SECTION 4.3: APPROPRIATE USE OF TECHNOLOGY
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 provide meaningful guidelines to the use and management of digital technologies at The Australian Ballet School (School). In accordance with legal and moral requirements and expectations, the School aims to provide both Staff Members and students with access to high quality, secure IT equipment and training, that will assist them to effectively use this communication tool for teaching, learning, data storage, research, archiving and performance/production enhancement.

Related Policies: This policy should be read in conjunction with Fraud Risk Management Policy (1.5.2), Business Continuity Policy (1.5.3), Intellectual Property and Copyright Policy (4.2), ICT and Cyber Security Policy (4.3.3), Workplace Behaviour (5.1), Bullying Policy (5.1.2), Sexual Harassment Policy (5.1.4), Social Media Policy (3.1.2) and the *Marilyn Rowe House Student and Parent Handbook*.

2. WHO DOES THIS POLICY APPLY TO

The policy applies to members of the Board, all Staff Members and students at the School and any Consultants, Contractors, Volunteers and service providers of the School while using or accessing any of the School's Network Services.

3. DEFINITIONS

Executive Team: means The Director of the School (Director), Executive Director and the Director of Development.

Information Technology (IT): is 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.

Metadata: means data that provides context or additional information about a file or record.

Network Services/Network: refers to all facilities and resources located on and delivered via a computer-based network, software and hardware including communications systems, internet services, mobile devices, electronic mail, webservices, printer services, database services, back-up services, file services and network management services made available for use by Board members, Staff Members, Volunteers and students and parents/carers.

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

4. POLICY

This policy covers the access and use of any of the School's Network Services (including computer devices provided by the School and/or any mobile device connected to the School's Network or used to access the internet via the School's Network, irrespective of whether that device is a personal device or provided by the School). The devices provided by the School to Staff Members and students to support their employment and/or learning activities is to be used in a lawful, ethical and responsible manner, solely for legitimate and authorised school purposes. All care must be taken by Staff Members and students to maintain the quality and condition of supplied devices. Damaged or missing devices must be reported to the Digital Lead as soon as practicable.

This policy and the related sub-sections are intended to raise User awareness of the risks of the online environment, including what constitutes acceptable and unacceptable use of the School's Network Services and to encourage a thoughtful and respectful approach to this and social media in the broader sense. Security and trustworthiness of online sources is critical.

Compliance with applicable laws and internal procedures when accessing the School's Network helps to maximise the efficient use of the School’s resources and ensures the School's Network is effective, reliable and secure, including free from viruses and other security risks.

All aspects of technology maintenance and innovation development, equipment and security are managed and the responsibility of the Digital Lead. Input and guidance in relation to all these aspects is sought from the School’s IT Consultant. Specific Incident Reports are provided by the IT Consultant. Overall responsibility for the equipment, security and use rest jointly with the Executive Director and Digital Lead.

The School takes all reasonable steps to protect the security of its Network Services, including Confidentiality, integrity and accessibility. A full-time security alert monitoring system is in place.

The School's Network Services are monitored and checked regularly. Logs on the School's server are checked weekly. There is a full-time content alert monitoring system in place. All these measures are overseen by the Digital Lead.

The School reserves the right to audit and remove any illegal or inflammatory material from the or of the School's Network Services without notice.

The School endeavours to provide up-to-date networked computers. Administration and curriculum networks are operated independently.

4.1 Use of the School’s Network for personal use:

The Network is provided by the School as a business, teaching, performance production, archiving and data storage tool. However, the School acknowledges that personal communication may need to be sent using the School internet or email facility from time to time. If the School’s Network is being used for personal use, Users must ensure that the amount of time and volume of electronic communication, attachments and files is kept to a minimum.

Using the School's Network Services for the printing of multiple copies of documents (particularly in colour) for personal use is unacceptable. Limitation's on a User's printing rights may be imposed if there is excessive use of printing for personal purposes not connected with the School or its courses.

4.2 Monitoring of traffic flow and content:

The School is committed to providing a safe learning, workplace and boarding environment. Accessing of material (including web browsing), that may pose a risk to Staff Members or students will be automatically flagged by the School's digital reporting system run by the IT Consultant. The Executive Director will be advised of this report and appropriate action taken.

Inappropriate use of the School's Network Services by Staff Members will be notified to the line manager of the Staff Member and will be discussed with that individual Staff Member. Depending on the nature of these discussions, support may be offered by the School to the individual through the **Employee Assistance Program** (EAP).

In keeping with the commitment of the School to provide a safe environment for children based on the Child Safety Standards, with particular recognition to Standard 9 – *Physical and online environments promote safety and well being while minimising the opportunity for children and young people to be harmed*, the School aims to provide a Network environment where the legitimate use and storage of data is secure against interference by other Users. Users, however, should not assume that their activities using the School's Network resources are completely private.

The School conducts annual information sessions for all students regarding online safety issues, including but not limited to inappropriate sites, stranger danger/tricky people, cyberbullying and scams.

Real-time monitoring of the School's Network Services is in place, with security logs checked a minimum of weekly by the IT Consultant. Full-time strong content filters are in place with anti-virus programs installed for the computer devices provided to the School's Staff Members. Student devices will have their usage and content monitored.

Emails and Metadata sent or received via the School's Network are logged using the School's internal email system. This includes any emails sent in a personal context using the School's email system.

The School may access an individual’s email account if they are not contactable, and in the case of Staff Members, when they are on leave and there is a business need or similar requirement.

4.3 Inappropriate use:

Inappropriate uses of the School's Network Services include (but are not limited to):

- any activities that breach any law or which are illegal, that violate the privacy or other rights of other individuals, or that may be harmful to others or the reputation of the School. Examples of these types of activities include including disseminating, promoting or facilitating child pornography or offering or disseminating fraudulent goods, services, schemes or promotions;

- use of the School’s Network Services for political lobbying or proliferation of unnecessary communications;

- storage or transmission of any software, videos, audio files, documents, pictures or other content that infringes the copyright, trademarks or other intellectual property rights of third parties;

- storage or transmission of any content is defamatory, obscene, harassing, abusive, invasive of privacy or otherwise objectionable;

- storage or transmission of any content or computer software that may damage, interfere with, intercept or otherwise affect any system, program, or data, including viruses, Trojan horses, worms or other malicious software;

- use of the School's Network Services to violate the security or integrity of any third party's Network Services or software;

- use of the School's Network Services to access the Network Services or software of a third party without permission, including probing, scanning or testing the vulnerability of any digital system or attempting to breach any security or authentication measures used by a third party's digital system;

- use of the School's Network Services to falsify or forge any communications data, including TCP/IP packet headers, e-mail headers or any other part of an electronic message describing its origin or route;

- unauthorised use of the School's Network Services to distribute, publish or send (or facilitate the sending of) unsolicited emails or other unsolicited commercial electronic messages (i.e., “spam”), including promotions or advertising the products and services of third parties;

- use of any manual or electronic means to avoid any access and storage restrictions placed on use of the School's Network Services;

- use of the School's Network Services to undertake or co-ordinate a Denial of Service (DoS) attack or to otherwise inundate a third party's network or computer device with communications requests so that the affected network or device either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective; or

- any other interference with the proper functioning or uses of the School's Network Services or the digital systems of a third party.

5. PROCEDURES

These procedures support this policy by clarifying the responsibilities of Users of the School’s Network Services; this includes how to manage data ethically, maintain trust, provide strategic direction as to the management of digital communications, information and documents and specifying how breaches of the policy will be handled.

5.1 Use of the Network:

When logging on to the Network, a User must only use their own user identification and password. Any attempt to impersonate another User will be treated by the School as a serious offence, as will any attempt to modify the School’s data which is not consistent with the individual’s designated role. Under no circumstances is another person’s account to be used to log on.

Users must not utilise proxy sites (anonymous surfing sites) to bypass the School’s filtering systems and access content that is blocked by the School.

The School's Network or other Networks connected to the internet must not be interfered with, which includes creating or distributing any computer virus or any other malicious attempt to harm, modify or destroy data of another User.

The addition of unauthorised devices to the School's Network and other equipment is forbidden. Users must not attempt to undertake their own repairs or try to troubleshoot any issues with the School's Network or its other equipment. Instead, any issues must be reported to the Digital Lead.

Users are not permitted to use the School's Network for advertising, sponsorship, profit making, commercial activities except where it is related to the business and development activities of the School and has been authorised by the Head of Marketing and Communications, Director of Development, Director, Executive Director or the Board.

Users are not permitted to use the Network for gambling or accessing inappropriate sites.

Inappropriate material or behaviour online (which includes sending unwanted email), which may be viewed as harassment is strictly forbidden and should be reported to the Department Manger or supervising teacher.

When a web-conferencing (video communications tool), is used for lessons, there must always be a meeting ID and associated password provided for access to the lesson to ensure strong security measures are in place for the students and for cyber security. Once the lesson has been completed, Staff Members and students must disable the microphone and camera access to their settings.

5.2 Network Security:

The security governance framework is part of Information Technology. If a security problem or fault on the School's system is suspected or identified, the Digital Lead or a member of the Executive Team must be advised immediately. The problem must not be demonstrated to other Users. In the event a Staff Member believes that data has been lost from the School Network they should notify the Digital Lead and/or IT Consultant as soon as possible. If it is believed that security has been compromised/an unauthorized person has obtained access, the Executive Director should be notified immediately. A cascading contact list is available to all Staff Members if the missing or lost data is business or time critical so recovery of the data from the back-up system can be promptly initiated.

5.3 Data Security:

Transmission of the School's data outside of the School's Network, including sending attachments by email to recipients that are not employed or engaged by the School, must be authorised first by the Digital Lead and then Executive Director. Any security procedures requested by the Executive Director or the Digital Lead (such as password-protecting attachments) must be adhered to.

Sensitive data (including personal information about the School's staff or students) is not to be transmitted by email or any other insecure means. This includes copies which are stored for official School business, often for short-term use (e.g., off-site performances and school tours). Such personal information must only be stored on a School-approved device. Notification of the device and nature of the information must be logged with the Digital Lead. Paper copies of such information should not be used.

Authorisation must be sought from the Executive Director and the Digital Lead. before any of the School's data is stored on or uploaded to a website or service hosted by an external party (for example, Dropbox, Google Drive or iCloud).

5.4 Storage:

All back-ups are stored off site in secure cloud storage and coordinated by the Digital Lead.

Long term retention of back-ups is stored in the cloud.

In the event there is a threat to the School's IT infrastructure or security, or the use of the School's IT presents a risk to the School, it may be necessary to for the School to take action to reduce the risks, with or without prior notice.

At the end of each day (or if a computer or other device is to be left unattended for a prolonged period), Users must always log off the Network and check that the logging out procedure is complete. If a computer is to be left temporarily, it should be locked or placed in sleep-mode in such a way as to require a password or PIN code to be enterer to re-gain access to the device to ensure it remains secure. A five-minute time-out lock is recommended.

Access to the local drive or the creation of local accounts on computer devices provided by the School is not permitted.

Only software provided on the Network may be run on the computers. The import of download applications, peer-to-peer file sharing programs, film and games is not permitted through the School system. Intentionally downloading or making available videos, music or pictures that breach the School's Intellectual Property and Copyright Policy (4.2) or any copyright legislation is forbidden. Copyright material of third parties must not be used without authorization or due credit and reference.

5.5 Access by Staff Members:

On commencement of employment with the School, each Staff Member will be issued with computer access, including a username, password and e-mail address. The Digital Lead advises the IT Consultant of any extra security level required by the new Staff Member above the baseline requirement for all staff. Secure storage of the server shared drives via an individual password is setup by the IT Consultant following authority given by the Digital Lead.

Any server access above the baseline level set by the School for all Staff Members must be conveyed in writing to the Digital Lead and Executive Director.

It is the responsibility of each Staff Member to ensure their password is secure. Staff Members are responsible for all actions which occur using their individual account. Staff Members should follow these guidelines:

- Passwords must be changed every **six months** or more frequently as appropriate. A security mechanism to cover auto prompt for password renewal and lock out if breached is in place;
- Set a password which is unique from previous passwords used for the School's Network and which is different from passwords for a User's other accounts (such as social media accounts);
- Do not use passwords based on known personal details, for example: names of pets, friends, children, birthdays, addresses, phone numbers;
- Do not send passwords by email or other forms of electronic communication; and
- Do not share your passwords with anyone or write down your password.

Any breach of these guidelines or this policy may result in the suspension or disconnection of any staff account or access to any of the School's Network Services (including if there is an immediate threat to the School). Disciplinary action may be taken against individuals if necessary, based on the recommendation of the Director or Executive Director.

Staff are to avoid leaving devices unattended or in unsecured locations.

5.6 Training of Staff Members:

A systematic approach to Staff Member training and professional development in all areas of technology use is encouraged and reinforced through the Performance Management process, this includes managing online personal safety issues which may arise with respect to students. (see Performance Review Policy (5.3.3) - *pending*. Staff will identify and include relevant digital management training and development in their plans as appropriate.

5.7 Student Access:

Access to the School's computer Network is a privilege and it is the student's responsibility to limit their usage of the School's Network Services to use that complies with this policy and which is legal, ethical and appropriate.

Students are required to check their School emails daily and use the technology available to support their studies.

Limited and appropriate personal use of the School's Network by students is also permitted. Students should be aware that the School's Wi-Fi network is only available between 8.00am and 6.00pm Monday to Friday. Students should not attempt to access the internet for personal use outside these times. Refer to *Marilyn Rowe House Student and Parent Boarding Handbook* for the policy governing *Responsible Use of Technology at MRH.*

As detailed above, the School automatically monitors all User accounts and the use of the internet via its Network. Access to websites which are regarded as providing material which may poses a risk to a student will be flagged by the system and brought to the attention of the Digital Lead, who then advises the Director and Executive Director. The School does not wish to intrude on a student's privacy but must balance this with keeping students safe.

Breach of any of these policies will result in access to the internet being removed for an appropriate period of time as determined by the School.

5.8 Working with Parents:

The School seeks to work together with parents/carers in promoting digital behaviours that develop cultural safety and cyber best practices at home and at school. Setting and communicating appropriate and complementary standards for digital management/internet use at home by parent/carers is encouraged. The School will contact parents or carers if there is a concern about a student's behaviour. Parents/carers are also encouraged to share their concerns with the School.

5.9 Breaches of this Policy:

Breaches of this policy will be considered to be misconduct by students and Staff Members. The School aims to impose discipline that fits the circumstances of the individual breach of this policy; this may include:

- for students, the issuing of a reprimand or suspension or expulsion of the student;
- for Staff Members, giving a written warning, reassignment of job duties or termination of employment; or
- termination of contract for a consultant or contractor to the School.

Some breaches may also have consequences under civil or criminal laws. These include:

- Child abuse material offences, relating to child pornography and child abuse material covered by the *Crimes Act 1958* (Vic);
- Objectionable material which has or may attract a classification of R18+ under the Guidelines for Classification of Films 2012, Guidelines for Classification of Computer Games 2012;
- Reckless or deliberate copyright infringement; or
- Accessing, use or distribution of any other material or activity that involves a breach of criminal law.