

ACCEPTABLE USE OF TECHNOLOGY

Background

The Division endorses the use of technology to support teaching and learning, and maintains a Division computer network that provides access to internal and external networks.

The use of the Division's network is solely for the purpose of enhancing and supporting teaching and learning by facilitating the exchange of information to further communication, education, administration and research that is consistent with the mission of the Division.

This administrative procedure applies to all persons using or accessing the Division network or who use Division-owned resources, including but not limited to employees, students, agents, appointees, consultants, contractors, student teachers and volunteers. This administrative procedure provides the boundaries that enable a safe environment in which to use technology resources and all users are responsible for individual compliance with this administrative procedure.

Procedures

NETWORK

1. The system's network, the messages transmitted, and any content or material created on it are the property of the Division. The Division reserves the right to restrict or terminate access to the network, or any divisional equipment or resources in any circumstances where there may have been violations or suspected violations of the administrative procedure or for any other reasons which are considered appropriate in the circumstances.
2. The network system and all electronic resources are subject to audit and access when required for operational needs and to ensure system integrity.
3. The Division has the right to supervise and monitor the use of such property. All users of such property should expect only limited privacy in the contents of any personal files, data, email or record of web activities. Individual searches or monitoring will be conducted if there is reasonable suspicion that this administrative procedure is being violated or that the activity of the user may be compromising the board's ability to ensure a safe and caring environment. This type of search and monitoring is considered reasonable.
4. The Division makes use of an internet filtering system in the interest of taking reasonable precautions to restrict access to controversial materials; however, it is understood that it is impossible to restrict or ensure denied access to all controversial materials.
5. Each person who is to access the Division network system must complete and sign a Responsible Use Agreement.

6. Staff will review and acknowledge the Responsible Use Agreement upon hire, annually, and at such times the Responsible Use Agreement is updated (using a communication process, such as, Public School Works).
7. Students will sign the Responsible Use Agreement as part of the registration process, and again in grades four, seven, ten, or when the agreement is updated. The signed agreement will be placed in the student file.
8. Teachers will annually review the Responsible Use Agreement with students.
9. Use of the Division network and electronic resources for extensive private or business venture, or political purposes is not permitted.
10. Any use of the Division network for illegal, immoral, unethical, offensive or objectionable activity is prohibited. This includes sending material deemed to be the same. Users must not harm or attempt to harm the physical or mental well-being of any person, or their assets or reputation.
11. Any use of the Division network or equipment to access or store obscene or pornographic material, on-line gambling services, tasteless humour, excessively graphic descriptions or depictions of violent acts, or any unlicensed media, software or any other copyrighted materials including materials that are bootlegged or illegally available for purchase or download are prohibited. Attempting to hack, exploit, or bypass security systems within the Division network is strictly prohibited.
12. Using programs that harass Division users or infiltrate a computing system and/or damage the software components is prohibited.
13. Users are to make the most efficient use of network resources to minimize interference with others
14. Any use of the Division network that accesses outside resources, must conform to the Acceptable Use of Technology administrative procedure.
15. Principals shall be responsible for authorizing and removing access for each staff member, which is facilitated through communication through the HR Department or the Director of Technology.
16. All users are expected to act in a responsible and polite manner consistent with practicing acceptable internet etiquette. Any statements of opinion that users make must be respectful, fair and not malicious.

SECURITY

17. Users will follow security procedures as outlined by the Division with respect to Two Factor Authentication/Multi-Factor Authentication as required.
18. Users will respect the rights and property of others and will not improperly access, misappropriate or misuse the files, data, or information of others.

19. Users may not share their account and/or passwords with anyone or leave the account open or unattended.
20. Accounts of staff members who leave the employ of the Division shall be immediately disabled. Student accounts are the responsibility of the enrolling school, and student access and/or account shall be disabled when no longer enrolled or registered in the school.

SOFTWARE

21. Users are responsible to take precautions to prevent viruses on their own equipment and the Division's equipment. Software piracy and the illegal use or possession of copyrighted software is strictly prohibited.
22. Evidence of all software licenses purchased by a school or the Division must be readily available for audit. It is the responsibility of the principal to request software purchases through the technology department (Director of Technology or designate). The technology department will maintain a register of all user/device licenses purchased by the Division and its school sites.
23. All software must be registered in the name of St. Thomas Aquinas RCSSD.
24. The illegal installation and/or storage of copyrighted software, videos, music, files and/or content for use on Division computers is prohibited. If illegally installed content is discovered it will be immediately deleted from division technology without notice to the user.
25. Users of software shall abide by the software licensing agreements between the Division and the vendors. Without notice, any equipment on the Division's property may be audited for compliance.

PERSONAL ELECTRONIC DEVICES (STAFF AND STUDENTS)

26. Personal electronic devices used to access Division network resources must adhere to the following conditions: there must be no violation of licensing agreements, access must be achieved through processes defined and supported by the Division, acknowledgement that liability for loss, damage or theft of the device resides solely with the user and support of the device resides solely with the user, and agreement with the terms and conditions set forth in this administrative procedure and the Responsible Use Form.
27. The Division is not obligated to supply electrical power access, or any other service, repair or support to personal electronic devices.
28. The Division does not guarantee the privacy or security of any item stored on or transmitted by any personal electronic device.
29. Personal electronic devices will not be connected to the Division's wired network.

30. Users of a personal electronic device will, to the best of their ability, ensure that their devices are virus-free and will maintain up to date with anti-virus and anti-spyware/malware software.
31. Employees using personal electronic devices are to be cognizant that paid time is to be spent providing employment-related services to the Division (e.g. routinely spending time texting friends while on recess supervision would not be appropriate). Individual circumstances and the professional judgement and discretion of the supervisor will determine what is deemed appropriate behaviour in this regard.
32. Administrative staff will contact the Superintendent or designate before searching student personal devices.
33. If administrative staff suspect a cell phone is being used for illegal or sexually explicit activities, the cell phone should be turned over to the police immediately, and the Superintendent or designate will be notified of such actions.
34. The principal may remove student user access to the network and suspend, ban, or limit the right to use personal electronic devices.
35. School authority is not limited to the geographical boundaries of the school grounds and the principal may discipline students who misuse personal electronic devices, or any other technology-enabled medium, away from school or on their own time if both of the following conditions are met: the student's use of the technology causes significant disruption at school or is injurious to the physical or mental well-being of others in the school and the student knew, or should have known, that the harm would happen.

OFF-DUTY ONLINE CONDUCT

36. Employees are reminded that they have a legal duty of fidelity to the Division as their employer. Employees are further reminded that many online communications are considered public spaces including, but not limited to, personal blogs and social networking sites. Consequently, employees are prohibited from making any negative or disparaging online comments about the Division that may threaten to affect its reputation or legitimate business interests. Employees are further prohibited from publishing any negative comments about other employees, posting material that may violate the privacy rights of others, or disclosing any confidential information.
37. For certificated staff their code of professional conduct for teachers and teacher leaders infers appropriate off-duty online conduct at all times and the code stipulates that at all times teachers are to act in a manner which maintains the honour and dignity of the profession.

E-MAIL

38. Division email is provided for the purpose of exchanging information consistent with the mission of the Division. Internet email use within the Division is subject to these procedures.
39. Division email cannot be used for private or commercial offerings of products or services for sale or to solicit products or services, or for political purposes. Nor is it to be used to

disperse information regarding personal or organizational fund-raising initiatives on a division-wide scale.

40. Division email use is subject to Division review at any time.

NO WARRANTIES

41. The Division makes no warranties of any kind, whether express or implied, for the service it is providing. The division will not be responsible for any damages. This includes loss of data resulting for delays, non-deliveries, misdirected deliveries, or service interruptions caused by the division's actions or inactions or by the user's own errors or omissions.
42. Use of any information obtained via the Internet is at the user's own risk. The division specifically denies any responsibility for the accuracy or quality of information obtained. All users need to consider the source of any information they obtain and consider how valid that information might be.

PROPERTY RIGHTS

43. The Division has the right to specify who uses its equipment and the information contained therein, under what circumstances, and to what purpose. Equipment purchased by the Division belongs only to the Division and neither employees, volunteers, nor students in the Division have ownership rights to any equipment loaned to them by the Division. Extensive use of Division equipment and software for private or personal business is strictly prohibited and may subject the violator to disciplinary action.

DATA SECURITY

44. The Division assumes no responsibility or liability if documents stored on Division equipment are lost or damaged, nor will the Division be responsible for security violations beyond the proper consequence for those persons involved in such violations. Persons identified in violations are subject to the discipline procedures of the Division.

INTELLECTUAL PROPERTY

45. Works covered by copyright that are developed by employees in the course of their employment shall be the intellectual property of the Division. Works covered by copyright that are developed by employees outside of school facilities, beyond the instructional day, not in the course of their employment, and intended for commercial distribution are not the intellectual property of the Division.

FALSE ENTRY/ALTERATION

46. No student, volunteer, or Division employee shall make any false entry or alteration of any document, either paper or electronic, used or intended to be used in connection with the operation of any school within the Division nor shall any student open or alter official school documents or private documents, either paper or electronic.

ENFORCEMENT

47. The Division shall rigorously uphold this administrative procedure and any laws pertaining to the use of technological equipment and the information contained in them and/or generated by its use. Anyone found to be violating this administrative procedure or any such laws may be subject to revocation of access privileges, disciplinary action up to and including termination, and/or appropriate legal, civil or criminal, proceedings in relation to any such violations.
48. All student users of Division networks shall read and sign an “Acceptable Use of Technology Agreement – Student” (Form 140-1). Parents/Guardians of students under the age of 18 shall read and sign the Division agreement along with their child. Any violations of the agreement will be subject to corrective or disciplinary action, such disciplinary action may range from minor interventions to the loss of access privileges, suspension or expulsion from schools, dependent upon the severity of the violation. If deemed appropriate by Division personnel, violations may be reported to the appropriate police authority.
49. All employee users shall read and digitally accept the “Acceptable Use of Technology Agreement – Staff” (Form 140-2). The acknowledgement of the agreement will be recorded in our division communication process, such as, Public School Works. Any violations of the agreement will be subject to corrective or disciplinary action up to and including termination.
50. The principal is responsible for ensuring compliance with this procedure at their school site and for informing themselves and all persons reporting to them about this administrative procedure.
51. School personnel are responsible for informing themselves and all students under their direction about this administrative procedure.
52. No liability will be assumed by the Division or any division employee for any user’s wilful and cognizant misuse of the network or Division equipment.

Reference: Section 31,32,33,52,53,196,197,222 Education Act

Freedom of Information and Protection of Privacy Act Canadian
Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
Code of Professional Conduct for Teachers and Teacher Leaders