RICHMOND CHRISTIAN SCHOOL
EST.1957

NAME: 04.02 TECHNOLOGY USE POLICY	**VERSION:** 2
ADOPTED: MARCH 10, 2014	**REVIEW:** 2017-2018

REVIEW EVERY 3 YEARS

PREAMBLE

4.2 Technology Use policy for Richmond Christian School is not an independent policy nor is it a static document. Consideration must be given with its relationship to other policies and procedures at Richmond Christian School, including but not limited to those for behaviour, anti-bullying, and the 'Code of Conduct' signed by employees, students and parents/guardians. Although this policy is primarily written to set out guidelines and expectations for employees and students, it does apply to all persons granted access to the network through their affiliation with the school. This includes volunteers who may be given limited access to the network and school resources.

4.2 Technology Use policy covers computer Internet use and access through mobile phone and other wireless devices. This policy applies to multi-media, social networking websites, blogs and wikis for both professional and personal use. To use these technologies effectively, one requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom. Information and communication technology has the potential for:

a. enhancing learning processes;

b. information management;

c. developing and encouraging decision making skills; and

d. improving communication.

Richmond Christian School has a responsibility to provide students with Internet access as part of our mission to provide a quality Christ centered education. However, Internet access is a privilege and the scope of access to information and learning expectations will vary from campus to campus and grade to grade.

Richmond Christian School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to inappropriate material will never occur via a school computer. Neither the school nor its Board of Trustees can accept liability for the material accessed or any consequences resulting from Internet use.

INTELLECTUAL PROPERTY AND COPYRIGHT

1. All users of network resources are required to respect copyright and licensing laws and regulations. The school will not accept responsibility for a user who willfully and knowingly contravenes copyright or licensing laws and or regulations.

CRIMINAL AND CIVIL LAW IMPLICATIONS

2. Maintaining professional boundaries in all forms of communication, electronic or otherwise, is vital to maintaining the public trust and safeguarding appropriate relationships with students.

3. Inappropriate use of electronic communication can result in criminal charges and possible civil action. Users are reminded that third party repercussions may result from:

    a. making inappropriate defamatory comments or disclosing confidential information about the school, its students or employees in breach of the workplace privacy policies and provisions of the *Education Act*;

    b. copyright infringement - posting the work of others without proper attribution;

    c. breaching a court-ordered publication ban;

    d. inciting hatred;

    e. disclosing information about a minor, contrary to the *Youth Criminal Justice Act*;

    f. using technology to harass a student, colleague or others, contrary to the *Criminal Code*;

    g. using a computer to lure a child or for juvenile prostitution under the *Criminal Code*; and/or

    h. exchanging or forwarding compromising photos, videos or audio recordings.

NETWORK STANDARDS

4. All network resources are the property of Richmond Christian School and are subject to the general policies and practices of the school.

    a. "Network resources" includes, but is not limited to, Internet access, e-mail accounts, installed software, personal file storage and all hardware attached to the network.

    b. The Network Administrator will make regular assessments to ensure that the content filtering methods selected for any particular user or groups of like users are appropriate, effective and reasonable.

5. Software installation must be done in consultation with the Network Administrator, subject to the following conditions:

    a. Appropriate licensing must be obtained prior to activating any installation, unless prior permission has been granted or licensing is not required.

b. Evidence of all software licenses purchased by the school or a department must be readily available for audit. It is the responsibility of the Network Administrator to maintain such evidence.

c. Where and when possible, all software must be registered in the name of Richmond Christian School.

d. Software licences purchased by Richmond Christian School are not permitted to be installed on personal computers.

i. Exceptions to this must be approved by the Directory of Information Communication Technology in Education (Director of ICT).

6. Network storage areas are the property of Richmond Christian School. The Network Administrator will review file storage and communications to ensure system integrity and responsible use of resources.

USER ACCOUNTS

7. User accounts may be created for employees, students and Board members.

a. Additional volunteers may be given user accounts where permission is granted by the Board of Trustees or the Superintendent.

b. Permission levels are set for different levels of access and responsibility.

8. All employees and adult volunteers given access to the school's network will sign a copy of the *Technology Use Policy – Employee Code of Conduct* before using any Internet resource at any campus.

9. The Network Administrator will maintain a current record of all volunteers, employees and students who are granted access to the school's network resources.

a. All users granted access must sign a copy of the appropriate *Code of Conduct* form which must be kept on file in the campus office.

i. Students and parents are expected to sign the form annually.

ii. Employees will sign the form at the time of employment and each time the document is revised.

iii. Volunteers given access over and above guest internet login access will sign the form annually.

10. User accounts must be reviewed every September to ensure that any outdated accounts are inactivated.

NETWORK ACCESS PROTOCOLS

11. The school will allocate an appropriate level of Internet access for employees and students on the basis of educational need.

    a. At the Elementary campus, student usage should be fully supervised, group logins may be appropriate for lower primary grades and upper grades may have individual accounts.

    b. At the Middle and Secondary campuses all students have individual accounts.

    c. Parental permission will be required for Internet access in all cases at all campuses.

    d. Parents will be informed of the level of supervision and access which may or may not be supervised at the Middle and Secondary campuses.

12. Access to network resources with devices which are not school property may be authorized subject to the following conditions:

    a. There must be no violation of licensing agreements;

    b. Access is achieved through processes supported by current network resources;

    c. Use is respectful of the expectations set out in the Code of Conduct for Technology Use forms; and

    d. Liability for damage to either the device or the network resources resides solely with the user.

PROFESSIONAL EXPECTATIONS OF EMPLOYEES

13. Employees are responsible for ensuring that any school property including a computer or laptop loaned to them by the school, is used to support their professional responsibilities.

    a. Computers or lap tops that are part of the Bring your Own Device loan program are not considered school property.

14. A professional breach in conduct, whether on a personal computer or one that is school property, may result in termination of employment.

15. Inappropriate use of network resources or inappropriate electronic communication may result in disciplinary action. Employees are reminded:

    a. To use school technology, or any components thereof, for permitted purposes only;

        i. Richmond Christian School owns the computer network and all associated parts, components, programs and licensing.

        ii. Richmond Christian School has established the rules for its use and these rules may change from time to time.

        iii. That all network and Internet use must be appropriate for educational purposes and relate to curriculum objectives.

b. To only access the network with the user's authorized account and password.

   i. Login and password information must remain confidential.

   ii. Use of someone else's login information will have serious consequences for all parties involved.

c. That the use for personal financial gain, gambling, political activity, advertising or illegal purposes is strictly prohibited.

16. Employees will be provided with specific programs and tools for posting information and communicating with the school community.

    a. When posting information for the benefit of the RCS community, only these communication tools may be used.

    b. Teachers must notify parents in September of their intention to use which communication tool and the up to date login information.

    c. Information and visual media posted must comply with all school parameters and must be professional, accurate and relevant to the audience it is addressing.

17. An overview of the Technology Use policy should be completed by the Superintendent or the Director of ICT during the prep week prior to the commencement of each school year. Staff are to be reminded on:

    a. Safe use of e-mail;

    b. Safe use of Internet including use of Internet-based communication services, such as instant messaging and social networks;

    c. Safe use of school network, equipment and data;

    d. Safe use of digital images and digital technologies, such as mobile phones and digital cameras;

    e. Publication of student information or photographs or student work(s); and

    f. E-bullying / Cyber bullying procedures.

VIOLATION OF TECHNOLOGY USE PROTOCOLS

18. Should an employee come across an unacceptable use situation, either directly or indirectly, they are to notify the Principal or Superintendent immediately.

    a. In the interests of fairness and transparency, all complaints and incidents will be recorded in writing, including any actions taken.

19. In the event of a questionable or serious offence by an employee, the following steps should be taken:

a. Ensure that any equipment involved in a serious allegation is secured for future audit if necessary.

b. Complete the *Alleged Misuse of RCS Technology Guidelines by an Employee* to identify the precise details and facts surrounding the alleged infraction.

c. Sanctions for inappropriate use by an employee may include a formal letter on their employment file, investigation by a third party, suspension or termination.

20. In the event of a questionable or serious offence by a student, the following steps should be taken:

a. Ensure that any equipment involved in a serious allegation is secured for future audit if necessary;

b. Complete the *Alleged Misuse of Richmond Christian School Technology Guidelines by a Student* to identify the precise details and facts surrounding the alleged infraction.

c. Consequences for inappropriate use by a student are set out in Category A through Category D and their application is dependent upon the circumstances of each individual situation.

i. Consequences are attached for reference only and do not form part of this policy.

E-SAFETY FOR STUDENTS WITH ADDITIONAL NEEDS

21. Students need to learn how to apply strategies that will help them to avoid certain "risks".

a. There are certain aspects of Internet use that are particularly challenging for students with additional needs or children who may be vulnerable in this learning context.

b. Internet use by special needs students requires direct supervision at all times.

JOB DESCRIPTION

22. Job descriptions for the Director of Communication and Technology in Education (Director of ICT) and the Network Administrator shall be reviewed in conjunction with this policy.

APPENDIX A - CURRENT TECHNOLOGIES

1. Bring Your Own Device (BYOD) will be implemented on a progression basis at all three campuses. Procedures and staff expectations will be determined and modified as the BYOD program develops.

2. E-mail

    a. E-mail should not be considered private and Richmond Christian School reserves the right to monitor all e-mail sent to or from an RCS account or through RCS network resources.

    b. Employees should only use their official school e-mail address as a way to communicate regarding school related business.

        i. Employees should refrain from providing their personal e-mail address to students currently enrolled at Richmond Christian School.

3. Phone

    a. The personal use of cell phones while class is in session is prohibited unless express permission is given by the instructor.

    b. Phones must be considered as a component of the Technology Use Policy because of the scope of features they now have. Mobile phones can be used to record student or employee behaviour, can transmit text messages without limit and can effectively interrupt classroom activities.

4. Social Networking

    a. Richmond Christian School employees who use social networking sites in their professional capacity as an employee of Richmond Christian School must always conduct themselves in a professional manner. Professional postings:

        i. must identify the user as an employee of RCS and their position at RCS

            (1) employees should neither claim nor imply that they are speaking on the School's behalf.

        ii. the user must ensure that posted information is well thought out, accurate and respectful of the community the information is being provided to,

        iii. must not disclose confidential or proprietary information about the school, its students, alumni or employees; sharing confidential information may be grounds for disciplinary action .

    b. The Internet is a public medium and employees are reminded that postings can impact their personal and professional reputation.

        i. The RCS Code of Conduct, school rules, policies and procedures always apply as do federation, college and Ministry of Education or relevant government regulations.

c. Richmond Christian School reserves the right to request that certain subjects are avoided, to require employees to withdraw certain posts and remove comments deemed inappropriate.

d. RCS employees are discouraged from connecting personally through social media with current students. All student communication through social media should be set up on a separate non-personal account.