Rockingham Montessori School Incorporated
ABN: 68 115 270 695

POLICY TITLE: Information and Communication Technology Use

BOARD APPROVAL DATE: August 2020 **SIGNED BY CHAIR:**

BOARD REVIEW DATE: August 2023

This document sets out the security, administration and internal rules which you should observe when communicating electronically or using the Information Technology (IT) facilities provided by Rockingham Montessori School (the 'School'). This includes, but are not limited to, computers and the School network, Internet, mobile phones, wireless devices, personal music devices MP3 players, PDAs, recording devices or portable storage devices, including USB and flash memory devices. This also includes, but is not limited to, platforms such as email, social media, messaging apps and video conferencing tools. You should familiarise yourself with the terms of this Policy in order to minimise potential damage to you, your colleagues, students and the School, which may arise as a result of misuse of email or Internet facilities.

This Policy applies to all teachers, students, employees and contractors of the School.

1. School Property

1.1 The School is the owner of copyright in all email, social media and video conferencing messages created by its employees, students and contractors in performing their duties.

1.2 Record Keeping and Management: The school must maintain within a formal record keeping system a software licence register that includes the following minimum details (number of software licences purchased; number of licences currently installed/ being used; receipts, invoices and payment approvals as proof of purchase; a copy of the software licence terms and conditions; all software keys, serial numbers and activation codes; end date of the licence agreement (where applicable). Maintenance and stocktake should occur bi-yearly of the software licence register.

1.3 Staff personal computers must not be used for school purposes.

2. Monitoring

2.1 From time to time, the contents and usage of email, social media and video conferencing chat messages may be examined by the School or by a third party on the School's behalf. This will include electronic communications which are sent to you or by you, both internally and externally.

2.2 You should structure your email, social media and chat messages in recognition of the fact that the School may from time to time have the need to examine its contents.

2.3 The School's computer network is a business and educational tool to be used primarily for business or educational purposes. You therefore have a responsibility to use these resources in an appropriate, professional and lawful manner.

2.4 All messages on the School's system will be treated as education or business related messages, which may be monitored. Accordingly, you should not expect that any information or document transmitted or stored on the School's computer network will be private.

2.5 You should also be aware that the School is able to monitor your use of the Internet, both during school or working hours and outside of those hours. This includes the sites and content that you visit and the length of time you spend using the Internet.

2.6 Emails will be archived by the School as it considers appropriate.

3. Personal Use

3.1 You are permitted to use the Internet and email facilities to send and receive personal messages, provided that such use is kept to a minimum, does not interfere with the performance of your work duties, and does not use your school email address.

3.2 However, you should bear in mind that any use of the Internet or email for personal purposes is still subject to the same terms and conditions as otherwise described in this Policy.

3.3 In the case of shared IT facilities, you are expected to respect the needs of your colleagues and use the Internet, email and video conferencing tools in a timely and efficient manner.

3.4 Sharing of personal mobile numbers and social media accounts between staff and parents/students is strongly not recommended.

4. Content

4.1 Email correspondence should be treated in the same way as any other correspondence, such as a letter or a fax. That is, as a permanent written record which may be read by persons other than the addressee and which could result in personal or the School's liability.

4.2 You and/or the School may be liable for what you say in an email message. Email is neither private nor secret. It may be easily copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation. The audience of an inappropriate comment in an email may be unexpected and extremely widespread.

4.3 You should never use the Internet, email, social media or video conferencing tools for the following purposes:

(a) to abuse, vilify, defame, harass or discriminate (by virtue of sex, race, religion, national origin or other);

(b) to send or receive obscene or pornographic material;

(c) to injure the reputation of the School or in a manner that may cause embarrassment to your employer;

(d) to spam or mass mail or to send or receive chain mail;

(e) to infringe the copyright or other intellectual property rights of another person; or

(f) to perform any other unlawful or inappropriate act.

4.4 If you receive inappropriate material by email, social media or video conferencing chat, you should delete it immediately and not forward it to anyone else. It would be appropriate for you to discourage the sender from sending further materials of that nature.

4.5 Comments that are not appropriate in the workplace or school environment will also be inappropriate when sent by email, social media or video conferencing chat. Such messages can easily be misconstrued. Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner.

5. Privacy

5.1 In the course of carrying out your duties on behalf of the School, you may have access to, or handle personal information relating to others, including students, colleagues, contractors, parents and suppliers. Email, social media or video conferencing chat should not be used to disclose personal information of another except in accordance with the School's Privacy Policy or with proper authorisation.

5.2 The Privacy Act requires both you and the School to take reasonable steps to protect the personal information that is held from misuse and unauthorised access. We stress therefore, that you take responsibility for the security of your assigned school computer and not allow it to be used by an unauthorised party, which specifically includes anyone who is not an employee of the School.

5.3 You will be assigned a log-in code and you will also select a password to use the School's electronic communications facilities. You should ensure that these details are not disclosed to anyone else. We suggest that you take steps to keep these details secure. For example, you should change your password regularly and ensure that your log-in code and password are not kept in writing close to your working area.

5.4 You are encouraged to either lock your screen or log-out when you leave your desk. This will avoid others gaining unauthorised access to your personal information, the personal information of others and confidential information within the School.

5.5 In order to comply with the School's obligations under the Privacy Act, you are encouraged to use the blind copy option when sending emails to multiple recipients where disclosure of those persons' email addresses will impinge upon their privacy.

5.6 In addition to the above, you should familiarise yourself with the National Privacy Principles ('NPPs') and ensure that your use of email, social media or video conferencing does not breach the Privacy Act or the NPPs. If you require more information on the Privacy Act and how to comply, please contact the Principal.

6. Distribution and Copyright

6.1 When distributing information over the School's computer network or to third parties outside the School, you must ensure that you and the School have the right to do so, and that you are not violating the intellectual property rights of any third party.

6.2 If you are unsure of whether you have sufficient authorisation to distribute the information, we recommend that you contact the Principal.

6.3 In particular, copyright law may apply to the information you intend to distribute and must always be observed. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files and downloaded information) must not be distributed through email, social media and/or video conferencing tools without specific authorisation to do so.

6.4 All employees must abide by the legal use of software in line with the licensing terms and conditions. They need to ensure they add the relevant details to the software licence register.

7. Encryption and Confidentiality

7.1 When an email is sent from the School to the network server and then on to the Internet, the email message may become public information. Encryption will reduce the risk of third parties being able to read the emails and should be used in cases where you feel additional security is required. If you require more information in relation to encrypting messages, you should contact the Finance Manager, who will refer you to the relevant IT expert.

7.2 As mentioned above, the Internet and email are insecure means of transmitting information. Therefore, items of a highly confidential or sensitive nature should not be sent via email. You should note that there is always a trail and a copy saved somewhere, not necessarily only on the School's network server.

7.3 This confidentiality requirement applies even when encryption is used.

7.4 Email sent over the Internet may be truncated, scrambled, or sent to the wrong address. There is a possibility that outgoing email sent over the Internet may arrive scrambled or truncated, may be delayed, may not arrive at all, or may be sent to the wrong address. Where outgoing email is important or urgent, you should verify that the recipient has received the email in its entirety.

7.5 You must ensure that all emails that are sent from your email address contain the School's standard disclaimer message, which will read as follows:

> Important Notice: If you have received this email by mistake, please advise the sender and delete the message and attachments immediately. This email, including attachments, may contain confidential, sensitive, legally privileged and/or copyright information. Any review, retransmission, dissemination or other use of this information by persons or entities other than the intended recipient is prohibited.

7.6 Please delete old or unnecessary email messages and archive only those email messages you need to keep. Retention of messages fills up large amounts of storage space on the network server and can slow down performance. You should maintain as few messages as possible in your in-boxes and out-boxes. If there are items in your email which you require

at later date, please ensure that these are saved in your network directory so that appropriate backups are made School wide.

8. Viruses

8.1 All files downloaded from the internet (including email) and brought in externally (i.e. USB or CDROM) have the potential to be infected with viruses. Viruses can potentially harm the School's network and computer equipment. Any files brought in externally or downloaded from the internet must be scanned for viruses. RMS reserve the right to deny external devices being connected to the school's network or files being downloaded from the internet if there are any concerns regarding the safety or security of the data

8.2 RMS utilises enterprise grade antivirus protection which is installed on all computers and servers in the school network, all files are scanned automatically on access. If you have concerns about the safety of a file which you intend to download or send or believe a file may not have been automatically scanned by the antivirus software, please contact an administrative officer who can assist you further.

8.3 RMS has provided you with an email address to use for all work related matters. Please refrain from using this address for personal matters.

8.4 If you receive an email from an unknown sender, or if you think any email looks suspicious, you should delete it immediately.

8.5 Whilst antivirus is installed on all computers on the school network, this is not a guarantee that the computer can't become infected. Caution should always be exercised before opening files from any source. If you are unsure, do not open the file until you seek further advice from an administrative officer.

9. The use of Computers in the Classroom

9.1 Children should have appropriate supervision when accessing the Internet in the classroom. Children will be made aware of websites they are permitted to access.

9.2 In accordance with the principles of Montessori Education computer use should not become a significant part of a child's work in the classroom or be a substitute for traditional classroom activities.

10. Mobile Phone use

10.1 Teaching staff and students are requested to place mobile phones on silent when class is in session.

10.2 Personal calls/text messaging should be kept to a minimum.

11. General

11.1 The terms and recommended conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the School's email and Internet facilities. You are encouraged to act with caution and take into account the underlying principles intended by this Policy. If you feel unsure of the appropriate action relating to use of email or the Internet, you should contact the Principal.

12. Damage

12.1 IT items must be treated with care and respect at all items.

12.2 Repairing of wilful damage of IT items may be charged to the person responsible.