SECTION 4.3.3: INFORMATION COMMUNICATIONS TECHNOLOGY AND CYBER SECURITY POLICY

The Australian Ballet School

RESPONSIBLE: Audit Risk and Compliance Committee (ARCC)
VERSION 1 APPROVED BY THE BOARD: April 2020
LATEST VERSION: October 2023
REVIEW DATE: 2024 (to reflect the Digital Transformation Project; thereafter every 3 years or earlier depending on regulatory or organisational requirements)
POLICY ACCESS LOCATION: Staff Portal and Student Portal

1. PURPOSE

The purpose of this policy is to ensure all electronic communications of The Australian Ballet School (School) are used efficiently, suitably and to safeguard the School from any cyber security risks.

As the development of digital systems to manage learning, teaching, communications, and information at the School continues to develop, there is the likelihood of increased complexity as the electronic systems and technological standards start to accumulate and, the impact of a security breach may become relevant. The School must continue to adapt to changing technological circumstances.

The impact of cyber-crime or the failure to focus on **Cyber Security** can have a serious effect on the running of an organisation. For the School, damage can occur in a number of ways, notably from error, fraud, service interruptions, the theft of its business/corporate information, its creative/intellectual property or any sensitive information, including personal records which are maintained by the School.

Related policies: This policy should be read in conjunction with Business Continuity Policy (1.5.3), Media Relations Policy (3.1.1), Social Media Policy (3.1.2) Intellectual Property and Copyright Policy (4.2), Appropriate Use of Technology Policy (4.3), and the *Marilyn Rowe House Student and Parent Handbook*.

2. WHO DOES THIS POLICY APPLY TO

This policy applies to all members of the **School Community**.

3. DEFINITIONS

Attribution: acknowledgement of the original creator when their work is reproduced or communicated.

Cyber Security: or information technology security is the protection of computer systems, cloud storage networks and programs from the disruption, misdirection or unauthorised use of the services provided, as well as the theft of or damage to their hardware, software or electronic data, and also from the disruption, modification or misdirection of the services they provide.

DNS blocking/filtering (Domain Name System): a strategy making it difficult for users to locate specific websites or domains on the internet. Originally introduced to block spam email from unknown, malicious IP addresses. Protects against **Malware** and **Phishing** at the source. Web security issues are particularly critical for the School in support of the safety and protection of students.

Information Communications Technologies (ICT): refers to a diverse group of technologies that provide access to information primarily through telecommunications technologies and covers devices that will store, retrieve/manage, transmit or receive information electronically in digital form. This includes the internet, wireless networks, mobile phones, email, USB memory sticks, printers, scanner, cameras, digital television, streaming materials, robots.

Information Technology (IT): means anything relating to computing technology - computers, storage, networking and other physical or cloud devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data and includes software, hardware, electronics and the internet.

Malware: is an abbreviation of malicious software; is a type of software designed to gain unauthorized access or to cause damage to a computer system, e.g.: computer viruses, spyware, worms and trojans.

Network Services: refers to all software, hardware, computer networks and other technology provided by the School and made available for use by the School Community.

Phishing: is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like login information and credit card numbers. It is the most common type of cyber-attack.

Social Engineering: is a tactic that adversaries use to trick a user into revealing sensitive information.

URL: is the address of a World Wide Web page.

User: means any member of the School Community, Staff Member, student, Contractor, Consultant, Volunteer or visitor to the School that uses or accesses any form of the School's Network Services.

4. POLICY

ICT used constructively in the education and learning environment, plays an important role, particularly in the process of empowering the technology into educational activities. Effective and appropriate use of ICT encourages and allows students and Staff Members to create and communicate information, ideas, solve problems and work collaboratively in all learning and operational areas.

ICT can enhance the quality of education by increasing learning motivation and engagement; by facilitating the acquisition of technological skills and by complementing and enhancing teacher training. They are transformational tools which, when used appropriately, can promote the shift to a learner-centred environment.

Cybersecurity operates to protect the School's Network Services and data from unauthorized access, while supporting the business continuity management plan (see: Business Continuity Policy - 1.5.3). It also improves stakeholder confidence and the School's credentials in the management of information security.

A successful cyber security policy has multiple layers of protection spread across the computer, networks, programs and data that is required to be kept secure. To achieve this, the Users, processes and technology must all complement each other to provide an effective barrier from cyber-attacks. Effective ICT skills and leadership by the Board and senior Staff Members ensures the ICT requirements of the School are maintained. Suitability, usability and value-for-money all need to be considered.

New and current technologies need to be assessed in light of their ethics; how they impact Staff Members, students and others in the broader school community both practically and socially, including data privacy.

Any User who is unsure whether a proposed use is permitted or authorized should seek guidance from the supervising teacher or Head of Teaching and Learning in the case of students and the Digital Lead for Staff Members, before proceeding.

5. PROCEDURES

5.1 Cyber Security:

Security requirements reinforce the provision of a safe, fair and productive computing environment, while ensuring they do not adversely affect the operation, reputation or assets of the School.

The use of electronic communication carries with it responsibilities which include understanding the role they have in Cyber Security, awareness of privacy requirements and security principles.

Users must understand and comply with the data security guidelines which include, but are not limited to:

- Choosing strong passwords: a mix of characters, nothing obvious from a personal perspective, unique from previous passwords and not use the same password for multiple sites;
- Passwords are to be changed by each Staff Member every **6 months**, or more frequently as appropriate. A security mechanism to cover auto prompt for password renewal is in place.
- Do not share passwords with anyone or write them down, particularly near a computer monitor;
- Change password immediately if it or the computer have been compromised: advise the Digital Lead and/or IT Consultant immediately;
- Notify the Digital Lead or IT Consultant if a problem is encountered changing a password;
- Being wary of email attachments, if it appears suspicious do not click on it, check the URL of the website – be aware of "bad actors", who will take advantage of spelling mistakes to direct users to a harmful domain;
- Back-up data regularly;
- Ensure anti-virus software (Microsoft security updates and choice of internet browser) is always up-to-date;
- Never leave devices unattended, ensure there is short-lock mechanism to engage;
- Be conscientious of what is plugged into a computer, Malware can be spread through infected flash drives, external hard drives and smartphones;
- Be aware that criminals can easily be friends or similar users on social networks;
- Offline, be wary of Social Engineering, where emails or phone calls may try to solicit sensitive information – it is recommended to say 'No' and check the company directly to verify information/credentials;

- Monitor accounts for any suspicious activity, unfamiliar information could be a sign of the account being compromised/hacked. Advise the Digital Lead of any concerns as soon as possible.

To prevent password guessing, accounts will be locked after five unsuccessful attempts. To have an account unlocked, the Digital Lead will need to be contacted.

It is essential to provide all Users with the technology solutions to protect computer security tools. Three main entities must be protected:

- Endpoint devices - computers, smart devices (this includes mobile phones) and routers;
- Networks;
- Cloud.

Common technology used to protect these entities include next-generation firewalls, DNS filtering, Malware protection, antivirus software and email security solutions.

In the event a device is lost or stolen, the Digital Lead or Executive Director must be advised as soon as possible.

The cloud services, servers and computers of the School are maintained to best practices, with back-up, security monitoring, email security filtering and verification, antivirus and other security system items in place.

5.2 e-Safety and Working with Parents:

Web safety guidance and advocating a culture of e-safety is a priority for the School. The School actively encourages working with parents/carers to support this requirement, this includes the setting and communicating of appropriate and complementary standards for internet use at home. The School will contact parents/carers if there are concerns about a student's behaviour and encourages parents to share their concerns with the School.

5.3 Copyright Infringement:

The copyright material of third parties, for example, software, database files, sound recordings, musical or video files, text and downloaded information, must not be used without authorisation from the appropriate copyright owner or a licensee of the copyright owner to do so. The ability to share, forward and distribute electronic messages and attachments increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing, sharing or distributing material by electronic means may inadvertently place the School or an individual in a position of liability.

It is a breach of the School's Intellectual Property and Copyright Policy to misuse the School's Intellectual Property (IP), knowingly infringe third party IP or authorize anyone to do so, or to engage in an act of false Attribution.