Document Reference Number	UoG/ILS/IS 012
Title	Policy for Use of Real Data in Nonproduction Systems
Owning Department	Information and Library Services
Version	2.1
Approved Date	24/07/2024
Approving Body	IT Management Board (IM)
Review Date	23/07/2026
Classification	Public – Non-sensitive

Version	Last Modified	Last Modified By	Document Changes
2.1	24/07/2024	Atif Siddique	Annual review. Scope and Policy Compliance sections and job titles updated.

Policy for Use of Real Data in Nonproduction Systems

1.0 Purpose

1.1 The purpose of the policy is to ensure the use of real data in nonproduction systems (development, test and staging) is carried out in ways that comply with lawful processing as set out in the Data Protection Legislation with considerations given to the requirements to maintain a degree of real data in such systems for operational reasons in certain circumstances.

2.0 Scope

2.1 This policy applies to all IT systems operated by the University.

2.2 This policy applies to all IT system owners, system administrators, developers and project managers.

2.3 Contractual clauses are to include the relevant agreements and measures to ensure data is processed in compliance with the Data Protection Legislation and must be in place for data processed by third parties on behalf of the University.

3.0 International Organisation for Standardisation (ISO) 27001 Reference

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 In all cases, when there are considerations to keep real data in nonproduction systems, alternative methods of processing within these systems will first be explored; such as the use of minimised or dummy data, or alternative ways of system testing.

4.2 Where business operations necessitate real data in nonproduction systems, this must be highlighted when completing a privacy impact assessment (PIA) for the system, to address any associated risks.

4.3 Where it is necessary to maintain a copy of a production system, this will primarily be used for support of complex issues as considered necessary to do so, along with occasions when nonproduction/user acceptance testing requires its use. The following will apply:

4.3.1 As a minimum, the same level of security controls as with the production system or more stringent controls will be applied.

4.3.2 Access to the production copy must be strictly controlled and formally authorised by an appropriate authoriser such as the system owner before access is given. Access will be given for a specific period, logged and reviewed periodically.

4.3.3 Access authorisation will be audited.

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 every two years and where necessary will be updated as part of the continual improvement process.

8.0 Related Policies and Procedures

- Information Security Policies
- Information Compliance Policies
- Risk Management Policy and Guide