Central School of Ballet
Acceptable Use Policy for IT Systems

1. Introduction

This Acceptable Use Policy (AUP) for IT Systems is designed to protect Central School of Ballet, 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.

2. Definitions

"Users" are everyone who has access to any of CSB's IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, students, visitors and business partners.

"Systems" means all IT equipment that connects to the corporate network or access corporate 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 Users and all Systems. For some Users and/or some Systems a more specific policy exists (such as for our students): in such cases the more specific policy has precedence in areas where they conflict, but otherwise both policies apply on all other points.

This policy covers only internal use of CSB's systems, and does not cover use of our products or services by third parties.

Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.

CSB 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. This Prevent duty informs its policy on the acceptable use of IT systems.

Staff members at CSB who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

Links to local laws and legislation relating to this document are provided at the end of this document (if you are reading this in an electronic format) or copies can be obtained from the IT department.

4. Use of IT Systems

4.1 Computer Access Control – Individual's Responsibility

Access to CSB's IT systems is controlled by the use of User IDs and passwords.

Usernames and passwords are assigned to students, for both logging onto a computer and individual emails, and consequently, all individuals are accountable for all actions on CSB's IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any IT system.
- Share passwords via email.
- Leave their user accounts logged in at an unattended and unlocked computer.
- 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.
- Connect any non-CSB authorised device to the corporate network or IT systems (such as personal laptops), except when connecting to authorised guest systems such as Wi-Fi
- Store CSB data on any non-authorised equipment.
- Give or transfer CSB data or software to any other person or organisation outside of CSB without the authority of a member of senior management and/or the IT department.

4.2 Internet, social media and email - conditions of use

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 CSB in any way, not in breach of any term and condition of enrolment and does not place the individual or CSB in breach of statutory or other legal obligations.

5. Software

Users must use only software that is authorised by CSB on CSB's computers.

Authorised software must be used in accordance with the software supplier's licensing agreements. All software on CSB computers must be approved and installed by the IT department.

Individuals must not:

Store personal files such as music, video, photographs or games on CSB IT equipment.

6. Viruses

The IT department 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.

7. Actions upon Termination of Enrolment

All CSB equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned after the period of study.

All CSB data or intellectual property developed or gained during the period of study remains the property of CSB and must not be retained beyond termination or reused for any other purpose.

8. Monitoring and Filtering

All data that is created and stored on CSB computers is the property of CSB and there is no official provision for individual data privacy, however wherever possible CSB 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.
CSB 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 2018 and General Date Protection Regulation, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.