Lambton Kent District School Board

ADMINISTRATIVE PROCEDURE NO: A-PR-200-18

ADMINISTRATIVE PROCEDURES

SUBJECT: Responsible Use of Technology

The Lambton Kent District School Board (LKDSB) provides access to technology for staff and students to support their educational, learning and business needs. Everyone that uses technology has a role to play in maintaining a secure and respectful environment. The purpose of these Administrative Procedures is to set out the expectations with respect to the use of technology and the responsibilities of each individual.

The LKDSB strives to model and teach safe, legal, ethical and responsible use of information technology and resources, and expects all users to embrace the following characteristics of use:

- Respect and protect yourself and others,
- Respect and protect intellectual and technical property.

These Procedures apply to all employees and students of the LKDSB as well as other users that have been granted permission to use the LKDSB computer system or access LKDSB-owned data (e.g., trustees, school council representatives, parents, volunteers, contracted workers).

Managers and principals are to ensure that all staff and students are aware of the requirements contained in these Procedures.

<u>System Integrity</u>

1. The computer system, including any data and information that is created, transmitted or stored on the LKDSB system is the property of the LKDSB.
2. There is no expectation of privacy in using LKDSB technology. The LKDSB may monitor and may access any files, documents, electronic communications and use of Internet at any time to ensure integrity of the system and compliance with these Procedures.
3. Users must not try to gain unauthorized access to the computer network or databases.
4. Users must not access or delete computer files or directories of others unless authorized by IT to do so.
5. Users must respect the integrity of the computer system by not altering hardware, software or wiring configurations.
6. Users must not cause damage to LKDSB technology (computers and/or equipment including, but not limited to, computer hardware, keyboard, monitor, mouse, cables).
7. Computer viruses and related problems can cause extensive damage to computer systems. Viruses can be spread in a variety of ways including downloading files from the Internet, email attachments, infected USB keys etc. Users should use caution when opening email attachments from unknown senders.
8. All USB keys and any other storage media brought from an outside source (e.g., home, provided by a vendor) must be scanned for viruses before use.
9. All supported workstations within the LKDSB are automatically scanned for viruses.

10. The LKDSB accepts no responsibility for the physical or software security of any device brought onto its property from any outside source (e.g., personally owned from home, provided by an external vendor).
11. Users must not download or install onto Board desktop and laptop computers any unauthorized materials such as programs, games or files from any source.
    a. Users may download mobile applications onto smartphones and tablet devices where they have been given permission to do so.
12. During the evaluation to adopt new system applications, the investigation must include security issues related to the software and network. All current system applications must be reviewed to ensure that they meet the minimum security standards established.
13. Users must not take any action to attempt to bypass the security measures put in place by the Lambton Kent District School Board. This includes, but is not limited to, accessing blocked sites or applications by using proxy sites, or VPN applications.

Password Management and System Access

14. Users will only use the network account and password assigned to them.
15. Users must not share passwords, nor use the passwords of others.
16. The initial passwords for Board network and email access will be assigned by the IT Help Desk and be consistent for all new users and consist of a minimum of 8 characters, including upper and lower case letters as well as numbers. Users will be required to change the initial password to a minimum of 8 characters, including upper and lower case letters as well as numbers. Users will avoid using any published information within a password that could potentially identify the user.
17. Passwords must be changed:
    a. At least twice a year for staff.
    b. At least yearly for students.
18. The user will be responsible for any activity using their account, including any time that the computer is left unattended.
19. If a User loses his/her password or feels that an unauthorized person has accessed their account, they must report it to a teacher, manager, or school administrator immediately.
20. Screen savers must be enabled on all devices, and must automatically activate for staff within 30 minutes of inactivity and must require a password to reactivate.
21. The Human Resources Department will notify the IT Help Desk as soon as possible when an employee leaves the system permanently and the accounts, on all systems, will be disabled or deleted.

Connection to The LKDSB Network (Wired and Wifi)

22. Users must not connect any electronic devices to the LKDSB wired network without the written permission of the Information Technology Department of the LKDSB.
23. Users may connect personally-owned devices to the guest wifi network.

Personal Safety

24. When using the Board supported networks, users must take care not to provide any personally identifying information about themselves or others unless it is to a trusted source.

25. Students must report to a teacher or school administrator any messages they receive that requests personal information, requests a personal meeting with a stranger, are inappropriate in any way, or make them feel uncomfortable.

Appropriate Personal Use

26. Board supported network accounts are granted to users to assist in fulfilling their learning and employment duties and responsibilities.
27. Users may use the LKDSB's network and Internet resources for incidental and occasional personal use, provided that such use is reasonable in duration, does not interfere with the user's learning and employment duties and responsibilities, does not result in increased cost to the LKDSB, and complies with these Procedures.
28. The LKDSB expects staff personal use to occur outside assigned work time, and student personal use to occur only during break time.

Use of Resources

29. Users must avoid the waste of limited resources such as paper, print supplies, hard drive space, and bandwidth.

User Behaviour

30. Users must act professionally and use language appropriate to the school setting at all times.
31. Users must not access any site that is transmitting inappropriate or offensive material.
    a. Users must immediately report accidental access to such sites to a school administrator or manager.
32. Users must not encourage the use of controlled substances, such as illegal drugs, alcohol or tobacco. Accessing sites promoting such products is considered an unacceptable use.
33. Users must not access or distribute material that advocates prejudice or hatred towards any identifiable group (for example, gender, ethnic, religious, minority, etc.).
34. Users must not create, access, download, transmit, store, distribute or print any files, messages or graphics that are profane, harassing, discriminatory, offensive or degrading.
35. Users must not access, download, transmit, store, distribute or print any files, messages or graphics that are illegal or advocate illegal acts, facilitate unlawful activity, or are not consistent with the philosophy of the Lambton Kent District School Board.
36. Users must not propagate chain letters or other junk mail.
37. Users must not attempt to hide, disguise or misrepresent their identity as the sender.
38. Users must not use inappropriate language in files/filenames, on websites or in email communication.
39. Users must not use LKDSB technology for personal financial gain, for commercial activity, or for any illegal purpose.
40. Users must not send any form of commercial electronic messages (CEMs) unless required to as part of their job duties with the LKDSB, and must first ensure consent has been obtained as per Canadian Anti-Spam Legislation (CASL).

Equipment Repairs

41. All employees, contracted staff and identified volunteers of the Lambton Kent District School Board must exclusively use the services of the Board's Information Technology (IT) Department to perform repairs, upgrades and maintenance including virus protection and malware removal on all Board supported technology.
42. Taking a piece of technology (computer, netbook or laptop, etc.) to a third party vendor or website for such services without the written permission of the Manager of Information Technology or delegate is strictly forbidden.

Copyright

43. All software licence agreements must be honoured. It is against the law to copy commercial software that has not been placed in the public domain or distributed as "freeware". This includes the downloading, copying, distribution, playing and publication of digital music and video files. Refer to LKDSB Fair dealing/ Copyright Regulations and information on the LKDSB Portal.
44. Under copyright laws all material remains the property of the author/creator and therefore permission is required for its use.
45. Do not take and present the work of others (e.g., writings, images) and present them as yours. If using the work of others proper credit must be given and permission obtained if copyright materials are used.

Mobile Devices

46. All mobile devices owned by the Board and used to conduct Board/school business must be used appropriately, responsibly, and ethically. The following must be observed:
    a. Mobile devices are to be protected by a 4-digit password. This password does not need to be highly complex, but simple combinations are not allowed (e.g. 1111, 1234, qwer etc.).
        i. The requirement for passwords and/or complexity may be waived for general use classroom devices.
    b. Mobile devices will be set by the default security policy to lock after 15 minutes of inactivity.
    c. Mobile devices will be set by the default security policy to automatically reset and wipe all data after 10 failed password attempts.
    d. Board-owned mobile devices must be treated, used, and safeguarded. If a user damages or loses a Board-issued mobile device, the user must notify the IT Help Desk immediately and the IT Help Desk will notify the Freedom of Information (FOI) Coordinator.
    e. No user is to use a Board-owned mobile device for the purpose of illegal transactions, harassment, or obscene behavior, in accordance with other existing user policies.
    f. Users are to reimburse the Board for personal use (e.g. calls, text messages, and data) not related to Board business.
    g. Airtime minutes and data plans that are included in the monthly rate are property of the Board.
    h. Where possible, lost or stolen mobile devices will be remotely wiped of all data including any applications that the user may have installed onto the device. The Board is not responsible for replacing or restoring of any data other than to the default configuration.

Non-Disclosure

47. Employees of the Board are provided privileged access to some information systems and to the confidential data and records contained in those systems. Privileged access imposes upon the employee the responsibility and obligation to use that access in an ethical, professional, and legal manner that is strictly within his or her authorized job functions. Employees must not disclose such information to unauthorized parties, or make public such information without appropriate approval.

Safeguard of Private and Confidential Information

48. Employees and other users may require access to Board confidential information or private information relating to staff or students.
    a. All recipients of such information must ensure that they provide appropriate safeguards in the handling of that information; for example, using encrypted laptops or encrypted USB drives, or using board-provided server storage.
49. It is the responsibility of the holder or recipient of confidential or private information to ensure that it is stored securely, and to notify the IT Department/ FOI Coordinator if they believe that the security of the information has been compromised.
50. Users should seek advice from the IT Department before handling confidential or private data if they are in any doubts in regards to how to store and use it.
51. At no time is confidential or private data to be stored on personally owned computer or mobile devices, including mobile media such as USB drives.
52. Users must notify the IT Help Desk immediately of a lost or stolen Board-owned device, or lost or stolen data storage media (Board owned or personally owned) such as USB drives that may contain confidential or personal information. The IT Help Desk will immediately notify the FOI Coordinator.
53. Any third party that is not an LKDSB staff member who requires access to any private or confidential information must agree in writing to be bound by these procedures and must comply with appropriate legislation such as the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Personal Health Information Protection Act (PHIPA). Such persons or organizations must ensure that: the information is appropriately safeguarded, that only essential information is obtained and stored for the purposes of use, that appropriate authorization has been provided to transfer the information, that they retain the information only for the time needed, and that the information is securely destroyed as soon as no longer needed.

Use of Cloud-Based Data Storage and Applications

54. Any web-based application that may be used to store private, confidential or personally identifiable information must be used with caution.
55. Users are expected to read the full terms and conditions and privacy statements of the service provider and make a judgment regarding whether it is safe to store information, or use the service.
56. If in doubt, users should contact the IT Department or FOI Coordinator before using such services.

Use of Social Media

57. While social media is a powerful tool, any use (both for work purposes and for personal reasons) must be considered public and permanent at all times.
58. It is expected that staff use social media responsibly at all times.
59. Inappropriate references to the Board or Board staff, schools or school staff, students, and parents in media such as social networking sites, blogs, web pages, or e-mail, whether Board-provided or personal, may represent a contravention of expected professional standards, or student behavior, and may be subject to further investigation and discipline.
60. Inappropriate use of personal technology, or services such as social media, while on or off school property, either during the school day or outside it, that has a negative impact on school climate, may result in investigation and action where appropriate. Such examples may include (but are not limited to) harassment and bullying occurring outside school hours.

61. Students are prohibited from using Board devices, networks and accounts to register or use online accounts such as social media where they are not of appropriate age. E.g. Students under the age specified in the software license agreement of online tools, social media accounts, etc are prohibited from using them.

Consequences

62. Any violation of these Procedures may result in sanctions, including the loss of computer privileges, suspension or expulsion for students, disciplinary action up to and including termination of employment for staff, and legal action or police involvement for all users.

Review

63. These procedures must be reviewed annually by the Privacy and Information Management Committee (PIMC).

Implementation Date: October 2016
Revised date: June 11, 2018

Reference: LKDSB Policy
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
Personal Health Information Protection Act (PHIPA)
Canadian Anti-Spam Legislation (CASL)