may be considered under the University's Disciplinary Procedure under Regulation 31.

5. LEGISLATION AND GOOD PRACTICE

5.1 The Information Commissioner's Office provides a guide to the UK data protection legislation on their website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

5.2 Details of the Freedom of Information Act 2000 can be found at the following link: https://www.legislation.gov.uk/ukpga/2000/36/contents

Review / Contacts / References	
Policy title:	Information Classification and Handling Policy
Date approved:	31 January 2023
Approving body:	University Executive Group
Last review date:	January 2023
Revision history:	Version 3: January 2023 Version 2: February 2021 Version 1: October 2018
Next review date:	January 2026
Related internal policies, procedures, guidance:	IT Information Security policies Data Protection Policy Records Management Policy and Guidance Master Records Retention Schedule Personal Data Breach Reporting Process
Policy owner:	General Counsel, Governance and Compliance
Lead contact / author:	Information Manager, Information Management Team