SUBJECT: Technology Acceptable Use Policy 02/2020 **P450**

Background

We are blessed to have a computer room and Internet access at Lacombe Christian School. These tools are useful to students and teachers in a variety of ways and enhance the process of education. The following rules are necessary to protect the students and the school community as a whole. Please read them carefully. If you have any questions please contact the school (office@lacs.ca or 403-782-6531)

Technology can support, enhance, and transform learning and the way we work and learn. The school expects that technology will be used in an ethical, legal, moral, relevant, and responsible manner consistent with the beliefs and values of Lacombe Christian School.
Computers and other mobile devices are tools used at school to support learning and enhance instruction. Computer networks allow people to interact with these devices within the school, and with other computers around the world. With the popularity of the internet growing each day, it is imperative that students, parents, and staff understand an Acceptable Use Agreement is necessary to ensure that computers or other mobile devices and the network be used in a responsible, relevant, ethical, and legal manner.

Definition

Vandalism is defined as any malicious attempt to harm or destroy data, equipment, the network, or agencies or other networks that are connected to the internet. This includes deliberately or recklessly exposing school technology to virus infection.

1. Students are not to damage or disassemble computers, printers, keyboards, mouse, etc. Students will have to pay for any damage done to computer lab equipment. Any malfunctioning equipment should be reported to the supervising teacher as soon as possible.

NOTE: Banging the mouse on the desk will result in the student's immediate removal from computer lab.

Procedures

1. The Technology Acceptable Use Administrative Procedure shall be reviewed with all students at the beginning of the school year, prior to being given access to the library and the school network.
2. The Technology Acceptable Use Administrative Procedure shall be reviewed with all school staff, by the Principal, at the beginning of each school year.
3. A Technology Acceptable Use Form (Student) will be included in the Annual Online Student Enrolment Verification, and will be acknowledged annually by parents. Additionally, the terms will be reviewed at the beginning of each year with students.
4. It is expected that each employee at the school shall review this Administrative Procedure and comply when using school technology, including wired and wireless networks.
5. Each employee shall sign a Technology Acceptable Use Form (Staff), at the time of employment, and then periodically, as deemed necessary by the Principal.
6. The school's technology resources (devices, networks, etc.) may not be used to:
   - 6.1. Transmit information/material that violates Canadian/Alberta legislation.
   - 6.2. Duplicate, store, or transmit pornographic material (including social media).
   - 6.3. Duplicate, store, or transmit threatening, abusive, or obscene material.
   - 6.4. Duplicate, store, or transmit copyrighted material in violation of copyright law.
   - 6.5. Threaten, intimidate, bully, or spread rumours (gossip) about another individual or group.
   - 6.6. Use anonymous proxies to get around content filters.
   - 6.7. Harass other users with unwanted email (spam).
   - 6.8. Students may not use the camera on the laptops for any purpose including taking pictures or video at any time except when approved by a teacher for a specific class.
7. All users of the school's owned technology, including networks, shall avoid plagiarism and other violations of copyright/licensing infringement.
8. Expected behaviour for users of social media include, but is not limited to the following:

8.1. All users must conduct themselves appropriately, using proper social decorum and adhering to all applicable "codes of conduct" as may apply to them (ie. provincial legislation, School Board rules and policies).

8.2. Staff will not issue 'friend' or 'follow' requests to students and will decline similar requests from students on all social media platforms.

8.3. The school technology is intended primarily for "educational purposes" and as such, during the school day, it is expected that use will be limited to activities related to teaching and/or learning and work-related tasks. A history of Internet sites visited by students is maintained on each computer. Random checks of students' internet use will be made from time to time.

9. Acceptable Use

The following sections are to assist users to more fully understand the intent and scope of this Administrative Procedure. Failure to adhere to the school's Acceptable Use Agreement may result in the user's access being revoked by the local school administrator and/or the school's Network Administrator.

9.1. Acceptable use includes:

9.1.1. Using the computer, network equipment, or other electronic communication devices for classroom activities or projects; this may include connecting to other systems and computers through the internet.

9.1.2. Sending and receiving email related to school activities.

9.1.3. Personally accepting responsibility for all websites and other materials accessed, downloaded, uploaded, viewed, and/or produced and knowing that the content is to be appropriate for school use at all times.

9.1.4. Knowing that the use of technology resources is a privilege - not a right.

9.1.5. Understanding that system administration personnel have access to all files at all times including email.

9.1.5.1. These files are monitored and may be viewed by teachers, school administration, and/or the police.

9.1.5.2. The school will cooperate fully with local, provincial, or federal officials in any investigation related to any illegal activities conducted through the school network or with school-owned technology.

9.2. Unacceptable use includes (but is not limited to):

9.2.1. Using profanity, obscenity, or language, which may be considered offensive or abusive to another person including but not limited to the use of vulgar, obscene, rude, lewd, inflammatory, threatening, disrespectful, or derogatory language.

9.2.2. Using the internet or other communication devices to intimidate, bully, harass, or embarrass anyone; including personal attacks, prejudicial or discriminatory attacks, or posting information or pictures that could cause damage, danger, or disruption of school operations.

9.2.3. Violating copyright laws, which include copying sharing, downloading, or installing copyrighted or unlicensed material as well as copying/printing material that is considered restricted or proprietary.

9.2.4. Giving out individual passwords or using another individual's password.

9.2.5. Reading, copying, or modifying another user's email, social networking, chat programs, or restricted files without prior consent.

9.2.6. For students: loading or modifying software without the consent of a staff member or school administrator.

9.2.7. Knowingly sabotaging computer or network equipment; this includes bypassing or disabling certain operating system functions or network configurations, ie such as clearing the internet or chat history or cache.

9.2.8. Using the computers or network for any type of illegal activity or personal gain including but not limited to online gaming activities, objectionable offensive or pornographic material, etc. Students will not be normally permitted to use instant messaging or “chat”, that is, to directly interact with unknown (or known) people.

9.2.9. For students: using computers or the network without permission from a teacher or staff member.

9.2.10. Using the printer excessively, and wasting paper. Students and staff are expected to use the printer only when they are sure they wish to print.

9.2.11. **Bringing food and drink in the computer lab.**

10. Internet Privacy Protections and Considerations for Students

10.1. All school employees have an obligation to ensure student safety and to balance this with the need for open communications when using the internet. There are documented instances of students being inappropriately identified via the internet and thereby becoming subjected to unhealthy situations or unwelcome communications.

10.2. School employees are expected to assist students in regard to their use of the internet, including personal electronic devices that access the internet. The purposes of these procedures are:

10.2.1. To inform school staff of the possible dangers of allowing students to post or publish identifying information on the internet;

10.2.2. To recognize that there are potential advantages of allowing students to post or publish information on the internet; and

10.2.3. To provide a recommended set of procedures governing how Student-identifying information is to be allowed in posting or Publishing on the internet.

10.2.3.1. There can be risks, as well as advantages, involved with allowing students to be identified on the internet. Students are not to be easily identifiable from materials they might post or publish on the internet.

10.2.3.2. No directory information is to be posted on the web for students whose parents have returned the form asking that such information is not to be released.

11. Personal Safety Guidelines

11.1. Students will not disclose their full name or any other personal contact information for any purpose. Personal contact information includes address, telephone, or school address.

11.2. Students will not share or post personal contact information about other people. Personal contact information includes address, telephone, school address, or work address.

11.3. Students will not share or post privacy-revealing personal information about themselves or other people.

11.4. Students are not permitted, nor should they ever agree to meet someone they have only ever met online.

11.5. Students are to tell/show their teacher or another trusted school employee (an adult) about any message they receive that is inappropriate or makes them feel uncomfortable.

11.6. Students are not to delete the message until instructed to do so by a staff member.

11.7. Pictures that are a part of student publishing are not to include identifying information.

11.8. In special circumstances, with parent-signed release, identifying information can be added.

11.9. If a teacher replies to electronically submitted student work, it must always be “appropriate” and the teacher’s email address (identity) is always to be displayed.

11.10. If a student becomes aware of a security problem (including compromise of passwords), the student will report the problem to the supervising teacher as soon as possible.

11.11. Each student will be assigned one computer to use. Students will not be permitted to use other computers without permission from a teacher.

11.12. Students must report any damage or problems to the Technology Department immediately for

documentation and/or repair. Failure to do so may result in the assessment of abuse/neglect
fees.

11.13. Students in junior high will be assigned their own email address. It is to be used primarily for communications between students and teachers, but may also be used for student communication on school related work.

11.14. Use of email at school will only be done under direct supervision of a teacher.

11.15. Students may access their school email address at home; however, use is restricted to school use only. It is not to be used for personal email.

11.16. The school's network administrator has access to and will monitor student email use.

11.17. Students will choose a password to access their email. This password is not to be shared with anyone else.

11.18. Students are not to send inappropriate, obscene or threatening emails. Students will report any abuse of email to their teacher as soon as possible.

11.19. Students who fail to abide by these email policies will have their email and/or computer privileges suspended or cancelled.

12. Portable Electronic Devices

12.1. Students assigned school's portable technology devices must follow the rules of the Acceptable Use Agreement.

12.2. It is the student's responsibility to immediately alert school personnel if the school-assigned device is lost, damaged or stolen.

12.3. Students using personal or school-assigned devices are subject to all school policies and procedures, plus any local, provincial, or federal laws, when using the device.

12.4. Students take full responsibility for electronic personal property brought to school and are to take all reasonable measures to protect against theft or damage.

12.5. Technology staff will not support or configure any personal electronic device.

12.6. Students are responsible for the safety and security of the laptop issued to them. The laptops must be under the students' control or stored in the locked laptop cart.

12.7. The laptops may only be carried in a proper and safe manner. Laptops must not be placed in positions (such as on the floor in hallways or classrooms) where other students may accidentally step on them, drop book bags on them or in any other way cause damage to the laptops. Laptops must be carried with both hands. For use, the laptops must be placed on a desktop or table top only, never on the floor. Tables and desktops should be free of unnecessary books and other equipment. Laptops may never be placed in book bags.

12.8. Students must treat the laptop with the care and respect required for an expensive electronic device. Failure to do so may result in the student's family being assessed an abuse/neglect fee for the diagnosis and repair of the laptop. If the laptop is broken beyond reasonable repair, the student will be assessed the fair market value of the laptop as a fee.

12.9. Students must keep all food and drink away from the laptop at all times. Care must be taken when using USB devices – the USB ports may break off if devices aren't plugged in and pulled out with care.

12.10. Students must physically handle the laptop in the manner directed during laptop orientation.

12.11. The laptops may not be picked up by the screen or carried by the corner of the case as there is too much danger of damage to the unit.

13. Portable Lab Procedures

13.1. All laptops will be stored in the laptop cart. The laptop cart will be kept locked at all times, except when it is being used in the classroom.

13.2. When not in use, the laptop cart will be stored in the computer room along the north wall.

13.3. Teachers are responsible to ensure that all (30) of the laptops are in the cart prior to locking it up.

13.4. Teachers are responsible to ensure that all (30) of the laptops are in the cart immediately after unlocking it in the classroom.

13.5. A group of 3 – 5 students from each class will be trained in assisting with the laptops. These will be known as the S.W.O.T. (Students Working on Technology) Team. Two of the S.W.O.T. team, as directed by the teacher, will be responsible for:

13.5.1. handing out and collecting the laptops at the beginning and end of each use

13.5.2. bringing the cart to the classroom and returning it to the computer lab

13.5.3. connection and disconnection of the wireless router in the classroom

13.5.4. ensuring that the laptops are correctly shut down upon return to the cart

13.5.5. ensuring that the laptops are plugged into the battery chargers

13.6. Students are to make sure that the laptop is fully shut down before returning it to the cart.

13.7. Elementary teachers are to ensure that students and parents have signed the LCS Computer Use Policy. This will be handled by the computer teacher for junior high students.

13.8. Laptops will be numbered and students will use the same laptop each time. Sheets to record this will be kept with the laptop cart. In the event that their regular laptop is out of service, students will need to sign out an alternate laptop for that period.

13.9. All laptops are to stay with the portable cart. Laptops are not to be individually used by the staff, either during the school day or on evenings and weekends. Laptops are not to leave the school building.

13.10. Teachers and students are responsible for reporting any malfunctions or other problems to the System Administrator as soon as possible.

13.11.

14. Terms and Conditions of Use Successful operation of technology resources in the school requires that all users regard it as a shared resource. It is important that users conduct themselves in a responsible, legal, professional, ethical, and courteous manner while using the school's technology (devices and/or networks) and when communicating online using social media tools or other technologies. All other policies, including those on harassment, equity, and proper conduct apply to the use of technology. Following is a list of guidelines, the violation of which could lead to suspension or termination of access privileges and may lead to further disciplinary and/or criminal proceedings.

14.1. System Security and integrity

14.1.1. Hacking into a network is a criminal act. You may not violate, or attempt to violate, the security or integrity of computers, data, or network in the school.

14.1.2. Users are prohibited from sharing their passwords or permitting others to use their account and must log off immediately after use to ensure that others may not access their account. Users are responsible for all activity within their account and will be held accountable for any inappropriate activity. Each student will choose a password to access their computer. Do not reveal your password to anyone. If you suspect that someone knows your password, see your teacher to obtain a new password as soon as possible.

14.1.3. Users are not to disclose anyone else's user ID, password, network, or internet credentials.

14.1.4. Vandalism may result in the termination of a student's technology privileges.

14.1.5. In order to enable fair use of technology, system administrator(s) may set quotas for disk/computer/network usage and usage time limits on some technologies.

14.1.6. In order to protect the integrity of the networks and maintain efficiency, the connection of personal technology equipment such as home computers, routers, servers, wireless devices, etc to the school networks, is not allowed without the permission and guidance of the school's Information Technology staff. Admittance as a guest on the school's networks require all users to agree to abide by this Administrative Procedure.

14.2. Privacy and Confidentiality

14.2.1. Use of the school's technology including internet access and email is neither private nor confidential and may be tracked.

14.2.1.1. Use of such technology by any individual may be monitored or reviewed by the school without prior notice.

14.2.1.2. In the case of misuse or suspicion of misuse of the network or services, the school reserves the right to access any files/data on the system.

14.2.2. The school may block or remove files that are unacceptable or in violation of this Administrative Procedure.

14.2.3. Parents have the right, where legally applicable, to request to see the contents of their child's data.

14.2.4. Due to the nature of some of the school's approved online technologies being hosted worldwide (ie Google Apps), it is possible that an individual's full name, student id, school name, email, and classwork may be stored on premises outside of Canada. In such cases, privacy laws of the country hosting the data may apply. Such technologies may only be used in the manner prescribed by the school.

14.2.5. The school will not disclose or post a student's personal contact information without the consent of the student's parent or of the student, if legal age. This includes the student's address, telephone number, school address, work address, or any information that clearly identifies an individual student.

14.2.6. The school will not disclose an employee's personal information without the consent of the employee.

14.2.7. Staff and students shall not post or discuss online, personal information or work-related issues including student work, without the permission of all parties involved.

14.2.8. When using social media or other websites to enhance classroom education or conduct school business, personal information including full names may not be posted unless authorised, and appropriate measures are to be taken to protect the privacy of individuals and content where applicable.

15. Notice of Fair Warning

15.1. All users of technology owned by the school and/or those who access school/system networks (including staff, students, and parents) are to understand that steps are routinely taken within the school to mitigate the connection to or the downloading of offensive material. However, due to the dynamic nature of the internet, there is no fail-safe way to ensure that students or staff are completely isolated from controversial, offensive, or questionable content.

15.2. The school and it's individual schools are not responsible for the information on remote systems.

15.3. Furthermore, it is understood that users will change passwords periodically and are responsible for logging off local and remote systems when they are not present.

15.4. Users are to be aware that any discovered illegal activity carried out over the internet may be reported to law enforcement officials for possible prosecution. Financial and legal consequences of such actions are the responsibility of the user (staff, volunteer, student, and student's parent).

15.5. Lacombe Christian School administration will deem what is inappropriate use of the Internet and or computer lab facilities and the decision of administration, in consultation with the teachers and school board if required, will be final.

FORMS:

Technology Acceptable Use Policy Form - Student and Parent

Technology Acceptable Use Policy Form - Staff

References	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	I.T.I.L. Standards, Alberta Education

Technology Acceptable Use Policy (Student and Parent) P450

I have read the LCS Student Computer Use Policy and I agree to follow it. I understand that failing to follow the policy may have serious consequences such as removal of Internet privileges, removal of computer privileges, in-school suspension or home suspension.

Computer Use:

Name of Student: ______________________ Signature of Student: ____________________

Date: ______________________

Internet Use and Email Use:

Name of Student: ______________________ Signature of Student: ____________________

Date: ______________________

Portable Use:

Name of Student: ______________________ Signature of Student: ____________________

Date: ______________________

As a parent **I have read the attached LCS Student Computer Use Policy** and agree to its terms.

Name of Parent: ______________________ Signature of Parent: ____________________

Date: ______________________

After signing, detach and return this page to your teacher. ***Students will not be allowed computer access until this sheet has been returned.***
Students must treat the laptop with care and respect due to an expensive electronic device. ***Failure to do so may result in the student's family being assessed an abuse/neglect fee for the diagnosis and repair of the laptop. If the laptop is broken beyond reasonable repair, the student will be assessed the fair market value of the laptop as a fee.***