

ADMINISTRATIVE PROCEDURE 141

Computers: Network, Internet and Electronic Devices

1. Purpose

- 1.1 The director of education has developed this administrative procedure to address the implications of the use of technology in terms of safety, privacy and intrusion into district schools. This procedure is intended to state clear expectations for staff members and students to practice responsible and ethical behaviour in their use of computers and electronic devices.
- 1.2 Staff members and students are required to promote responsible use of shared resources and to refrain from unauthorized access or abuse. Staff members and students are expected to make every attempt to avoid inappropriate materials. They are required to use computers and electronic devices as educational and communications tools and to avoid any use which has a negative impact on safe, caring and orderly schools.

2. Background

- 2.1 Staff members and students in the Renfrew County District School Board have access to computer networks for educational purposes. These networks include:
 - 2.1.1 the Internet, an unregulated world-wide network of computers;
 - 2.1.2 the Board's network for electronic mail within and among the schools in the district; and
 - 2.1.3 in-school networks.
- 2.2 The district supports access to information that furthers its mission and key outcomes. While the district does restrict access to internet sites known to be inappropriate for educational use, it is not possible to control all information available. Because of this, from time to time, users may be able to obtain access to materials that are or might be considered to be inappropriate, obscene, abusive, offensive, harassing, illegal, or to counsel illegal activities. Staff members and students are expected to refrain from accessing and using such materials.
- 2.3 This procedure is intended to restrict the use of computers and electronic devices in ways that violate the privacy and dignity of others, that bully and harass others, and that put district resources and the security of district information at risk. These uses are not permitted.
- 2.4 The Renfrew County DSB network is maintained by network systems administrators who may from time to time intercept electronic communication. Although email and other electronic communications are not regularly monitored, there can be no assumption of privacy when using the network.

- 2.5 The security of the Renfrew County DSB Network is critical and all users are expected to safeguard and respect security precautions that are in place.

3. Guidelines for Use

All staff members and students must adhere to the following guidelines in return for the privilege of using the district and school networks and access to the Internet.

- 3.1 Use the access to the Internet and to Board and school networks only for educational or administrative purposes.
- 3.2 Use only the passwords and accounts assigned and refrain from sharing accounts and passwords and from using another person's account.
- 3.3 Report immediately any security problem to a person in authority (who shall notify a network system administrator) and refrain from sharing the problem with others.
- 3.4 Refrain from use of the networks for any of the following specifically prohibited purposes:
- 3.4.1 to access resources or data of others for any purpose without authorization, including passwords, files or tapes, whether at school or elsewhere;
 - 3.4.2 to send messages or files containing digital information likely to result in loss or disruption of the recipient's work or system ("viruses"), or to load such messages or files onto the networks;
 - 3.4.3 to transfer commercial software, materials protected by trade secret or other copyright protected material;
 - 3.4.4 to commit any illegal act;
 - 3.4.5 to intentionally obtain or send any materials which are or might be considered inappropriate, obscene, abusive, offensive, harassing, illegal, or counsel to illegal activities;
 - 3.4.6 to obtain or attempt to obtain any material or item prohibited by the district; and
 - 3.4.7 to use the networks for commercial purposes, or for games.
- 3.5 The principal will be the initial arbiter of what constitutes materials which are or might be considered inappropriate, obscene, abusive, offensive, harassing, illegal, or counsel to illegal activities, or what constitutes any other violation of these regulations. Any appeal of the decision will be to the appropriate superintendent.
- 3.6 All network accessible computer locations will have a copy of this administrative procedure posted in them, as well as a copy of Form 141-1 Networked Computer Contract with RPS and Netiquette, which includes "Rules for Personal Safety" and "Netiquette" guidelines.
- 3.7 Penalties for violation of these procedures may include temporary or permanent withdrawal of network computer privileges, suspension from school or employee duties, and/or prosecution under the law.

- 3.8 All users, and in the cases of users under the age of eighteen (18), a parent or guardian, will sign an agreement acknowledging an understanding of this procedure, as well as the form noted above. All users will follow “Netiquette” guidelines regarding appropriate use of networks, especially for the purposes of e-mail and chat activities. The signature will also demonstrate a commitment to abide by this procedure, as well as knowledge of the range of consequences for failing to do so.

4. Computer Security: Staff

- 4.1 This section sets out some specific procedures for staff members related to maintaining a secure computing environment.
- 4.2 District information is a corporate resource with substantial value that must be protected from unauthorized modification, destruction or disclosure, whether intentional or inadvertent.
- 4.3 Access to confidential information is restricted to those with a demonstrated “need to know” to the extent required to perform job functions.
- 4.4 The district recognizes and respects its disclosure and privacy protection obligations as identified in the *Municipal Freedom of Information and Protection of Privacy Act*.
- 4.5 Critical data are securely managed throughout their life cycle and backed up as appropriate. Information and equipment disposal practices ensure the continued protection of privacy.
- 4.6 All software on the Board’s computers must be installed in compliance with licensing requirements of the software’s owners. Use of “pirated” software or software secured through unauthorized reproduction is strictly prohibited.
- 4.7 Pass words and related security codes must be kept secure at all times and disclosed only as provided for by the disclosure procedures and practices of the owners.
- 4.8 Personal computers or terminals must not be left unattended when the power is on and confidential or critical information is being accessed.
- 4.9 Failure to comply with the computer security procedures will result in disciplinary action up to and including dismissal.

5. Use of the Internet and Electronic Devices

- 5.1 Cyber bullying is using electronic means to intimidate, harm, shun, attack or ruin a reputation. Cyber bullying includes the use of e-mails and instant messaging, text or digital imaging sent on cell phones, web pages and web logs (blogs), chat rooms and discussion groups. Cyber bullying may include but is not limited to:

- 5.1.1 using a chat group or gaming site to attack the person's character;
 - 5.1.2 impersonating someone by breaking into his or her e-mail account, posing as that person and sending damaging messages;
 - 5.1.3 denigrating someone by sending or posting cruel rumours to damage his or her reputation;
 - 5.1.4 misusing a cell phone to take embarrassing photos and e-mailing them to others;
 - 5.1.5 outing or trickery, which involves revealing someone's secrets or embarrassing information online or tricking someone into revealing secrets while online;
 - 5.1.6 setting up polling sites by developing web pages so that peers can vote on who is the "dumbest" or "ugliest" student or staff member in the school; and
 - 5.1.7 creating hate sites, such as pages on Facebook.com, designed to insult others.
- 5.2 These activities, when taking place off the school site or outside school hours normally are not school matters, but rather community or police issues. However, these activities can have an impact on the school and negatively affect the safety, climate and the learning environment at the school. In such cases, the use of the Internet and text messaging for bullying or harassment may be dealt with by the principal.
- 5.2.1 References to the Renfrew County District School Board and/or its schools (name, logo, or other identifiers) on personal social networking websites must in no way bring discredit to the Board.
- 5.3 The principal, in consultation with the superintendent responsible, will determine whether conduct outside the school constitutes a school matter. Key factors in determining whether the behaviour concerns the school will be:
- 5.3.1 whether there is evidence that the person or persons who have been threatened or intimidated are consequently impaired in their ability to progress in their studies or duties at school;
 - 5.3.2 whether criminal charges have been laid and whether the perpetrator has conditions of the court placed upon him or her in regard to attending school; and
 - 5.3.3 whether the conduct is injurious to the moral tone of the school and/or affects school safety and security.
- 5.4 If the principal determines that off-site conduct has had or is having a negative impact on the school, the principal may impose discipline in accordance with administrative procedures and Board policy and/or, in consultation with the superintendent responsible, may involve police services.
- 5.5 Cellular phones and other electronic signalling devices are disruptive if they are activated in class. Even if used for silent messaging, incoming signals distract the student's attention away from the instruction and can interfere with both learning and teaching. Cellular telephones, pagers, and similar types of communications devices carried by students are to be turned off and not used within the school.

- 5.6 Communications devices also have the potential to be used for academic dishonesty. Cellular telephones, pagers, personal digital assistants (PDAs) and similar types of electronic devices may not be carried or be in the possession of students during examinations and/or other major assessments.
- 5.7 Integrated digital cameras, cell phones and personal digital assistants (PDAs) can be used in a manner that violates the privacy and dignity of others. Use of cellular telephones with camera capabilities and similar devices is restricted in the school setting, in general, and is absolutely prohibited in areas where there is an increased expectation of privacy, such as washrooms or change rooms.
- 5.8 Unless it is a school-sanctioned activity, the taking of photographic images of a person or persons on school property, at school events, and during school activities and/or school hours is prohibited without the permission of the person or persons being photographed.
- 5.9 The electronic transmission or posting of photographic images of a person or persons taken on school property, at school events, and during school activities and/or hours, is prohibited without the permission of the person or persons being photographed, and where the student is below the age of eighteen (18), the consent of the parent or guardian.
- 5.10 Violations under section 5 will be dealt with according to administrative procedures, Board policy and/or the police protocol.

6. **Loss, Theft or Confiscation of Devices**

- 6.1 The school is not responsible for students' personal electronic devices in the event of loss, damage or theft.
- 6.2 If a student violates this administrative procedure, the electronic device may be confiscated and returned to the parent or guardian, or to an adult student after the instructional day, or as appropriate to the circumstances.

Legal References:

Education Act

Ontario Regulation 298 Operation of Schools

Municipal Freedom of Information and Protection of Privacy Act

PPM No. 128 - The Provincial Code of Conduct and School Board Codes of Conduct

PPM No. 144 - Bullying Prevention and Intervention

PPM No. 145 - Progressive Discipline and Promoting Positive Student Behaviour

Renfrew County District School Board References:

AP 140 - Code of Conduct

AP 180 - Records Management

AP 340 - Bullying Prevention and Intervention

AP 350 - Student Conduct and Progressive Discipline

AP 358 - Student Discipline: Suspension

AP 359 - Student Discipline: Expulsion

AP 450 - Human Rights

AP 451 - Workplace Conflict and Workplace Harassment

Form F141-1 Networked Computer Contract with RPS and Netiquette