Library Content and Collections Security Policy

1. Context

The Library of Trinity College Dublin is responsible for the security of the content and collections in its care and must ensure that appropriate and proportionate measures are in place to prevent loss, harm or damage. The Library embeds security measures in all its operations, storage facilities, IT infrastructures and services. Its approach is risk-based and includes regularly reviewing and upgrading the security measures to ensure maximum effectiveness with the available resources.

The Library's content and collections are a significant national cultural asset. The mandate of their preservation arises from successive Copyright Acts since 1801, granting legal deposit rights and obligations, as well as from the Statutes of the University (see the 2010 Consolidated Statutes, p. 221).

The Library is mandated to make its content and collections as widely accessible as possible to the Trinity community and to others external to the University, where appropriate. This Policy recognises that there is an inherent risk (both internal and external) to the Library's content and collections to cyberattack, loss, theft and vandalism. The Library's regulations and controls need to balance the demands for access and the imperatives for security, within the overall aim of creating an environment where users and staff feel safe, supported and well-informed.

2. Purpose

This Policy details a strategic framework for the management of the security of the Library's content and collections. This framework is implemented via operational procedures, which are documented and maintained separately.

3. Scope

This Policy applies to all content and collections within the care of the Library or licenced by it (see also the definition below). It applies to their control in Library buildings and third-party facilities; digital hosting; staff procedures; use of content and collections by readers, including access and borrowing; and loans for exhibition display.

4. Principles

This Policy encompasses the values articulated in the Library Manifesto, re-published in the *Continuity and Development of the Library Strategy – 2026*, specifically the Library's cultural, statutory, financial and professional responsibility to its content and collections.

5. Definitions

In the context of this Policy, the following definitions apply:

Security: *"*The condition of being protected from loss, harm, or damage*"* (*ASIS Risk Assessing Standards, 2016*, referenced by the Archives & Records Association UK & Ireland on their Security Guidance website: https://www.archives.org.uk/security-guidance/security-guidance#what-is-security).

Content and Collections: comprising all print, object, and manuscript **collections**, as well as born digital and digitised **content** – whether purchased, licenced, created, donated or acquired through Irish and UK legal deposit legislation.

6. Policy

The Library Content and Collections Security Policy maintains that:

i. There is an overall institutional commitment to providing effective content and collections security, by physical and technical measures, including authentication, operational procedures, resilience planning and continuous training and education of staff and users.

ii. The Library allocates staff and financial resources to content and collections security, working closely with other relevant units in the University, e.g. Estates & Facilities, Data Protection Office, and IT Services.

iii. All members of Library staff are expected to understand the importance of content and collections security and their specific role in it and are encouraged to develop a culture which pro-actively protects the Library's assets, content and collections while being sensitive, fair and respectful to the needs of Library users.

iv. Buildings, IT infrastructures and services managed by third-party suppliers conform with Library-specified content and collections security standards.

v. The Library will respond to any security incident and investigate any reported loss of property, content or collection items.

vi. Readers, students, visitors, suppliers, and staff face disciplinary action, exclusion, and/or will be subject to legal proceedings in cases of deliberate breaches of security, serious or gross negligence or misconduct, theft, or significant damage to buildings, content or collections.

vii. Security measures are balanced against the legitimate access to, and use of, content and collections by present and future generations.

viii. Security features prominently on the Library's risk management programme, feeding into the University's risk register, which is used to continually monitor threats and develop appropriate responses.

ix. The safety of people is paramount: staff and users must not put themselves in physical danger to protect the Library's content and collections.

x. The Library cooperates and collaborates with other collecting institutions and interested bodies, including An Garda Síochána, Trinity's insurer and sectoral security networks, for information sharing and best practice.

7. Responsibility and Implementation

The Librarian and College Archivist has overall responsibility for Library content and collections security. The Deputy Librarian has delegated authority for implementation and operational oversight, including the management of Library security staff. Members of the Library Leadership Team monitor implementation at departmental level, with support from the Content and Collections Security Working Group(s).

The Content and Collections Security Working Group(s) include representation from across Library departments, Estates & Facilities, Data Protection and IT Services. Membership can be extended to one or more external advisors. Group remit includes review of security measures, security audits, and security incidents.

8. Related Documents

This Policy relates to, and closely interacts with, other Library and University policies, including:

Library (see also Policies web page):

i. Disposal Policy
ii. Content & Collections Development Policy
iii. Donations Policy
iv. Digital Preservation Policy
v. Library Access and Use Regulations
vi. TCD Library Emergency Response Plan Manual
vii. TCD Library Exhibition Loans Policy and Agreement Conditions documents

University:

i. CCTV Policy
ii. Protected Disclosures (Whistleblowing) Policy
iii. Lone Working Policy
iv. IT Services Policies (including Cyber Security)
v. TCD Risk Management Policy
vi. Data Protection Policy

This Policy should also be considered in relation to the Library's Strategic Plan.

9. Version Control

This policy will be reviewed every two years by the Content and Collections Security Working Group(s), the Library Leadership Team, and the Librarian & College Archivist.

Date of initial approval: previous Library Security Policy was last revised in 2008
Date revised policy approved: ? 2024
Revision approved by: Critical Infrastructure Committee
Date policy effective from: ? Board
Date of next review: Academic Year 2026/2027
Officer responsible for review: Librarian & College Archivist