I-PATH
International Performing
Arts & Theatre

CYBER SECURITY POLICY

Policy Owner: Head Office
Oversight Committee: Examinations & Standards Committee
Approval Body: Grand Council
Applies to: All staff, examiners, trustees, consultants, contractors and third-party providers
Review Cycle: Annual, or following a significant incident or regulatory change

1. Purpose

This policy sets out how International Performing Arts & Theatre Limited (I-PATH) identifies, manages and mitigates cyber security risks in order to:

- protect the confidentiality, integrity and availability of data
- safeguard assessment materials, learner evidence, results and certification
- ensure the secure delivery of examinations and qualifications
- support business continuity and resilience
- maintain public confidence in I-PATH qualifications
- meet Ofqual expectations, UK GDPR and other relevant legal and regulatory requirements

Cyber security is recognised as a critical component of qualification integrity and organisational governance.

2. Scope

This policy applies to:

- all I-PATH staff and office holders
- all I-PATH examiners and moderators
- all contractors, consultants and agents
- all third-party suppliers processing data or providing systems on behalf of I-PATH
- all systems, platforms, devices and data used for:
    - assessment delivery
    - marking and moderation
    - results processing and certification
    - centre approval and governance
    - regulatory reporting

3. Governance and Accountability

3.1 Strategic Oversight

The Grand Council holds ultimate responsibility for cyber security and information risk and is responsible for:

- approving this policy and any material amendments
- ensuring appropriate resources are allocated
- receiving assurance on cyber risk and incidents

The Examinations & Standards Committee provides oversight where cyber risks impact assessment integrity or regulatory compliance.

3.2 Operational Responsibility

I-PATH appoints a Designated Cyber Lead (or equivalent role) responsible for:

- day-to-day implementation of cyber security controls
- maintaining the cyber risk register
- coordinating incident response and recovery
- liaising with awarding organisations, regulators, the ICO and external specialists where required

3.3 Individual Responsibilities

All individuals working for or on behalf of I-PATH must:

- comply with this policy and related procedures
- follow secure working practices
- protect login credentials and devices
- complete mandatory cyber awareness training
- report suspected or actual cyber incidents immediately

Failure to comply may result in disciplinary or contractual action.

4. Cyber Risk Management

4.1 Risk Identification

I-PATH maintains an up-to-date risk register which includes cyber and information security risks, such as:

- phishing, malware and ransomware
- unauthorised access to systems or assessment materials
- loss or compromise of learner, centre or examiner data
- system outages affecting assessment delivery or results
- third-party or supplier failures

Risks are assessed for likelihood and impact and reviewed regularly.

4.2 Risk Mitigation and Controls

Proportionate technical and organisational controls are implemented, including:

- strong password and authentication requirements

- role-based access and least-privilege principles
- secure user account management
- up-to-date malware and endpoint protection
- regular patching and system updates
- encryption of sensitive data in transit and at rest
- secure configuration of cloud platforms and databases
- regular, tested backups of critical data and systems
- logging and monitoring for suspicious activity
- restrictions on removable media and unauthorised software

4.3 Business Continuity and Resilience

To support Ofqual expectations on resilience:

- I-PATH maintains business continuity and incident contingency arrangements covering cyber events
- systems critical to assessment, marking, results and certification are prioritised for recovery
- contingency arrangements are reviewed following incidents or significant system change

This policy operates alongside the Emergency, Crisis and Business Continuity Guidance Policy.

5. Cyber Security Incidents

5.1 Definition

A cyber security incident may include (but is not limited to):

- data breaches or loss of personal data
- ransomware, malware or phishing attacks
- unauthorised access to systems or assessment content
- disruption to systems supporting examinations or results
- compromise of user credentials

5.2 Reporting

All suspected or actual cyber incidents must be reported immediately to the Designated Cyber Lead.

5.3 Response and Mitigation

In the event of an incident, I-PATH will:

- act promptly to contain and limit impact
- isolate affected systems where necessary
- preserve evidence and audit logs
- restore systems and data securely
- prioritise protection of learner outcomes and qualification integrity

5.4 Notification and Communication

Where required, I-PATH will:

- notify the awarding organisation promptly where assessment integrity, compliance or public confidence may be affected
- notify the Information Commissioner's Office (ICO) and affected individuals in line with UK GDPR
- manage internal and external communications carefully to avoid misinformation

5.5 Post-Incident Review

Following an incident, I-PATH will:

- conduct a root-cause analysis
- document lessons learned
- strengthen controls and training
- report outcomes to senior leadership and the Grand Council

6. Data Protection and Information Integrity

I-PATH ensures that:

- personal data is processed lawfully, fairly and securely
- access to sensitive information (including assessment materials and results) is tightly controlled
- user access rights are reviewed regularly and revoked when no longer required
- audit trails are maintained for key systems and decisions
- third-party processors meet equivalent security standards

7. Third-Party and Supplier Assurance

Third-party providers must:

- comply with I-PATH's cyber security and data protection requirements
- implement appropriate technical and organisational safeguards
- notify I-PATH promptly of any incidents affecting I-PATH data or services
- cooperate with audits or assurance checks where required

8. Training and Awareness

To maintain a strong security culture:

- all staff, examiners and relevant contractors receive regular cyber security and data protection training
- phishing awareness and safe digital working practices are reinforced
- cyber security responsibilities form part of induction processes

9. Monitoring, Compliance and Enforcement

- Compliance with this policy is mandatory
- I-PATH reserves the right to monitor system use, audit access and suspend accounts where risk is identified
- Breaches may result in disciplinary action, termination of contract, or escalation under the Malpractice and Maladministration Policy

10. Review and Approval

This policy is reviewed:

- annually
- following any significant cyber incident
- after material changes to systems, suppliers or regulatory expectations

All updates require approval by the Grand Council.

Designated Cyber Lead: David Stinson