Cyber Security Policy v1

The Open College

Document Version	1.0
Owner	QA Office
Approved By	Academic Board
Effective Date	2025-05-01
Next Review Date	2026-05-01
Status	**Approved**

Contents

Figure 1: A close up of a sign Description automatically generated

Cyber Security Policy
The Open College

1 Document Control

Document Version
1.0
Responsibility
Leadership Team
Review Cycle
Yearly
Next Review
This policy is due for review upon publication of updated QQI QA guidelines in 2025/2026

1.1 Record of Revisions

Version	Date	Description	Approved by
1.0	May 2025	Initial Version	AB

Cyber Security Policy
Purpose:
To ensure the protection of digital assets, learner data, and institutional systems supporting fully online education, aligning with the QQI's 2023 guidelines for online provision and The Open College's commitment to quality, integrity, and responsiveness.
Scope:
Applies to all staff, learners, contractors, and third-party partners who access or manage The Open College's digital platforms, including Moodle, Microsoft 365, bespoke student databases, and integrated systems such as BigBlueButton and ScreenPal.
Principles:

- **Integrity:** Maintain accuracy, reliability, and trust in all digital systems and data.
- **Confidentiality:** Ensure data is accessible only to authorised users.
- **Availability:** Ensure systems are reliably accessible for online teaching, learning, and operations.
- **Compliance:** Adhere to GDPR, Irish legislation, and QQI data protection expectations.

Policy Areas:

1. **Access Control**

- Staff and learners are issued unique, secure credentials.
- Two-factor authentication (2FA) is mandatory for all staff accounts on Moodle and Microsoft 365.
- Role-based access is enforced across all platforms.

2. **Data Protection**

- All systems storing personal data are hosted within the EU and managed under GDPR-compliant agreements.
- Sensitive data is encrypted at rest and in transit.
- The college database and LMS undergo daily encrypted backups, retained for 30 days.

3. **System Security**

- Moodle is hosted via Enovation with SLA guarantees, regular patching, and real-time monitoring.
- Microsoft 365 is used for internal communications and document control, with access logs and audit trails enabled.
- Vulnerability scanning is conducted quarterly, and penetration testing is reviewed annually.

4. **Incident Response**

- A formal incident response plan is maintained, led by the Operations Manager.
- Security breaches must be reported within 24 hours.
- Incident logs and post-mortem reports are maintained to improve resilience.

5. **Staff and Learner Awareness**

- Cybersecurity training is included in all staff induction and updated annually.
- Learners receive guidance on safe digital practices during onboarding and via Moodle prompts.
- Phishing simulations and awareness campaigns are run bi-annually.

6. **Third-Party Risk Management**

- All third-party vendors must sign a data protection and security agreement before integration.
- The IT Support reviews third-party compliance annually.

7. Business Continuity

- In the event of a cyber incident, the contingency protocol activates Teams and email as communication backups.
- Critical recovery time (RTO) is 24 hours; data recovery point (RPO) is 24 hours.

Monitoring and Review:

- The IT Support and Education Technologist perform quarterly security reviews.
- Annual external audits are conducted as part of the QA review cycle.
- Any incidents, updates, or threats are reported in quarterly Leadership Team meetings.