Information Security Policy

Organisation: Dublin Cultural Institute

Dublin Cultural Institute
34a Bachelors Walk,
Dublin 1, D01 A437, Ireland

Approved by: Jonathan Duignan / Senior Management

Effective Date: 19 DEC 2025

Review Date: 19 DEC 2026

---

1. Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of information held by Dublin Cultural Institute. This includes personal data relating to learners, staff, host families, and partners, as well as business and academic information. The policy supports compliance with data protection legislation and accreditation requirements.

---

2. Scope

This policy applies to: - All staff, teachers, and management - Temporary staff, contractors, and volunteers - Third parties with access to school information systems - All information assets, whether held electronically or in paper form

---

3. Information Security Objectives

The school aims to: - Protect personal and sensitive information from unauthorised access or disclosure - Ensure information is accurate, complete, and reliable - Ensure information is available when required for legitimate purposes - Comply with legal, regulatory, and contractual obligations

---

4. Legal and Regulatory Framework

This policy is informed by: - EU GDPR - Data Protection Act 2018 - Children First and safeguarding requirements (where information relates to minors) - Accreditation body requirements (ACELS, QQI)

---

5. Roles and Responsibilities

5.1 Senior Management

- Approve and support information security policies

- Allocate appropriate resources for information security

5.2 Data Protection Lead / IT Lead

- Oversee implementation of information security controls
- Maintain information security procedures
- Respond to information security incidents

5.3 All Staff and Users

- Comply with this policy and related procedures
- Protect login credentials and access rights
- Report information security incidents immediately

---

6. Information Classification

Information will be classified according to sensitivity: - **Public:** Information intended for public use - **Internal:** Information for internal school use only - **Confidential:** Personal data or sensitive business information - **Highly Confidential:** Special category data, safeguarding records, or financial data

Appropriate handling and security controls must be applied based on classification.

---

7. Access Control

- Access to information systems is granted on a least-privilege basis
- Unique user accounts must be used; sharing credentials is prohibited
- Access rights are reviewed regularly and removed when no longer required

---

8. Passwords and Authentication

- Strong passwords must be used for all systems
- Multi-factor authentication should be enabled where available
- Passwords must not be shared or written down insecurely

---

9. Physical Security

- Paper records are stored securely when not in use
- Offices, classrooms, and storage areas are secured outside operating hours
- Visitors must be supervised where access to information is possible

---

10. IT and Network Security

- School devices must use up-to-date security software
- Systems and applications must be kept up to date with patches
- Use of personal devices for school data must follow approved procedures

---

11. Remote Working and Mobile Devices

- Remote access must be secure and authorised
- Devices used for school data must be protected by passwords or encryption
- Loss or theft of devices must be reported immediately

---

12. Data Backup and Recovery

- Critical data is backed up regularly
- Backups are stored securely and tested periodically
- Procedures are in place to restore data in the event of loss or system failure

---

13. Information Security Incidents

All actual or suspected information security incidents must be reported immediately. This includes: - Data breaches - Loss or theft of devices - Unauthorised access to systems

Incidents will be investigated and managed in line with the school's Data Breach Response Procedure.

---

14. Third Parties and Suppliers

- Third parties with access to school information must meet appropriate security standards

- Data Processing Agreements and confidentiality clauses must be in place where required

15. Training and Awareness

- Staff receive information security and data protection training
- Regular reminders and updates are provided to maintain awareness

---

16. Monitoring and Compliance

- Compliance with this policy may be monitored
- Non-compliance may result in disciplinary action or termination of access

---

17. Policy Review

This policy will be reviewed annually or sooner if there are significant changes to systems, legislation, or risk.

Approved by: _____Jonathan Duignan_____

Date: _____19 DEC 2025_____