Goldsmiths
UNIVERSITY OF LONDON

# Information Security Policy

| | |
|---|---|
| Ownership: | Chief Information Officer |
| Policy Contact: | Information Security Manager |
| Approval: | Information Security Steering Group |
| Protective Marking: | Public |
| Policy Unique ID: | POL0003_infosec_v3.3 |
| Last review date: | June 2023 |
| Next review date: | June 2026 |

# Contents

# 1 Introduction

1.1 This policy underpins all Goldsmiths policies, procedures, standards and guidance for the security of electronically stored data. This policy is related to the College's policies on data protection and records management and is prepared and implemented in reference to the Goldsmiths Risk Management Policy.

1.2 The three basic tenets of information security are confidentiality, integrity and availability of IT systems and data. Confidentiality ensures data is only accessible to the right people; integrity ensures data has not been tampered with and availability ensures data is available when required.

1.3 Goldsmiths recognises the need for its students, staff and visitors to have access to the data they require in order to carry out their work and study. Information security helps protect against breaches of confidentiality, failures of data integrity or interruptions to the availability of data and ensures appropriate legal, regulatory and contractual compliance.

# 2 Scope

2.1 This policy applies to:

- Any IT systems attached to Goldsmiths' networks;
- Any IT systems supplied by Goldsmiths;
- Any communications sent to or from Goldsmiths;
- Any data which is owned, controlled or processed by Goldsmiths, including data held on systems external to the university network;
- All approved users of Goldsmiths' data including all staff and students, contractors, suppliers, partners and external researchers who may be authorised to access Goldsmiths' data;
- All locations from which Goldsmiths' data is accessed including home and offsite use; and
- All equipment used to access Goldsmiths' data at any time.

# 3 Policy statements

- Goldsmiths Information Security Policy follows the principles, guidelines and responsibilities as set out in the Information Security Management System (ISMS) ISO 27001 ISO/IEC 27001:2022
- Information security management also follows the Information Security Management Toolkit Edition 1.0 Volume 1 provided by the

University and Colleges Information Systems Association (UCISA) which is based on ISO27001.

These include:

- Data will be protected in line with relevant legislation, notably those relating to Data Protection, Human Rights and Freedom of Information as well as relevant Goldsmiths' policies.
- Each information asset group will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
- Data will be made available solely to those who have a legitimate need for access.
- All data will be classified according to the Goldsmiths data classification as defined in the Protective Marking Policy.
- The integrity of data will be maintained.
- It is the responsibility of all individuals who have been granted access to data to handle it appropriately in accordance with its classification.
- Data will be protected against unauthorised access.
- Compliance with the Information Security Policy will be enforced.

Goldsmiths follows a risk-based approach to Information Security. To determine the appropriate level of security control applied to IT systems, a risk assessment will identify the likelihood and impact of a security incident and define security requirements. The Information Security Manager (ISM) can provide advice for an Information Security Risk Assessment. The Data Protection Officer (DPO) can provide advice on compliance with UK Data Protection law.

This policy follows ISO 27001 Information Security Principles.

## 3.1 Information security policies

3.1.1 Further policies, procedures, standards, and guidelines exist to support the Information Security Policy and have been referenced within this document. Further information is available for staff on the Goldmine IT & Digital Services (IT&DS) pages.

3.1.2 The current IT&DS security related Goldsmiths' Policies are:

- Acceptable Use of IT Services Policy
- Email Policy
- Password Policy
- Patching Policy
- Microsoft Teams Policy for Teaching and Learning

3.1.3 Goldsmiths' IT equipment connects to the internet via Jisc's JANET network and must comply with their security policies and legal requirements. Goldsmiths' polices will be updated to reflect significant changes in Jisc's policies and all applicable law.

## 3.2 Organisation of information security

3.2.1 Goldsmiths will define and implement roles for the management of information security. This includes identification and allocation of security responsibilities to initiate and control the implementation of information security across Goldsmiths.

3.2.2 The hierarchy of responsibility is:

- Council is accountable for the Goldsmiths Risk Register;
- Senior Management Team are responsible for managing Goldsmiths risks as informed by the ISSG.
- The Information Security Steering Group (ISSG) has representatives from all relevant sections of Goldsmiths and its purpose is to influence, oversee, promote and improve information security by identifying and assessing security requirements and risks;
- The ISM supported by the IT&DS Leadership Team, Governance and Legal Services and the DPO, manages information security, providing advice and guidance on the implementation of this policy;
- Information owners for IT systems, such as Business Service Owners are responsible for compliance with this policy;
- IT system owners are responsible for ensuring that appropriate security arrangements are in place for IT administrative access and security controls on managed systems are compliant;
- Information users assume local accountability for compliance with this policy. They are responsible for reporting any actual or suspected information security issues to IT&DS.

## 3.3 People and Organisational Development security

3.3.1 All approved users of Goldsmiths IT services must demonstrate an understanding of the Data Protection Act 2018. Staff must successfully complete the mandatory Information Security Awareness and Data Protection Training computer-based courses every two years.

3.3.2 Security responsibilities should be included in job role descriptions, person specifications and personal development plans. Individuals accessing Goldsmiths' data must seek advice from IT&DS they are not clear about their information security responsibilities.

3.3.3 Employee contracts enforce compliance with Goldsmiths' policies.

3.3.4 Upon termination of a staff appointment, People and Organisational Development will revise the staff record system, accordingly, triggering IT systems account termination processes. Not all system access is automatically controlled, for example local systems and records. Therefore, line managers must ensure that appropriate staff exit procedures are in place to remove access to all systems upon staff exit or change of role.

3.3.5 Line managers must ensure that all IT assets owned by Goldsmiths must be returned upon termination of contract.

3.3.6 The ISM may authorise legally compliant monitoring of IT systems to investigate security incidents and compliance with Goldsmiths' policies.

## 3.4 Asset management

3.4.1 All assets (data, software, processing equipment and IT services) will be identified and owners documented. The owners are responsible for the maintenance and protection of those assets in accordance with Goldsmiths' policies. All data created, received, or retained must be protected according to the Goldsmiths data classification, as defined in the Protective Marking Policy. Brief details are given in section 3.4.2, and more detailed advice is available from Governance and Legal Services.

3.4.2 The four Goldsmiths data classifications are:

- Public: Available to anyone
- Unclassified: Available to anyone with a Goldsmiths campus ID.
- Protected: Personal data or data only available within a department.
- Restricted: Sensitive personal data or confidential and restricted to specific roles.

3.4.3 All Goldsmiths information assets will follow the Goldsmiths' Retention Schedule. Data must be stored on facilities provided by Goldsmiths as advised on Gold Storing and sharing files. Protected and Restricted data must not be copied onto devices. Email is a communications mechanism and must not be used as a replacement for file storage.

3.4.4 Removable mass storage devices should be treated in the same way as Protected/Restricted data and must be locked away at the end of the working day. For further guidance for staff refer to the IT&DS file storage guidance.

3.4.5 Dispose of physical records containing Protected/Restricted data securely by using provided confidential waste shredding services or shredders.

## 3.5 Access control

3.5.1 A procedure for user account creation and deletion must be maintained for access to all IT systems. Access will be granted according to an individual's role and the data classification.

3.5.2 Mandatory authentication must be used. Multi factor authentication must be used for accessing Protected/Restricted data, where this service is provided by Goldsmiths. Users with administrative rights must use their normal user accounts for standard IT system access and only use elevated privileges when required.

3.5.3 Users must not share their login details to access IT services. Passwords must be in accordance with the Password Policy.

3.5.4 All IT equipment and systems connected to the Goldsmiths network or connecting remotely must meet the minimum specification defined in the Patching Policy, utilising an operating system still receiving security updates with antivirus software installed.

## 3.6 Encryption

3.6.1 Goldsmiths IT&DS will provide guidance and tools to ensure proper and effective use of encryption to protect the confidentiality and integrity of data and IT systems. Where IT&DS manages devices, the encryption keys will be securely managed.

3.6.2 Where a staff member manages their own encryption, it is critical that encryption keys are securely backed up, as forgetting an encryption key will mean the encrypted data is lost for ever.

3.6.3 Data encryption is required for Protected/Restricted data transmitted over data networks. Protected/Restricted data must be encrypted if stored away from the Goldsmiths campus.

3.6.4 Mobile computing devices must be encrypted. If unsure take advice from the IT&DS Service Support before applying an encryption key.

## 3.7 Physical and environmental security

3.7.1 Data centres, computer rooms, and communications facilities used for hosting equipment for information processing must be physically protected from unauthorised access to prevent theft or damage. Facilities must also be adequately protected against environmental damage such as by fire or flood.

3.7.2 Computer equipment must be password protected if left unattended. A screen lock must be activated when there is no activity for a short period of time. Passwords must not be written down anywhere near IT equipment.

3.7.3 Portable computing devices must be locked away at the end of the working day.

3.7.4 All Goldsmiths owned equipment must be disposed of in a controlled manner. Any staff wishing to dispose of IT equipment must contact the IT&DS Service Support to arrange collection.

## 3.8 Operational security

3.8.1 Operational changes to equipment, infrastructure, or software affecting Goldsmiths' Production IT services and suppliers must follow IT&DS change management procedures.

3.8.2 IT&DS provide backup services for managed storage. Information owners must ensure that appropriate backup and system recovery measures are in place for locally managed and third-party services they use. Appropriate security measures must be taken to protect against damage or loss of backup media. Backup recovery procedures must be tested on a regular basis.

3.8.3 It is not permitted to connect personally owned equipment to any network socket; personally owned devices should use the wireless network.

3.8.4 Any device connected to the Goldsmiths network must comply with the Patching Policy. Devices which are not compliant will be liable to physical or logical disconnection from the network without notice. All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing.

3.8.5 Individuals installing software themselves are responsible for that installation. Those responsible for software must monitor relevant sources of information for security update alerts.

3.8.6 Goldsmiths inspects systems connected to our network for vulnerabilities. If critical and high vulnerabilities are detected that cannot be mitigated, the system will be disconnected from the network.

3.8.7 Goldsmiths follows the IT&DS Cyber Monitoring Strategy to monitor controls implemented within the University for logging and monitoring.

## 3.9 Communications security

3.9.1 Goldsmiths maintains network security controls to ensure the protection of data within its network and the internet.

3.9.2 Segregation must exist between wired and wireless traffic and Production, Development, Test, and management services according to data classification. Appropriate controls will be enforced between security zones to reduce the risks of compromise, denial of service attacks, malware infection and unauthorised access to data.

3.9.3 Guidance should be sought from the IT&DS Service Desk for information on secure data transfer.

## 3.10 System acquisition, development, and maintenance

3.10.1 Information security requirements must be defined during the development of business requirements for new IT systems and reviewed following significant changes to existing IT systems. IT&DS can provide advice on the security requirements for new IT services and significant changes to existing IT services.

3.10.2 All new projects that will implement systems that process personal data must seek advice from the DPO during the development of business requirements.

## 3.11 Supplier relationships

3.11.1 Suppliers must follow Goldsmiths' security policies, change control process, and support arrangements. Contact IT&DS Service Desk for further guidance.

3.11.2 Supplier activity may be monitored according to the data classification, IT service and perceived risks to Goldsmiths.

## 3.12 Information security incident management

3.12.1 All information security incidents or other suspected breaches of this policy must be reported immediately to the IT&DS Service Support. For the escalation and reporting of data breaches that involve personal data, follow the Data Breach and Information Security Incident Reporting Procedure.

3.12.2 Information security incidents will be investigated in accordance with the Security incident procedures to determine whether any underlying security concern need to be recorded, corrected, and built into future controls. If appropriate, concerns will be added to the IT&DS risk register and reported to the IT&DS Leadership Team.

### 3.13 Information security aspects of business continuity management

3.13.1 Goldsmiths will protect critical IT services from the impact of major incidents to ensure recovery in line with documented priorities. This includes appropriate backup and resilience. Business continuity plans must be maintained and tested. Business impact analysis should be undertaken of the consequences of major security incidents.

### 3.14 Compliance

3.14.1 Compliance with the controls in this policy will be monitored by the ISM and reported to the ISSG.

3.14.2 The design, operation and use of IT systems must comply with all contracts and regulations, relevant UK, EU, and international law. This includes the Data Protection Act 2018, the Payment Card Industry Data Security Standard (PCI-DSS) where relevant, the UK Government's Prevent duty, and Goldsmiths research contractual commitments.

3.14.3 Goldsmiths is subject to independent audit and aims to comply with the spirit of ISO 27001 and the UK Governments Cyber Essentials scheme. Business critical systems and other systems identified as high risk will be regularly penetration tested.

## 4 Sanctions

4.1 Security incident investigation, or the failure to comply with this policy subsidiary policies, procedures or regulations, may result in withdrawal of access to Goldsmiths IT services and may result in disciplinary action or termination of contract.

## 5 Monitoring

5.1 This policy and its implementation will be subject to internal monitoring and auditing, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. Goldsmiths will also undertake appropriate benchmarking and auditing exercises as may be applicable periodically.

# 6 Exceptions

6.1 If an individual or third party cannot comply with this policy they must contact the IT&DS Service Support for advice on security controls to enable compliance, otherwise they must cease using Goldsmiths' data and IT services.

# 7 Definitions

- ISSG: Information Security Steering Group
- ISMS: Information Security Management System.
- ISO: International Standards Organisation
- ISO 27001: Industry standard for an ISMS
- GDPR: General Data Protection Regulation
- JANET: Is a high-speed network for the UK research and education community provided by Jisc
- Jisc: A UK not-for-profit company whose role is to support post-16 and higher education, and research.
- ISM: Information Security Manager
- DPO: Data Protection Officer

# 8 Related documents

- Acceptable Use of IT Services Policy
- Email Policy
- Password Policy
- Patching Policy
- Data Breach and Information Security Incident Reporting Procedure
- Protective Marking Policy (Data Classification)

# 9 Related requirements

- Risk Management Policy
- Data Protection Act 2018
- Freedom of Information Policy
- Data Protection Policy
- Retention Schedule
- Records Management Policy

- Data Privacy Impact Assessment
- IT Services regulations for students
- JANET Policies
- PCI DSS
- ISO/IEC 27001:2022
- Information commissioner's office - GDPR guidance
- National Cyber Security Centre - Cyber Essentials guidance
- UCISA - Information Security Management Toolkit Edition 1.0 Volume 1
- Microsoft Teams Policy for Teaching and Learning

## 10 Review plan

10.1 This policy shall be updated regularly to remain current in the light of any relevant changes to any applicable law, Goldsmiths' policies or contractual obligations and reviewed by the ISSG at least every three years.

10.2 Minor reviews of this policy will be undertaken by the ISM as required and will be approved by the ISSG.

## 11 Revision history

| Version | Date | Details | Author | Approved |
|---|---|---|---|---|
| 2.0 | 01/10/15 | Approved by SMT | David Swayne | Approved |
| 3.0 | 20/06/19 | Submitted to ISSG | Peter Hircock | Approved |
| 3.0 | 11/11/19 | Submitted to E&IC | Peter Hircock | Noted |
| 3.1 | 09/06/21 | Submitted to ISSG | Peter Hircock | Approved |
| 3.2 | 21/06/23 | Submitted to ISSG | Peter Hircock | Approved |
| 3.3 | 20/09/23 | Edits for audit at ISSG | Peter Hircock | Approved |