Electronic Messaging Policy

Electronic mail systems are provided to our employees as a business tool to facilitate communications between staff and individuals exclusively for the benefit of the Warroad Public School. When communicating via e-mail or other electronic media, all the existing Warroad Public School professional standards for written communications apply. Non-business related messaging wastes valuable work time and uses computer resources that are needed for business purposes. As such, employees should limit personal use of Warroad Public Schools electronic mail systems.

All electronic mail messages on the system are records of the school, and, except as described herein, are neither private nor confidential. In order to protect its business interests, Warroad Public School reserves the right to enter employees' electronic mail files, and monitor content, level of usage, and destination of e-mail, and any other aspect of the electronic messaging, in its sole discretion. Certain electronic messages, to which Warroad Public School In-house or outside counsel are a party, however, may be the subject of attorney-client privilege, and nothing in this policy shall serve as a waiver of such privilege.

Violations of the Electronic Messaging Policy may result in disciplinary action against the employee. Restrictions regarding an employee's use of the Internet or other public electronic communications also apply to the employee's use of e-mail. Please reference the entire Internet and e-mail Acceptable Use Policy for further details.

Internet Usage Policy

Warroad Public School provides Internet access to be used by employees for research and communications to enhance the performance of their jobs, and for other business purposes. Warroad Public School will limit Internet access to those employees who have a legitimate business need. Personal use of the Internet should be limited. Offensive or business inappropriate content is strictly forbidden.

Internet access an activity using Warroad Public School systems is controlled and may be monitored to insure compliance with corporate policies and applicable laws. Warroad Public School has the right, but not the obligation, to monitor any and all aspects of its computer system, including, but not limited to, monitoring sites employees visit on the Internet, reviewing material downloaded or uploaded by employees, and reviewing e-mail sent and received by employees. Employees waive any right to privacy in anything they create, store, send or receive on Warroad Public School's system or networks.

Use of Company Internet access to commit infractions such as misuse of Company assets or resources, prohibited harassment, misappropriation of theft of intellectual property, and unauthorized communications, is also prohibited. Please request the entire Internet and e-mail acceptable Use Policy for further details.

Blogging and Social Media Policy

Warroad Public School recognizes that employees may, on their own time, engage in "blogging", participate in social network sites or engage in other forms of social media activity. Participation in social media activity has become a part of everyday life, and we support *responsible* use by employees.

Guidelines for operating in an electronic world are the same as the values, ethics and confidentiality policies employees are expected to live every day, whether you're tweeting, talking with parents or socializing with friends or neighbors. You are an employee, and therefore your actions reflect on the School. For that reason, this policy applies to both School sponsored social media and personal use as it relates to the Warroad Public School.

If you discuss the Warroad Public School or talk about work related matters that are within your area of job responsibility, you should disclose your affiliation with Warroad Public School. Because your conduct on social media platforms may reflect on the Warroad Public School, your online postings must be ethical and responsible.

You must:

- Explicitly and conspicuously state that the views you are articulating are your own and not the views of Warroad Public School. Unless authorized by written permission to speak on behalf of Warroad Public School, you must not state or imply you are speaking for the School.
- When engaging online, represent yourself and your job status at Warroad Public School honestly.
- Obey all laws.

You must never:

- Disclose any trade secrets or other confidential or proprietary information about the School, its staff, students, parents or vendors. This includes any information that is not already in the public domain.
- Disclose any personal or confidential information about third parties, including other employees or others associated with the School, or post pictures of them, without their permission.
- Discriminate on the basis of race, gender, religion, age, disability or any other protected criteria under federal, state or local laws, regulations or ordinance.
- Disclose legal information involving a legal case, legal issue or attorneys without first gaining permission from the Warroad Public School Legal team.
- Use vulgar, sexually explicit, harassing, defamatory, or threatening language or images.

You are personally responsible for the information you put on the Internet. If you choose to engage in blogging, social networking or other public discourse on the Internet, you do so at your own risk. The School will not protect you from claims resulting from such activities.

Please keep in mind that any sarcastic, demeaning, flippant, unprofessional or ill-considered posting you make on the Internet may be forwarded or saved and may become impossible to retract. The internet caches almost everything so, even if you delete, it will probably continue to exist somewhere online. Anything that negatively affects your job performance, the performance of other employees, students, parents or Warroad Public School legitimate business interests may result in disciplinary action up to and including termination.

Any employee is free to report suspected violations of this Social Media Policy. Employees who report suspected violations will not be subjected to any form of retaliation.

Always remember that employees who violate the policy are subject to the Warroad Public School disciplinary process and could cost us the ability to retain students or become involved in unnecessary legal situations. Do the right thing, follow Warroad Public School's Media Policy and live in the Schools values and guiding principles.

Computer Software Policy

Warroad Public School licenses the use of copies of computer software from a variety of outside companies.

The School shall use the software only in accordance with the license agreement.

The School specifically forbids the unauthorized duplication of software. Employees are not permitted to install their own copies of any software onto School computers. Employees are not permitted to copy software from School owned computers and install it on home or any other computers. Employees learning of any misuse of software or related documentation within the school shall notify the Superintendent. According to U.S. Copyright law, unauthorized reproduction of software is a federal offense. Offenders can be subject to civil damages, penalties, fines and imprisonment.

Any employee who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to the School, or who places uses unauthorized software on the School's premises or equipment, may be subject to disciplinary action not excluding termination of employment.

Network Access Policy

To remain competitive, better serve our students and provide our employees with the best tools to do their jobs, Warroad Public School makes available to our workforce access to the School's internal computer network.

As required, users will be assigned an account and password to access network and computer resources. To maintain good security practices, never share your username and passwords with other employees or 3rd parties. Passwords need to be changed on a regular schedule. In the event that you believe your

username and password have been compromised you should change your password and immediately notify IS personnel.

Employees must never attempt to gain access to systems or resources they have not been authorized to use. All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner.

Personal electronics that have network and internet connectivity are common. Those devices that employees bring on to the School facilities should not be connected to the School internal networks without prior approval.

Some employees and contractors may be required to access School networks from outside locations. This is done by providing Virtual Private Network (VPN) access over the Internet. However, due to the high risk of computers being compromised by hackers and computer viruses, Warroad Public School has defined the following required guidelines for configurations of remote computers to access our network:

No policy can lay down rules to cover every possible situation. Instead, it is designed to express our philosophy and set forth general principles when accessing our network remotely. These policies are not only for Warroad Public School's benefit, but employees' computers and private information kept on them will also benefit from these policies.

All computers that have VPN access are required to have current antivirus software installed.

Employees must not connect to Warroad Public School's network if they suspect that their computer has a virus or has been compromised by a hacker until they are reasonably sure that the problem has been corrected.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

Cell Phone/Wireless Device Policy

Personal cell phone use is permitted only during non-working time, such as meal periods and authorized non-working breaks. Cell phones should not be used during work hours unless used for School purposes. This includes text messaging, e-mailing, or similar activity. Furthermore, the use of any Smart phone, mobile device or any other form of technology to take pictures, videos, or audio recording in the workplace is strictly prohibited, unless prior written authorization is obtained from you supervisor.