Document Reference Number	**UoG/ILS/IS 002**
Title	Policy for Information Security and Data Protection Training
Owning Department	Information and Library Services
Version	1.8
Approved Date	10/12/2024
Approving Body	IT Management Board (IM)
Review Date	09/12/2025
Classification	Public – non-sensitive

Version Control

Version	Last Modified	Last Modified By	Document Changes
1.8	10/12/2024	Atif Siddique	Added version control and requirement for role specific training.

Policy for Information Security and Data Protection Training

1.0 Introduction

1.1 The purpose of this policy is to provide training and awareness to staff, students and all other users of the university's information and information systems on their responsibilities for safeguarding these assets and how their responsibilities are discharged.

1.2 The university's Information Security Awareness training is designed to educate and raise awareness about the importance of employing good information security practice in day-to-day job tasks and learning environments to facilitate and promote appropriate use and safety of its information assets.

1.3 The university has a statutory duty under data protection legislation, for following data protection principles. The Data Protection including GDPR training is designed to raise awareness on the importance of data protection and how data should be managed correctly.

1.4 Both training courses are available to all users, however, are mandatory for all staff, postgraduate research students and affiliates who have access to university PII. Where training has been mandated, completion of the courses will be monitored and reported on. This applies to the induction training and the ongoing refresher training.

1.5 The university is committed to complying with its statutory duty, not only so that it can avoid data breaches and hence possible fines and damage to its reputation, but also so that it can fulfil its obligations to those data subjects (students, staff, and some other individuals) about whom it holds and processes data. These courses are an important part of the university's effort to achieve this.

1.6 It is necessary that all staff, students, contractors and third-party agents who access, use or support the university's information assets are adequately trained in information security and data protection principles to be able to implement safeguards to maintain the confidentiality, integrity and availability of these assets, and to identify and respond to information security threats and risks appropriately and responsibly.

1.7 The university will test the effectiveness of its training through simulated activities such as phishing tests.

2.0 ISO 27001 Reference

2.1 This policy complies with the university's information security strategy and draws upon the ISO 27002 code of practice.

3.0 Responsibility

3.1 Staff, Postgraduate Research Students and Affiliates

It is the responsibility of all members of staff, postgraduate research students and affiliates, who have access to university PII, to ensure that they use the university's information and information systems appropriately. Responsibilities are detailed below:

- Required to complete the online Data Protection including GDPR training within 3 weeks of being provided access to an account.
- Required to complete the online Information Security Awareness training within 3 weeks of being provided access to an account.
- It is the line manager's responsibility to ensure a new member of staff is aware that they must complete the mandatory training modules. Completion of the courses should be recorded in staff probation/appraisal records.
- It is the postgraduate research supervisor's responsibility to ensure a new postgraduate research student is aware that they must complete the mandatory training modules.
- Whoever has management responsibility around the activity of an affiliate who has access to university PII is responsible for ensuring that the affiliate completes the mandatory training modules.
- All members of staff, postgraduate research students and affiliates who have access to university PII, are required to complete refresher training every two years following the completion of the initial courses.
- Staff, postgraduate research students and affiliates, who have access to university PII, may be required to complete the training courses at any time during the course of their employment or contract with the university if there are any substantial changes to the course content or if the individual is involved in any activity that suggests that retraining may be necessary, such as a security incident or an actual or potential data breach. This requirement will be at the discretion of the information and cyber security teams or the information compliance team. Completion of the training will be mandatory and must be completed within the given time.
- Where mandatory training is not completed within the given period, access to corporate systems will be removed and can only be regained by requesting access through the IT Service Desk and completing the training before the next day.

3.2 All members of staff who work in specialist roles which may involve access to privileged or business sensitive systems or information may be required to complete supplementary training relevant to their roles.

3.3 This policy also applies to students who have been contracted as university staff or have roles that require access to business-sensitive information.

3.4 Part-time or hourly-paid lecturers are also required to complete the training courses and should liaise with their supervisors to agree a suitable time to do so.

3.5 Contractors and Third-Party Agents

3.5.1 Contractors and third-party agents who access, use or manage the university's information or information systems are responsible for coordinating and implementing relevant awareness and training courses for their staff.

3.5.2 The university's Information Security Awareness and Data Protection including GDPR training courses are available via the university's online Portal. All contractors and third-party agents who have access to the university's Portal should complete these courses where training is not provided by the organisations they work for.

4.0 Simulated Phishing Tests and Training

4.1 Simulated phishing tests shall be conducted throughout the year, and results shall be communicated as needed to raise awareness. Where a user fails to detect a phishing email, they will receive training to enhance their awareness and skills. Additional follow-up actions and training will be implemented where a requirement is identified. Completion of the training will be mandatory and must be completed within the given time. Failure to complete the training may be escalated to the individual's Pro Vice-Chancellor or Executive Director.

4.2 Where there are repeated failures to detect phishing emails, the matter may be escalated to the individual's Pro Vice-Chancellor or Executive Director. Where further action is required, the matter may be escalated to the People Directorate and the Chief Information Officer.

4.3 All university staff, postgraduate research students and affiliates who use university email services shall be included in the phishing tests.

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 may 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 approved 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 Related Policies, Processes and Standards

- Information security policies and associated documents
- Information compliance policies and associated documents