INFORMATION SECURITY POLICY

Effective for employees, students, directors, and volunteers on or after 1 September 2023

2023-2024

Next review due: September 2026

Please Note: A formal, full review of this document will take place on a 3-yearly basis. However, in the interim, the document will be updated as necessary to remain current with any statutory legislation and/or significant Government guidance updates on the subject.

DOCUMENT CONTROL

DOCUMENT TITLE:	INFORMATION SECURITY POLICY
AUTHOR:	FRANCES DEELEY
CHANGE AUTHORITY:	THE BOARD OF TRUSTEES

Frances Deeley

Signature: _____ _____ **Date:** 18.07.2023

Designation: CHIEF EXECUTIVE OFFICER **Review Date:** September 2026

Please Note: A formal, full review of this document will take place on a 3-yearly basis. However, in the interim, the document will be updated as necessary to remain current with any statutory legislation and/or significant Government guidance updates on the subject.

CHANGE MECHANISM

Any person seeking to alter this document must consult the author before making any change.

ESS Change Authority must endorse any alterations to the approved version of this document before any wider dissemination of the altered document version.

The person making the alteration must indicate every change between the previous (approved) document version and the altered document version.

COPYRIGHT

The copyright in this work is vested in ESS, and the document is issued in confidence for the purpose for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under agreement or with the consent in writing of ESS and then only on condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of ESS. Copyright© ESS, 2026. All Right Reserved

Contents

INTRODUCTION

This Information Security Policy is relevant to all Departments and to all of the staff within them.

SCOPE OF THE POLICY

It is the policy of the Centre to ensure that the information it manages is appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of information. This Policy provides management direction and support for information security across all Departments.

Information managed by the Centre is not just held in electronic format and therefore this Policy covers the security of information held on all media.

RESPONSIBILITIES

Responsibility for ensuring compliance with this Policy lies with the Senior Management Team.

The Senior Information Risk Owner (SIRO) for the Centre is the CEO and SMT. The SIRO is responsible for ensuring information security risk assessments are completed, policy breaches are addressed and acts as advocate for information risk management at the highest level.

The ICT department is responsible for the maintenance of this Policy as well as maintaining associated guidelines and promoting compliance with them.

Compliance with this Policy and any associated procedures is compulsory for all staff employed by the Centre. A member of staff who fails to comply with the Policy may be subjected to disciplinary action under the Centre disciplinary policy. It is the responsibility of Head of Departments and their Directors to ensure that their staff are made aware of the existence of this Policy and its content.

REQUIREMENTS FOR INFORMATION SECURITY

The Senior Management Team will ensure there is clear direction, adequate resourcing, and visible management support for security initiatives.

The ICT department will devise and co-ordinate the implementation of information security controls according to this Policy. The department will also advise heads of department on any risk management issues arising from the implementation of new systems.

The responsibility for ensuring the protection of information systems and ensuring that specific security processes are carried out will lie with the System Owner 1.

INFORMATION ACCESS POLICY A1

OBJECTIVES AND SCOPE OF THE POLICY

This Policy applies to all users of Centre IT related information systems and sets out Centre policy regarding the accessing of information, giving guidance in accordance with current legislation and best practice initiatives.

The Policy objectives are to ensure that:

- the integrity and security of all electronic systems is maintained.
- all information is stored in a secure manner and that appropriate safeguards are in place to prevent improper access.
- any attempts to gain improper access to information are detected and recorded accordingly.
- Centre information systems are not compromised or used for unauthorised activities.
- only authorised members of staff can collect and view pertinent information,
- which must then only be used for legitimate purposes.
    - information is only relayed to other legitimate and authorised users both inside
    - and outside the Centre.

GUIDANCE

USER LOGIN AND PASSWORDS

All users who need access to a computer system within the Centre are required to have a legitimate user login and password. The Centre expects all users to adhere to the following guidelines:

- users will not attempt to gain unauthorised access to Centre IT systems.
- passwords must be a minimum of eight characters in length and should be changed every 180 days when prompted.
- any temporary passwords issued must be changed at first use.
- passwords must never be written down or disclosed to another individual or organisation.
- passwords should never be sent in the form of clear text e-mail messages.

Users are responsible for the secrecy and integrity of their passwords. The Centre will consider password sharing a breach of this Policy and this may result in disciplinary action being taken by the Centre. Inactive network accounts will shut down after a defined period of inactivity to prevent unauthorised access.

Security awareness activities will be scheduled on a regular basis and information security training is scheduled as a mandatory activity for all new staff.

EXTERNAL ACCESS TO INFORMATION

External access to Centre IT systems is strictly forbidden unless the user has a valid login and password. Any authorised user logging in to the Centre network from home or from another external access point should only do so in accordance with the guidelines specified in the Remote Access Policy.

INFORMATION ACCESS BY THIRD PARTY ORGANISATIONS

Access to Centre IT facilities by third parties will not be provided until a copy of the Acceptable Use Policy has been signed by an appropriate third-party representative. The Centre will also utilise data sharing agreements in all situations when the information being disclosed can be classified as personal or confidential data. All authorised third parties who require access to IT infrastructure will also be directed to read this Policy and the Data Protection Policy.

INFORMATION ACCESS - INCIDENT REPORTING

Any IT security incident involving the unauthorised accessing of information within the Centre must be reported to the Head of ICT as soon as possible. In the event that the Head of ICT is implicated in proceedings, notification of the incident should be made to the SIRO. In the event that both the SIRO and the Head of ICT are implicated, the incident should be reported to the Director. The Centre will aim to assess any reported incidents and will look to ensure that appropriate technical and procedural measures are taken to address identified security weaknesses.

POLICE REQUESTS

The police will sometimes request information from the Centre to help with their enquiries. All police requests that are accepted by the Centre should therefore be handled sensitively and in accordance with the Data Protection Act 1998 and the Data Protection Policy Guidance 5 on 'Disclosing Information to the Police'.

ACCESS LEVELS

Procedures for the registration and deregistration of users and for managing access to information systems have been established to ensure that all users' access rights match their authorisations. These procedures are detailed in the ICT User Management Procedure2; this should be used in conjunction with the Network Registration Form and Acceptable Use Policy. All business system user access rights will be reviewed at regular intervals by the system owner or other staff as defined in the User Management Procedure to help safeguard against potential security breaches.

DISPOSAL OF DATA

The Centre will ensure that when permanently disposing of equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site. Damaged storage devices containing sensitive data will also undergo appropriate risk assessment, to determine if the device should be destroyed, repaired, or discarded.

OWNERSHIP, STORAGE AND ARCHIVING OF INFORMATION

Centre information that is deemed confidential or is classed as personal data or sensitive personal data under the Data Protection Policy cannot be stored on or transferred to any unauthorised and non-encrypted storage device or media (eg. memory stick, personal laptop or Centre laptop without encryption software, CD, PDA). Only the Head of ICT and the CEO can authorise the use of a device for this purpose.

All information assets are owned by the Centre and a System Owner will oversee each ICT system holding information or records. This individual will be named on the Information Asset Register.

The Centre will ensure that appropriate backup and system recovery procedures are in place before any archiving of data can commence. The Centre will also ensure that day- to-day information is stored efficiently and is readily available to authorised users.

Where storage is allocated to system or share owners directly the data held will be managed by the system or share owner.

Storage media used for the archiving of information must be appropriate to its expected longevity and the format in which the data is stored will be carefully considered, especially where proprietary formats are involved.

ACCESS TO RECORDS

All information used for, or by the Centre, will be filed appropriately and according to its classification. Paper copies of sensitive or classified material will be handled in accordance with the Centre Records Management Policy.

SOFTWARE MANAGEMENT POLICY C1.

Objectives and Scope of the Policy

This Policy applies to all users of Centre IT related information systems and sets out Centre policy regarding the management of software in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

- all software installations within the Centre are controlled in a secure and legitimate manner.
- only authorised individuals will perform software updates.
- risks to information and information systems are minimised.
- appropriate procedures are in place regarding the maintenance of software within the Centre.

C2. Guidance

BUSINESS APPLICATIONS

Centre business applications will be managed by suitably trained and qualified staff, trained in relevant information security issues.

SOFTWARE IMPLEMENTATION

The Centre will ensure that procurement or implementation of new or upgraded software is carefully planned. Information security risks associated with such projects will be mitigated using a combination of procedural and technical controls.

To prevent copyright infringements and protect all information systems, the Centre will run regular audits and closely monitor all software renewals.

Software must not be installed onto any PC within the Centre by unauthorised staff or students and anyone caught doing so may face disciplinary proceedings.

BUSINESS REQUIREMENTS

Business requirements for new software or enhancement of existing software shall specify the requirements for information security controls.

VENDOR SUPPLIED SOFTWARE

The Centre discourages any modifications to vendor-supplied software. Only strictly controlled essential changes shall be permitted and the development of interfacing software, will be tested before changes are moved to the live environment.

OPERATIONS POLICY D1.

Objectives and Scope of the Policy

This Policy applies to all users of Centre IT related information systems and sets out Centre policy regarding the operation of key systems, in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

- Centre information processing systems are used and managed in accordance with best practice initiatives regarding the protection of information security.
- Changes to operational procedures involving business critical or sensitive
- Information will be analysed, and all associated risks will be assessed to ensure that the needs of information security have been addressed.
- The implementation of any Centre IT systems will be effectively managed in a secure and robust manner.

D2. Guidance

PHYSICAL SECURITY AND ACCESS CONTROL

Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Centre staff with authorisation to enter such areas will be provided with information on the potential security risks and the measures used to control them.

OPERATION OF IT SYSTEMS

The procedures for the operation and administration of Centre business systems will be appropriately documented, with all such procedures and documents being regularly maintained and reviewed by the System Owner.

SECURITY INCIDENTS

The reporting of security incidents and suspected security weaknesses in Centre business systems should be recorded via the ICT helpdesk.

SOFTWARE FAULTS

The reporting of software malfunctions and faults in Centre information processing systems will be made via the Managed Services Helpdesk. Faults and malfunctions shall be logged and monitored, and timely corrective action taken.

SYSTEM DEVELOPMENT AND TESTING

New systems and upgrades are accepted for use subject to testing. Suitable testing of the system will be carried out by system owners prior to migration to operational status.

In collaboration with the third-party vendor, processes will be established by the System Owner to control the maintenance and development of all operational software.

SECURITY RISKS

Security risks to the information assets of all system development projects shall be assessed by the relevant Project Manager or System Owner and access to those assets shall be controlled.

SYSTEM MANAGEMENT POLICY E1.

OBJECTIVES AND SCOPE OF THE POLICY

This Policy applies to all users of Centre IT related information systems and sets out Centre policy regarding the management of IT systems, in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

- the management of Centre computer systems is appropriately structured and relevant responsibilities and required behaviours are suitably identified.
- all software and services will be managed and maintained in a clear and precise manner.

E2. Guidance

STAFF TRAINING

Centre systems are managed by suitably trained and qualified staff. All system management staff shall be given relevant training in information security issues.

ACCESS CONTROLS AND SERVICES

Access controls shall be maintained at appropriate levels for all Centre systems by ensuring that users are granted appropriate access rights to systems. This is also supported by the Centre Network Registration Form, Acceptable Use Policy, and ICT User Management Procedure. Any change of access permissions must be authorised either by the System Owner or another appropriately authorised person or committee.

Access to all information services will be via a secure log-on process. All access to information services is to be logged and monitored by the Centre to identify potential misuse of systems or information.

The Information Access Policy provides the relevant guidelines regarding the use of passwords within the Centre.

SYSTEM SECURITY

Access to system commands is to be restricted to those persons who are authorised to perform systems administration or management functions.

The implementation of new or upgraded software must be carefully planned and managed.

SYSTEM CAPACITY

The capacity demands of systems supporting business processes will be monitored by System Owners and various projections of future capacity requirements made to ensure that appropriate processing power, storage and network capacity is available when required.

SYSTEM PLANNING POLICY F1.

Objectives and Scope of the Policy

This Policy applies to all users of Centre IT related information systems and sets out Centre policy regarding the planning of IT systems, in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

- information systems within the Centre are appropriately specified and designed.
- any requirements or risks associated with Centre information systems will be suitably identified and risk assessed.
- information systems will be specifically designed and configured to enable appropriate security safeguards to be implemented.

F2. Guidance

SYSTEM AUTHORISATION

New information systems, or enhancements to existing systems, must be authorised via the Information Management Steering Group. The proposals and business requirements for all authorised systems must specify requirements for security controls. Where Personal Data is to be held, a Privacy Impact Assessment must be completed.

SYSTEM IMPLEMENTATION

The implementation of new or upgraded systems must be carefully planned and managed, by the relevant Project Manager or System Owner, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls.

INFORMATION ASSETS

Information assets associated with any proposed new or updated systems must be identified, classified, and recorded, in accordance with the Records Management Policy, Software Management Policy and Business Continuity Plan. The details should be held in the Information Asset Register. A risk assessment will also be undertaken to identify the probability and impact of security failure.

EQUIPMENT

Equipment supporting business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment supporting business systems shall be correctly maintained and given adequate protection from unauthorised access, environmental hazards, and electrical power failures.

ACCESS CONTROLS

Access controls for all information and information systems are to be set at appropriate levels in accordance with the Information Access Policy. Access to operating system commands and application system functions is to be restricted to those persons who are authorised to perform systems administration or management functions.

REMOTE ACCESS POLICY G1

Objectives and Scope of the Policy

This Policy applies to all users of Centre IT related information systems and sets out Centre policy regarding the remote accessibility of networks and systems, in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

- security of Centre information assets is maintained when working with mobile devices.
- Centre information assets are accessed from a mobile device in ways that are
- compliant with information security policies.
- the benefits of teleworking can be achieved without unduly increasing the risk to information assets.

G2. Guidance

MOBILE COMPUTING

The Centre will seek to protect mobile computing equipment against unauthorised access and register devices appropriately to monitor ownership and location.

Users borrowing laptops, phones and any other mobile computing equipment from the Centre will do so according to this policy and the ICT Equipment Loans Policy and Procedures.

Mobile Computing Guidelines are available for users.

NETWORK MANAGEMENT POLICY

Objectives and Scope of the Policy

This Policy applies to all users of Centre IT related information systems and sets out Centre policy regarding the management of the Centre network, in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

- The Centre adopts a continuing risk assessment approach to network management.
- Appropriate technical and procedural controls are in place to reduce the impact of potential network risks.
- Emergency measures are in place to deal with faults and incidents relating to the Centre network.

H2. Guidance

NETWORK SUPERVISION

The Centre network shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity in collaboration with individual system owners. All network management staff shall be aware of information security issues.

NETWORK PERFORMANCE

The network will be designed and configured to deliver high performance and reliability to meet Centre needs whilst providing a high degree of access control and a range of privilege restrictions.

NETWORK PROTECTION

The network will be segregated into separate logical domains with routing and access controls operating between the domains. Appropriately configured firewalls shall be used to protect the networks supporting Centre business systems.

Wireless access will be supported by appropriately configured SSIDs.

NETWORK RESOURCES

Access to the resources on the network will be strictly controlled to prevent unauthorised access and access control procedures must provide adequate safeguards through robust identification and authentication techniques. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.

NETWORK AUTHENTICATION

Any user who requires access to the Centre network will need to complete the appropriate registration forms in accordance with the Acceptable Use Policy.

CHANGE CONTROL PROCEDURES

The implementation of new or upgraded software or firmware must be carefully planned and managed. All changes must be thoroughly tested and authorised before moving to the live environment.

NETWORK ACCESS POINTS

Moves, changes and other reconfigurations of users' network access points will only be carried out by staff authorised by IT Services according to procedures laid down by them. These are subject to controlled access.

NETWORK ATTACKS

Networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised intrusion.