Document Reference Number	**UoG/ILS/IS 003**
Title	Policy for Information Security & Privacy Impact Assessments and Secure Data Handling
Owning Department	Information and Library Services
Version	2.1
Approved Date	12/12/2023
Approving Body	IT Management Board (IM)
Review Date	24/10/2024
Classification	Public – Non-sensitive

UNIVERSITY of GREENWICH

Policy for Information Security & Privacy Impact Assessments and Secure Data Handling

1.0 Purpose

1.1 The purpose of this policy is to outline the university's approach for addressing the risks relating to the use and handling of its data, including the risks associated with implementing and managing the IT systems that process this data.

1.2 This Policy covers the principles that address the following areas:

i. Information Security and Privacy Impact Assessments
ii. Information Classification, Labelling and Handling

2.0 Scope and Compliance

2.1 This policy applies to all activities that involve handling, storing, processing, managing and disposing of university data and IT systems by or on behalf of the university.

2.2 The policy applies to all university staff, contractors and third-party agents.

3.0 Reference to International Organisation for Standardisation (ISO) 27001

3.1 This policy complies with the university's Information Security Strategy and draws upon the ISO 27002 Code of Practice.

4.0 Principles:

4.1 **Information Security and Data Privacy Assessments:**

4.1.1 To identify and effectively manage data privacy and security risks that university processes, projects and use of IT systems may create, information security and privacy impact assessments (PIA) will be carried out. At the start of a process or project and during its implementation, information security and data protection requirements must be defined, and the assessments of any related risks completed.

4.1.2 Process and project leads, system or service owners must ensure the necessary assessments are carried out. They should consider the confidentiality and value of the information involved, and the outcome of a serious incident (information loss or leak, user account misuse or compromise or a technical failure) when determining the security controls and risk mitigation measures to use. Residual risks should be recorded in relevant local risk registers and monitored appropriately.

4.1.3 Use of third-party IT systems or services including cloud services must be authorised by the Executive Director and Chief Information Officer, or a nominee. Project leads and sponsors must ensure that information security and data protection requirements are adequately addressed by suppliers. The use of such systems or services must comply with the university's Information Security and Information Compliance Policies.

4.1.4 To ensure the continuity of business operations, under a carefully monitored procedure, an emergency change/upgrade to an IT system or service with significant data protection and information security elements may be allowed to forgo security assessments, and the system/service owner will carry the assumed risk. However, information security and data protection assessments must be conducted immediately after the change or upgrade has been completed. The Executive Director and Chief Information Officer or a nominee must authorise this change or upgrade. Refer to the Procedure for Information Security and Privacy Impact Assessments for further guidelines.

4.2 **Data Classification, Information Labelling and Handling:**

4.2.1 To promote the secure handling of university data and to address any associated risks, data owners shall be responsible for ensuring that the data used within their departments is classified, labelled and handled according to requirements set out in the Procedure for Data Classification, Information Labelling and Handling. Data owners and Records Coordinators are to ensure their departments follow the guidelines provided in this policy, the university's Information and Records Management Policy and related guidelines to support the management of data.

4.2.2 Project leads/managers must ensure that documentation exists describing the data used, named data owners, the classification group(s) and labelling, and the relevant handling procedures.

4.2.3 Where information falls under more than one classification group, the more stringent information labelling and handling procedure should apply. Refer to the Procedure for Data Classification, Labelling and Handling for further guidelines.

4.2.4 For information handling, only university-approved collaboration tools must be used. Only the communication methods approved by the Internal Communications Team should be used.

4.2.5 Where information is shared between the university and external parties, the university's Data Transfers and Data Sharing Protocol will be used where practical, and the appropriate information handling procedures should apply.

4.2.6 Periodically, the classification groups assigned to university data should be reviewed by data owners to ensure data classifications are still appropriate in the light of new or changes in legal, academic and administrative requirements. In all cases, data sensitivity and value to the university should guide any data reclassification and handling.

4.2.7 Data users should be made aware of the classification group assigned to data to ensure data is handled appropriately.

4.2.8 Third parties responsible for handling information on behalf of the university are required to have procedures for appropriate and secure handling of university information to safeguard such information and maintain compliance with regulatory requirements.

5.0 Policy Compliance

5.1 The necessary steps to verify compliance with this policy shall be undertaken. This includes, but is not limited to, business tool reports, internal and external audits and feedback to the policy owner.

5.2 Failure to adhere to this policy will be addressed under the university's disciplinary processes and relevant contractor and third-party contractual clauses relating to non-conformance with the information security policies.

6.0 Exception to Policy

6.1 Any exception to this policy must be authorised by the Executive Director and Chief Information Officer or a nominee.

7.0 Policy Review and Maintenance

7.1 This policy shall be reviewed annually and where necessary will be updated as part of the continual improvement process.

8.0 Supplementary Documents and Procedures:

i. Procedure for Information Security and Privacy Impact Assessments
ii. Procedure for Data Classification, Information Labelling and Handling
iii. Procedure for Disposal of IT Equipment

9.0 Related Policies Links

Links to Information Security Policies,
Links to the Information Compliance Policies.
Links to the Sustainability Policy