BRISTOL OLD VIC THEATRE SCHOOL

Information Security Policy

1 Introduction

The continued confidentiality, integrity and availability of information systems underpin the operations of Bristol Old Vic Theatre School (BOVTS, 'the School') . A failure to secure information systems would jeopardise the ability of the School to fulfil its mission of delivering world-class teaching and have greater long-term impact through the consequential risk of financial or reputational loss.

This Information Security Policy provides the guiding principles and responsibilities of all members of the School required to safeguard its information systems. Other supporting School policies, procedures and guidelines will give greater detail on specific subject areas.

The Data Protection Officer will lead the School commitment to deliver a successful implementation of information security management, but this will only be possible if all members of the School community are aware of and carry out their own personal responsibilities.

1.1 Purpose of Policy

The intention of this policy is to:

Protect the information systems managed by the School from security threats and mitigate risks that cannot be directly countered, ensuring the confidentiality, integrity, and availability of School data.

Ensure that all members of the School are aware of and able to comply with relevant UK and EU legislation related to information security, data protection, and privacy.

Educate and empower all users to understand their personal responsibilities in protecting the confidentiality and integrity of the data they access, and to comply with this policy and other supporting policies.

Safeguard the reputation and business of the School by ensuring its ability to meet its legal obligations and to protect it from liability or damage through misuse of its IT facilities, including data breaches or unauthorised access.

Promote a culture of continuous improvement in information security by conducting timely reviews of policies and procedures in response to feedback, changes in legislation, emerging threats, and other factors, in order to enhance ongoing security measures and practices.

1.2 Scope

This Information Security Policy applies to:

All members of the Bristol Old Vic Theatre School, including faculty, staff, students, volunteers, contractors, and any other individuals with access to School information systems.

All third parties who interact with School information, including vendors, partners, contractors, consultants, and other external entities.

All systems used to store, process, or transmit School information, including but not limited to computers, servers, laptops, mobile devices, networks, databases, cloud services, and any other IT infrastructure owned, operated, or used by the School.

This policy is applicable to all individuals and entities mentioned above, and compliance with this policy is mandatory to ensure the protection and security of School information and systems.

2 **Policy**

2.1 Awareness and communication

All authorised users will be provided with information about this policy and supporting policies and guidelines when their account is issued. Updates to guidance will be communicated through the School's website and will be highlighted at major points of interaction with individuals, as deemed

appropriate for the change. This may include email notifications, system alerts, or other forms of communication to ensure that users are aware of any updates or changes to the information security policies and guidelines. It is the responsibility of all users to regularly review and comply with the most current version of the policies and guidelines to maintain a secure information environment at the Bristol Old Vic Theatre School.

2.2 Definitions

School - Bristol Old Vic Theatre School.

Staff – Staff, whether academic, administrative, technical, or other, currently employed by the School, or engaged on a contract of service.

Student – An individual currently enrolled or registered with the School, or undertaking study of any kind provided by, at, or under the auspices of, the School.

Visitor – An individual, other than Stuff or Students, who uses the School IT Systems in any way.

School IT Systems – any of the School's IT facilities, including email, connection from the School's sites to the Internet and other networks, and all computers, laptops, other mobile devices, and any other related software and hardware.

Information Asset Owner - These will be individuals in the School who hold the responsibility for ensuring that IT assets in their particular area are processed and shared.

Data Manager - Subject matter experts who are responsible for business definitions and the quality of data sets within a data domain (e.g. defining terms such as "applicant," or "course" in the student registry domain).

Data Manager – The Data Manager is responsible for the safe custody, transport, storage of the data and implementation of business rules.

2.3 Information Security Principles

The following principles provide a framework for the security and management of the School's information and information systems.

Information Classification: All information should be classified in accordance with any legislative, regulatory, or contractual requirements that may increase the sensitivity of the information and its security requirements.

Proper Handling of Information: All individuals covered by the scope of this policy must handle information appropriately in accordance with its classification level, relevant laws, regulations, and policies.

Need-to-Know Principle: Information should only be made available to those individuals who have a legitimate need for access in order to perform their job duties or responsibilities. Access to information should be granted based on role-based permissions and least privilege principles.

Unauthorised Access Protection: Information should be protected against unauthorised access and processing. This includes implementing appropriate technical, administrative, and physical safeguards such as strong authentication, access controls, and audit trails to prevent unauthorised access or data breaches.

Data Loss Prevention: Measures should be in place to protect information against loss and corruption. This may include regular data backups, redundant storage, and disaster recovery plans to ensure business continuity in case of data loss or system failure.

Secure Disposal of Information: Information should be disposed of securely and in a timely manner, in accordance with the appropriate measures based on its classification level. This may include shredding, secure deletion, or other approved methods for disposal of information in compliance with relevant data protection regulations.

Breach Reporting: Any breaches of this policy must be reported by anyone who becomes aware of the breach in a timely manner, following the School's established incident reporting procedures, including reporting breaches to the Information Commissioner's Office - https://ico.org.uk/

Reporting breaches promptly allows for timely investigation, containment, and mitigation of potential security incidents.

IT security awareness training: Relevant training will be in place to assist staff in their day-to-day handling of information. All new staff must complete the School's mandatory information security training (online) to ensure they are aware of the risks and their responsibilities in handling information. Staff will be

required to complete refresher training annually reflecting any changes and updates in information governance best practice.

By adhering to these principles, the School aims to ensure the confidentiality, integrity, and availability of its information assets and maintain a secure information environment.

2.4 Legal and regulatory obligations

The Bristol Old Vic Theatre School and its staff/students/users/members must adhere to all current UK legislation as well as regulatory and contractual requirements. The School provides policy statements and guidance for staff and students in relation to compliance with relevant legislation to help prevent breaches of the School's legal obligations. However, individuals are ultimately responsible for ensuring that they do not breach legal requirements.

Users of the School's online or network services, or when using or processing Information Assets, are individually responsible for their activity and must be aware of the relevant legal requirements when using such services.

2.5 Information Classification

An Information Classification levels framework would be established which are part of the Information Security Principles. The Information classification includes definitions from the Data Protection Policy.

Category - Highly Restricted

Description

Highly confidential information whose inappropriate disclosure would be likely to cause serious damage or distress to individuals and/or constitute unfair/unlawful processing of "sensitive personal data" under the Data Protection Act; and/or seriously damage the School's interests and reputation; and/or significantly threaten the security/safety of the School and its staff/students.

Examples

Sensitive personal data relating to identifiable living individuals

Individual's bank details

Large aggregates (>1000 records) of personal data such as personal contact details

Non-public information that facilitates protection of individuals' safety or security of key functions and assets e.g. network passwords and access codes for higher risk areas

Category - Restricted

Description

Confidential information whose inappropriate disclosure would be likely to cause a negative impact on individuals and/or constitute unfair/unlawful processing of "personal data" under the Data Protection Act; and/or damage the School's commercial interests, and/or have some negative impact on the School's reputation.

Examples

Personal data relating to identifiable living individuals

Student assessment marks

Staff contact details

Research data or information or IP with commercial value/obligation

Category - Internal Use

Description

Information not considered being public which should be shared only internally but would not cause substantive damage to the School and/or individuals if disclosed.

Examples

Non-confidential internal correspondence e.g. routine administration such as meeting room and catering arrangements

Final working group papers and minutes

Internal policies and procedures

2.6 Compliance and Incident notification

Compliance with the information security policy at the Bristol Old Vic Theatre School is imperative for all users of information systems. Any breach of information security is a serious matter that may result in the loss of confidentiality, integrity, or availability of personal or other confidential data. Such breaches could lead to criminal or civil action against the School, as well as potential business loss and financial penalties.

In the event of an actual or suspected breach of this policy, it must be immediately reported to the Data Protection Officer in accordance with the incident investigation procedure. All reported security incidents will be thoroughly investigated, and appropriate actions will be taken in line with this policy, the Acceptable Use Policy, School disciplinary policy, and relevant laws and regulations.

If the breach involves personal data, the Data Protection team must be promptly notified in accordance with the School's Data Protection Policy.

Compliance with this policy should also be incorporated as a contractual requirement with any third party that may have access to School systems or data.

By promptly reporting and addressing breaches, and ensuring compliance with this policy, the School aims to safeguard its information assets, protect against

potential legal and financial risks, and maintain a secure information environment for the benefit of all users.

3 **Responsibilities**

3.1 Individuals

Individuals must adhere to the Acceptable Use Policy and follow relevant supporting procedures and guidance. An individual should only access systems and information they have a legitimate right to and not knowingly attempt to gain illegitimate access to other information. Individuals must not aid or allow access for other individuals in attempts to gain illegitimate access to data. In particular, individuals should adhere to the information security 'dos and don'ts' outlined in the table below.

Do/Do Not
Do use a strong password and change it if you think it may have been compromised. Don't give your password to anyone.
Do report any loss or suspected loss of data. Don't reuse your School password for any other account.
Do be on your guard for fake emails or phone calls requesting confidential information - report anything suspicious to the DD&T service desk. Don't open suspicious documents or links.
Do keep software up to date and use antivirus on all possible devices. Don't undermine the security of School systems.
Do be mindful of risks using public Wi-Fi or computers. Don't provide access to School information or systems.
Do ensure School data is stored on School systems. Don't copy confidential School information without permission.
Do password protect and encrypt your personally owned devices. Don't leave your computers or phones unlocked.

3.2 Data Protection Officer (DPO)

In accordance with the GDPR the School has appointed a Data Protection Officer to carry out the DPO role as defined in the legislation. The DPO is responsible for providing advice and assistance on all matters relating to data protection, including drafting data protection statements for forms and questionnaires, advising on requests for access to personal data, responding to queries on data protection issues, overseeing the School's data protection compliance.

3.3 Data Custodians

Data custodians are responsible for the information systems that hold data and are typically systems administrators. In addition to their individual responsibilities 3.1 they must:

Ensure that the physical and network security of systems is maintained.

Ensure that the systems they maintain are suitably configured, maintained and developed.

Ensure that the data are appropriately stored and backed up.

Ensure that appropriate access controls are in place to meet the requirements of Data Stewards.

Understand and document risks, take suitable steps to mitigate and ensure that these are understood by Information Asset owners.

Document operational procedures and responsibilities of staff.

Publish procedures for users of the systems to allow secure access and usage.

Ensure that systems are compliant with legal and other contractual requirements.

4 Supporting Regulations, Policies and Guidelines

Other policies issued by Bristol Old Vic Theatre School support and reinforce this policy statement. These include but are not limited to:

The following policies and procedures are related to the information security policy:

Choosing a password

School regulations

Data Protection Policy

Information Classification Framework

IT Acceptable Use Policy

4.1 Payment Card Industry Data Security Standard (PCI DSS)

The School must comply with the Payment Card Industry Data Security Standard (PCI DSS) when processing payment (credit/debit) cards. Details of the standards can be found HERE.

5 Policy Review

The School will review this policy when required to ensure that it remains appropriate and up to date. Any questions or concerns should be made to the IT Security Team.

Owner	Data Protection Officer
Approval Date	October 2024
Approved By:	Director of Studies
Date of last review:	N/A
Date of next review:	October 2025