IT Acceptable Use Policy

1. Purpose

The purpose of this policy is to set out the expectations placed on staff, students and authorised third parties in relation to their use of all electronic communications facilities, equipment and services provided by Bristol Old Vic Theatre School ('the School').

The Acceptable Use Policy (AUP) for IT Systems is designed to protect the School, our employees, students and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Everyone who works or studies at the School is responsible for the security of our IT systems and the data on them. As such, all users must ensure they adhere to the guidelines in this policy at all times. Should any user be unclear on the policy or how it impacts their role they should speak to their manager, tutor or a member of Senior Management

2. Definitions

"Users" are anyone who has access to any of the School's IT systems. This includes permanent employees, temporary employees, students, and any authorised third parties.

"Systems" means all IT equipment that connects to the School's network or accesses the School's applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

3. Scope

This is a universal policy that applies to all students, staff and authorised third parties. It relates to all IT systems owned, leased, hired or otherwise provided by the School, whether accessed on the School's premises or remotely.

4. Compliance with Legislation

The School has a statutory duty under the Counter Terrorism and Security Act 2015, which is termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism. The PREVENT duty informs the School's policy on the acceptable use of IT systems.

Individuals must also be aware of their responsibilities under additional legislation listed below:

Computer Misuse Act 1990

Data Protection Act 1998

Regulation of Investigatory Powers Act 2000

Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000

Terrorism Act 2006

Counter-Terrorism and Security Act 2015

5. Responsibility

It is the responsibility of all students, staff and authorised third parties to ensure that when using the School' IT systems, their behaviours and activities are in accordance with the requirements of this policy.

Access to the School's IT systems is controlled by the use of User ID's and passwords.
All User IDs and passwords are uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the School's IT systems.
User IDs and /or passwords must be changed if there is any suspicion that they have been compromised.

Line Managers are responsible for ensuring that individual staff are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Students and authorised third parties will be made aware of this Policy and the limits of their authority as part of their induction.

Individuals must not:

- Allow anyone else to use their user ID and password on any IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Leave confidential material unattended.
- Dispose of business-related printed material by any means other than via confidential waste bins, bags or shredders.
- Use someone else's user ID and password to access IT systems.
- Leave their password unprotected (for example writing it down on a piece of paper).
- Attempt to perform any unauthorised changes to IT systems or information.
- Attempt to access data that they are not authorised to access or use.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-School authorised device to the corporate network or IT systems (such as personal laptops), except when connecting to authorised guest systems where these exist.
- Store the School's data on any non-authorised equipment.
- Give or transfer the School's data or software to any other person or organisation outside of the School without the authority of a member of senior management and/or the IT department.

6. Acceptable use of internet, social media and email

The use of internet, social media and email is intended for work use and/or to aid in studies. Personal use is permitted where such use does not affect the individual's work/study performance (i.e. at lunchtime), is not detrimental to the School in any way, does not breach of any term and condition of employment and does not place the individual or the School in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet, social media and email systems.

Individuals must not:

- Use the internet, social media or email for the purposes of harassment or abuse.
- Use the internet, social media or email to promote or encourage extremism or radicalisation.
- Use profanity, obscenities, or derogatory remarks in communications of any type.

- Access, download, send or receive any data (including images), which the School considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to the School, alter any information about it, or express any opinion about the School unless they are specifically authorised to do so.
- Send unprotected sensitive or confidential information externally.
- Forward the School's (internal) mail to personal (non-School) email accounts (for example an external personal Hotmail account).
- Make official commitments through the internet or email on behalf of the School unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property rights.
- Download any software from the internet without prior approval of the IT Department.
- Connect School devices to the internet using non-standard connections.

7. Equipment

The following statements define restrictions regarding the use of personal and School provided equipment.

It is accepted that laptops and mobile devices will be taken off-site and all School laptops are configured by default for use with remote access. Remote access (staff only) is the preferred method for working offsite. When using remote access, all data remains onsite and protected. However, the following controls must be applied

- Equipment and media taken off-site must not be left unattended in public places.
- School laptops must be carried as hand luggage when travelling.
- School equipment used off-site must be protected at least by a password or a PIN and, where available, encryption.
- Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable.
- No data should be taken offsite on mobile storage devices for security and data protection reasons.
- Only School-authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

8. Software and viruses

Only authorised software must be used on the School's IT systems and must be used in accordance with the software supplier's licensing agreements. All software must be approved and installed by the School before use.

The School has implemented centralised, automated virus detection and virus software updates. All PCs have antivirus software installed to detect and remove any virus automatically.
Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved anti-virus software and procedures.

9. Monitoring and Filtering

All data that is created and stored on the School's computers is the property of the School and there is no official provision for individual data privacy. However wherever possible the School will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy.

The School has the right (under certain conditions) to monitor activity on its systems, including internet, email and social media use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

The School employs filtering of web content to prevent users from accessing illegal or inappropriate material. Examples of filtered web content include but are not limited to:-

- content from sites that are illegal or which encourage illegal activity.
- content that is likely to draw people into terrorism.
- content that is obscene or deliberately offensive.
- content that is likely to result in harassment or bullying of others.
- content that may compromise the School's IT security

In the event that users attempt to access blocked material, a message will be displayed advising that access to the website has been blocked in accordance with the IT Acceptable Use Policy

If, for valid academic reasons, staff require access to material that would ordinarily be blocked, they can request access by contacting the Finance Director to authorise access from our IT consultants.

10. Consequences of Policy Breach

All breaches of this policy will be investigated. Where investigation reveals misconduct, disciplinary action may follow in line with the School's disciplinary policies and procedures.

11. Further Information

This policy should be read in conjunction with the School's Safeguarding Policy and Procedures and the School's Data Protection and Access to Information Policy and Procedures.

User Agreement Form

This form relates to the IT Acceptable Use Policy to which it is attached.

Please complete the sections below to indicate that you have read, understood and agree to the terms of the policy

Access to the School's IT systems cannot be granted until a signed agreement form has been received.

If you have any questions regarding the IT Acceptable Use Policy, please contact your line manager, tutor or a member of Senior Management

---

I have read and understand the IT Acceptable Use Policy and agree to the terms when using the School's IT systems both on-site and off-site.

Name (Printed): .....

Date: .....

Role: .....

Signature: .....

Please retain a signed copy of this agreement and return the original to:

HE Administration & Student Support Manager, Bristol Old Vic Theatre School, 1-2 Downside Road, Clifton, Bristol BS8 2XF
