POINT BLANK
MUSIC SCHOOL

POLICY 069
Information and Cyber Security Policy

DOCUMENT CONTROL BOX

SCOPE						
Course Type	**BA(Hons)**	x	**CertHE**	x	**Professional/ Auditing**	x
School	**London**	x	**Online**	x	**International**	
Version	1.0			**Date Approved**	February 2024	
Date of Next Review	August 2024					
Publication	**Staff Access**			X		
	Student Access			X		
	Public Access via Website			X		

If you have a disability which makes reading this document or navigating our website difficult and you would like to receive information in an alternative format, please contact: support@pointblankmusicschool.com.

Document Revision History

Version Log

Committee / Approval Date	Author	Version	Publication Date	Page Reference & Summary

Related Documentation

Document Reference No. (Policy version / Supporting doc. #)	Document Type	Link or Dept. Owner	Document Title
			Data Breach and Incident Management Policy.
	Policy		Data Protection Policy.

1. PURPOSE

This Information and Cyber Security Policy is integral to Point Blank Music School's commitment to protect the information we collect, analyse, store, communicate, and report. Such information is susceptible to threats like theft, misuse, loss, and corruption (e.g. a ransomware attack). Moreover, the systems that manage this information are also at risk, especially when faced with inadequate education, training, and breaches in security controls.

We are acutely aware that incidents of information security can lead to serious consequences, including but not limited to, embarrassment, financial loss, and non-compliance with legal and regulatory standards. Furthermore, such incidents could potentially result in legal actions being taken against the school. Therefore, this policy has been developed not only to address these risks but also to sit alongside the Data Breach and Incident Management Policy, and Data Protection Policy. Together, they provide a comprehensive framework for managing the school's information security and cyber risks.

By integrating these policies, we aim to maintain a high level of vigilance and resilience against information security threats. This approach is essential in safeguarding our digital environment, ensuring the confidentiality, integrity, and availability of our information assets, and supporting our overall risk management strategy. This policy forms the foundation of our commitment to uphold a secure digital space for our educational community, where information is protected against various digital threats.

This comprehensive Information and Cyber Security Policy at Point Blank School is essential to safeguarding sensitive information in today’s digitally driven educational environment. With the increasing reliance on digital technologies for teaching, administration, and data management, the school faces various risks such as data breaches, cyber threats, and information misuse. This policy will provide a structured framework to protect against these risks, ensuring the confidentiality, integrity, and availability of critical information. It aligns with best practices and regulatory requirements, thereby reinforcing the school’s commitment to maintaining a secure and trustworthy educational setting. It emphases the importance of regular reviews and updates, the policy ensures that Point Blank School remains resilient and adaptable to evolving cybersecurity challenges.

Point Blank's security objectives are to:

1. Integrate Security in IT Development: Ensure information security is a fundamental principle in the development and procurement of IT systems.
2. Secure Access and Sharing: Enable authorised users to securely access and share information, crucial for performing their roles effectively.
3. Balance Controls with User Experience: Achieve a balance between physical, procedural, and technical controls and user experience, ensuring robust security without compromising usability.
4. Fulfil Legal Obligations: Understand and meet all contractual and legal obligations related to information security.
5. Incorporate Security in School Activities: Embed information security considerations in all teaching, research, and administrative activities.
6. Raise Security Awareness: Ensure all individuals accessing our information are fully aware of their information security responsibilities.
7. Responsive Incident Management: Effectively resolve incidents affecting our information assets and use these experiences to enhance our resilience.

8. Risk Management: Proactively identify, manage, and treat information risks in line with an agreed-upon risk tolerance level.

2. POLICY DETAILS

Point Blank Music School is committed to safeguarding its information, and this policy ensures the secure handling and management of all information within the school through the following principles:

- Confidentiality: Only authorised individuals will have access to information, ensuring it remains confidential.
- Integrity: We will maintain the accuracy and completeness of our information at all times.
- Availability: Information will be readily accessible to authorised users and necessary processes whenever it is needed.

Point Blank Music School adheres to the Department for Education's cyber guidance, complementing this with the protocols outlined in the Cyber Essentials framework and incorporating recommendations from the National Cyber Security Centre (NCSC). This approach ensures that the school's cybersecurity measures align with national educational standards and cater to the specific needs of stakeholders, including partners and external collaborators. By prioritising these guidelines in its cybersecurity strategy, Point Blank Music School shows a firm commitment to sustaining a secure and resilient digital environment.

Point blank will adopt a risk-based approach to the application of controls:

1. INFORMATION SECURITY POLICIES

A set of lower level controls, processes and procedures for information security will be defined, in support of the high level Information Security Policy and its stated objectives. This suite of supporting documentation will be approved by the Governance Board and communicated to users and relevant external parties.

2. ORGANISATION OF INFORMATION SECURITY

Point Blank will define and implement suitable governance arrangements for the management of information security. This will include identification and allocation of security responsibilities, to initiate and control the implementation and operation of information security within the school.

Point Blank will appoint at least:

- a Governance Board to influence, oversee and promote the effective management of information held by Point Blank
- an Executive to chair the Governance Board and take accountability for information and cyber risk
- an Information Security specialist to lead the information security function

- Information Asset Owners (IAOs) to assume local accountability for information management; and Information Asset Managers (IAMs) responsible for day-to-day information management

3. HUMAN RESOURCES SECURITY

Point Blanks security policies and expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities. Information security education and training will be made available to all staff, and poor and inappropriate behaviour will be addressed.

Where practical, security responsibilities will be included in role descriptions, person specifications and personal development plans.

4. ASSET MANAGEMENT

All assets (information, software, electronic information processing equipment, service utilities and people) will be documented and accounted for. Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.

All information assets will be classified according to their legal requirements, business value, criticality and sensitivity, and classification will indicate appropriate handling requirements. All information assets will have a defined retention and disposal schedule.

5. ACCESS CONTROL

Access to systems and information will be controlled and audited, and will be driven by business requirements. Access will be granted or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include mandatory authentication methods based on the sensitivity of the information being accessed, and will include consideration of multiple factors and device settings as appropriate.

Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented where practical.

6. CRYPTOGRAPHY

Point Blank will provide guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, integrity and authenticity of information and systems.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

Information processing facilities will be housed in secure areas, physically protected from unauthorised access, damage and interference by defined security perimeters. Layered internal and external security controls will be in place to deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive. This includes where we use third party services to process information.

8. OPERATIONS SECURITY

Point Blank will ensure the correct and secure operations of information processing systems. This will include documented operating procedures; the use of formal change and capacity management; controls against malware; defined use of logging; vulnerability management.

9. COMMUNICATIONS SECURITY

Point Blank will maintain network security controls to ensure the protection of information within its networks, and provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities, in line with the classification and handling requirements associated with that information.

10. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

Controls to mitigate any risks identified will be implemented where appropriate.

Systems development will be subject to change control and separation of test, development and operational environments.

11. SUPPLIER RELATIONSHIPS

Point Blanks information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected.

Supplier activity will be monitored and audited according to the value of the assets and the associated risks.

12. INFORMATION SECURITY INCIDENT MANAGEMENT

Guidance will be available on what constitutes an Information Security incident and how this should be reported. Actual or suspected breaches of information security must be reported and will be investigated. Appropriate corrective action will be taken and any learning built in to controls.

13. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Point Blank will have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely recovery in line with documented business needs.

This will include appropriate backup routines and built-in resilience.

Business continuity plans must be maintained and tested in support of this policy. Business impact analysis will be undertaken of the consequences of disasters, security failures, and lack of service availability.

14. COMPLIANCE

The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements.

Currently this includes data protection legislation, the payment card industry standard (PCI-DSS), the Government's Prevent guidance and Point Blanks contractual commitments.

Point Blank will use a combination of internal and external audit to demonstrate compliance against chosen standards and best practice, including against internal policies and procedures.

This will include penetration tests, gap analysis against documented standards, internal checks on staff compliance, and returns from Information Asset Owners.

3. POLICY SCOPE

The Information and Cyber Security Policy and its supporting controls, processes and procedures apply to all information used at Point Blank, in all formats. This includes information processed by other organisations in their dealings with Point Blank.

The Information and Cyber Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to our information and technologies, including external parties that provide information processing services to Point Blank.

A detailed scope, including a breakdown of users, information assets and information processing systems, is included in the supporting Information Security Management System (ISMS) documentation.

4. RELATED POLICIES

Data Breach and Incident Management Policy.
Data Protection Policy.

5. POLICY OWNER

This policy is under the responsibility of the Executive Committee. The responsible committee will ensure the cyclical review of this policy is carried out in line with Point Blank's Quality Assurance Framework.

The Executive Committee delegates the operational responsibility of this policy to the following staff:

- *IT Manager*
- DPO

6. PROCEDURES

The relevant procedure(s) to accompany this policy are confidential and subject to change to reflect the current operating procedures and security risk profile.

7. EXHIBITS, APPENDICES AND FORMS

There are no further relevant exhibits, appendices or forms.

8. REFERENCES AND SUPPORTING INFORMATION

8.1 Built with security guidance from:
National Cyber Security Centre - NCSC.GOV.UK
National Institute of Standards and Technology (nist.gov)

9. DOCUMENT HISTORY AND NEXT REVIEW

Version:	1.0
Approved on:	20.02.24
Approved by:	Executive Committee
Date of Next Review:	August 2024