ADMINISTRATIVE PROCEDURE 141

Computers: Network, Internet and Electronic Devices

DEFINITIONS

A "**User"** means all staff, students, volunteers, parents, school councils, school volunteers, service providers and community members i.e. any person using RCDSB technology equipment or networks.

B **"RCDSB"** means Renfrew County District School Board.

C "**Technological Devices"** may include computers, cell phones, mp3 players, cameras, game consoles or any electronic device that can access information over the Internet or on a network.

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 all users who access the Board network or who use Board or personal-owned devices while on Board property.

1.2 Users are required to promote responsible use of Board resources and to refrain from unauthorized access or abuse. Users are expected to make every attempt to avoid inappropriate materials. They are required to use computers and electronic devices as educational, business and communications tools and to avoid any use which has a negative impact on safe, caring and orderly schools/administrative buildings.

1.3 School/Site staff will develop their own procedures for ensuring that all students, staff and appropriate members of the community are aware of the AP. This procedure must be published in at least two of the following:

1.3.1 parent handbook;
1.3.2 student handbook;
1.3.3 staff handbook;
1.3.4 behaviour guideline;
1.3.5 school code of conduct;
1.3.6 school newsletter;
1.3.7 September information package;
1.3.8 posting in prominent locations
1.3.9 staff entry plan

2. Background

2.1 Users in the RCDSB may have access to the following:
2.1.1 the Internet, an unregulated world-wide network of computers;
2.1.2 the RCDSB's network; and
2.1.3 in-school wired and wireless networks.

2.2 The RCDSB supports access to information that furthers its mission and key outcomes. While the RCDSB attempts to 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. Users are expected to refrain from accessing and using such materials. Network users are responsible for appropriate behaviour on RCDSB networks and while using RCDSB or personal electronic devices.

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 RCDSB resources and the security of RCDSB information at risk. These uses are not permitted.

2.4 The RCDSB 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 RCDSB networks is critical and all users are expected to safeguard and respect security precautions that are in place.

2.6 The RCDSB makes no warranties of any kind, whether expressed or implied, for the network service it is providing. The RCDSB assumes no responsibility or liability for any phone charges, line costs or usage fees, nor for any damages that a user may suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. Use of any information obtained via the Internet is at the user's own risk.

3. Guidelines for Use

3.1 The RCDSB encourages the responsible use of technology. Such use must be consistent with the RCDSB's Code of Conduct (AP140).

3.2 Generic or shared accounts are not permitted. All accounts are assigned to a named user, with the activity of the account their responsibility.

All Users Will:

3.3 Use only the passwords and accounts assigned and refrain from sharing accounts and passwords and from using another person's account.

3.4 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.

3.5 Refrain from the use of the networks for any of the following specifically prohibited purposes:

3.5.1 to access resources or data of others for any purpose without authorization, including passwords, files or tapes, whether at school or elsewhere;

3.5.2 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;

3.5.3 to transfer commercial software, materials protected by trade secret or other copyright protected material;

3.5.4 to commit any illegal act;

3.5.5 to intentionally obtain or send any materials which are or might be considered inappropriate, obscene, abusive, offensive, harassing, illegal, or counsel to illegal activities;

3.5.6 to obtain or attempt to obtain any material or item prohibited by the RCDSB;

3.5.7 to use the networks for commercial purposes, or for non-sanctioned gaming; and

3.5.8 to download and/or use software designed to circumvent the user agreement and/or other security measures implemented by the RCDSB.

3.6 The principal or manager 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.

3.7 Penalties for violation of these procedures may include temporary or permanent withdrawal of access to technological devices and network privileges, suspension from school or employee duties, and/or prosecution under the law.

3.8 All Student users (Grades 4-12) will have a parent or guardian sign an agreement acknowledging an understanding of this procedure, Form 141-1 Appropriate Use Contract for Students. Adult student users (18) or users who are 16 or 17 and have withdrawn from parental control shall also sign Form 141-1 Appropriate Use Contract for Students. All users will follow the guidelines regarding appropriate use of networks, especially for the purposes of e-mail and chat activities outlined in this policy. 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.

3.9 Principals and Managers will ensure that they review the contents of this procedure with their staff at each significant revision of this procedure. New staff, at the time of hiring, will access this procedure as part of the hiring package from the Human Resources Dept. Principals will also ensure that teachers review this same procedure and Form 141-Appropriate Use Contract for Students with students from grade 4-12 at the beginning of each school year.

4. Computer Security: Staff and Service Providers

4.1 This section sets out some specific procedures for staff members and service providers related to maintaining a secure computing environment.

4.2 RCDSB 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 RCDSB 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 is securely managed throughout its life cycle and backed up as appropriate. Information and equipment disposal practices ensure the continued protection of privacy.

4.6 All software on the RCDSB's technological devices 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 Passwords 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 Technological devices such as 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. This includes downloading and/or using software designed to circumvent the user agreement and or other security measures implemented by the RCDSB.

5. Responsible Use of RCDSB Networks, 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, gaming or social networking 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 an electronic device to take embarrassing photos and electronically sending 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 social networking sites, designed to insult others.

5.2 These activities, when taking place off the school/work site or outside school/work hours normally are not school/work matters, but rather community or police issues. However, these activities can have an impact on the school/work and negatively affect the safety, climate and the learning environment at the school/work. In such cases, the use of the Internet and electronic messaging for bullying or harassment may be dealt with by the principal or manager.

5.3 The principal or manager, in consultation with the superintendent responsible, will determine whether conduct outside the school/work constitutes a school matter. Key factors in determining whether the behaviour concerns the school/work 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/work;

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/work; and

5.3.3 whether the conduct is injurious to the moral tone of the school/work and/or affects school/work safety and security.

5.4 If the principal or manager determines that off-site conduct has had or is having a negative impact on the school/work, the principal or manager may impose discipline in accordance with administrative procedures and RCDSB policy and/or, in consultation with the superintendent responsible, may involve police services.

5.5 Technological devices (for example but not limited to: smart phones, ipods, pagers, etc.) may not be carried or be in the possession of students during examinations and/or other major assessments unless the Principal has given permission for students to do so.

5.6 Using an electronic device to violate the privacy or integrity of someone else is prohibited in all areas, especially those where there is an increased expectation of privacy, such as washrooms or change rooms (ex. taking a camera or recording sound or video).

5.7 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 unless it is for a school sanctioned activity (i.e. yearbook, school paper).

5.8 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 or consent of the student if he/she is 16 or 17 and has withdrawn from parental control.

5.9 Violations under Section 5 will be dealt with according to administrative procedures, RCDSB policy and/or the police protocol.

6. Personal Technological Devices

6.1 Personal technological devices may be used during instructional time for educational purposes. Principals and teachers need to establish guidelines for the use of these devices with students which emphasize responsible and safe use as referenced in this policy.

Personal technological devices may be used outside of instructional class time, so long as the use of these devices does not distract from instructional class time, extracurricular activities, co-curricular activities and the use of the device does not violate any other school or RCDSB policy or negatively impact the network.

6.2 The school and/or RCDSB is not responsible for personal technological devices in the event of loss, damage or theft.

6.3 Users are responsible for the security of their personal device.

6.4 Users assume full responsibility for sharing or lending their personal device to others.

6.5 Users will not leave their personal device unattended in hallways, classrooms, or other school spaces.

6.6 Users agree to follow RCDSB Administrative Procedure 141: Computers: Network, Internet and Electronic Devices.

6.7 Users are responsible for maintaining their personal device at all times (troubleshooting, repair, connectivity to the wireless network, etc.).

6.8 Users will only connect to the wireless network and not to any wired network.

6.9 Users will not plug into the network any devices capable of broadcasting or sharing private access (e.g. wireless routers, game consoles, etc.). Users understand that such devices are NOT permitted under any circumstance.

6.10 Users will turn off all peer-to-peer (music/video/file-sharing) software or web-hosting services on their devices while connected to the school wireless network and respect the personal information of others.

6.11 Users understand that devices may be used in many areas of the building. However, they must always abide by the school rules and contribute to an atmosphere that supports class work and individual study.

6.12 Users understand school and RCDSB technology staff members may access their personal electronic device if there are reasonable grounds to believe there has been a breach of school rules, or discipline policies, or a network violation and that a search of the device could reveal evidence of the breach. This may include, but is not limited to, audio and video recording, photographs taken on school property that violate the privacy of others, and issues regarding bullying, viruses, trojans or other possibly damaging programs, etc.

6.13 If a student violates this administrative procedure, their personal technological device may be confiscated and returned to the parent or guardian, or to an adult student or 16/17 year old withdrawn from parental control, after the instructional day, or as appropriate to the circumstances.

6.14 All staff using personal devices containing access to confidential information shall have a pass code lock on that device to help prevent unauthorized access to data in the case of loss or theft. Loss or theft of devices (personal or Board owned) containing access to confidential information must be reported to the appropriate principal or manager.

7. Damage, Loss or Theft of RCDSB Property

7.1 Replacement resulting from wilful or malicious damage or theft of equipment or software shall be the responsibility of the perpetrator and/or parent or legal guardians. Malicious damage includes but is not limited to the deliberate introduction of a virus, or noxious program.

7.2 Damage caused by community groups shall be the responsibility of such group to arrange appropriate restitution.

7.3 Damage or loss of school or RCDSB equipment is the responsibility of the person, school, or RCDSB Department, assigned to the equipment.

7.4 Staff who possesses RCDSB-owned portable technological devices is expected to take reasonable measures to secure the devices when left unattended.

7.5 Staff will inform their principal or manager of damage, theft or loss of RCDSB-owned technological equipment. The principal or manager will also contact police in the case of theft.

7.6 The school principal or department manager will inform their respective superintendent and the IT manager of the theft of RCDSB-owned electronic devices and will arrange for replacement of the device. When contacting the superintendent a statement as to whether there was confidential information on the device will be made.

7.7 School or department staff will complete an Information Technology Help Desk ticket for RCDSB-owned technological devices that require repair.

7.8 The school administration, manager or superintendent will determine appropriate disciplinary action, including restitution, when electronic equipment has been willfully damaged and/or stolen.

7.9 The school administration will be responsible for seeking restitution from students and/or guardians when it has been determined that the electronic equipment was accidentally or willfully damaged and/or stolen.

7.10 If the school or department is not able to cover the replacement or repair costs, the administrator should contact the family of schools or department superintendent.

8. Electronic Social Media

8.1 The RCDSB recognizes the use of electronic social media by staff as a viable means to involve colleagues, parents, and students in academic dialogue.

8.2 The RCDSB is committed to supporting staff use of electronic social media to interact knowledgeably and responsibly via the Internet.

8.3 The social media policy applies to blogs, personal websites, RSS feeds, postings on wikis and other interactive sites, such as, but not limited to: Facebook, MySpace, Blogger, Twitter, Instant Messaging, and postings on video or picture-sharing sites and elsewhere on the Internet.

8.4 The RCDSB recognizes that teachers and other RCDSB employees are role models. Parents entrust educators with the duty to educate their children. The RCDSB recognizes that the use of the Internet and social media has the potential to affect this trust.

In accordance with the above-stated policy, RCDSB staff will implement the following procedures:

8.4.1 **Interactions Representing the RCDSB**

I. Staff, student council members etc. are not authorized to use electronic social media sites to speak on behalf of the school, department, or RCDSB unless given written permission from a principal or manager;

II. Personal sites and comments not related to the RCDSB will clearly state that staff are not representing the views of the school, department, or RCDSB.

8.4.2 **Respect, Privacy, and Confidential Information**

I. RCDSB staff will not disclose confidential student information or confidential school, department, or personnel records without first obtaining written consent from the principal, manager, or guardian for students under the age of 18 or from students aged 16 or 17 who have removed themselves from parental control;

II. RCDSB staff will not use electronic social media sites to be defamatory towards students, RCDSB employees, or RCDSB policies and procedures;

III. RCDSB staff will not engage electronically in behavior or comments that would reflect negatively on the school or RCDSB's reputation;

IV. Staff may be disciplined if their social media comments and posting, whether personal or school/RCDSB related, result in a disruption to the school or RCDSB environment; or negatively impact the staff's ability to perform his or her duties;

V. RCDSB and school logos will not be used without first obtaining permission from the school principal or manager;

VI. RCDSB staff will use only their own name, when participating in an online social media group for school/RCDSB-related purposes;

VII. RCDSB staff will ensure that their online comments are respective of the RCDSB's values and adhere to the procedures as outlined in the RCDSB's Character Development plan;

VIII. RCDSB staff can be disciplined for electronic commentary, content, or images that are defamatory, pornographic, proprietary, harassing, or that create a negative work environment;

IX. RCDSB staff may use the RCDSB network to access social media sites that are work-related; staff will not access non-work related social media sites during school/work hours;

X. RCDSB staff participating in social media activities will respect copyright laws, not only with respect to the content produced on the social media sites, but also to the software that enables it;

XI. RCDSB staff participating in social media activities acknowledge that all information posted to sites is subject to the provisions of the *Municipal Freedom of Information and Protection of Privacy Act;*

XII. Principals and managers may monitor employee use of social media and social networking websites.

8.4.3 **Staff-Student Online Correspondence**

I. Principals will inform all staff that online correspondence between staff and students must be related to course work, or school-sanctioned clubs/activities;

II. Principals will only approve school-based social media groups that include a staff member advisor and have at least two staff members with administrative privileges;

III. Principals will ensure that all school-sanctioned social media groups adhere to regular school code of conduct practices;

IV. Principals will inform staff members participating in school-created social media groups with students that the ethical standards for the teaching profession apply at all times, whether in a traditional school environment or an online environment;

V. RCDSB staff will not be initiating or accepting "friend" invites from students unless the networking is part of an existing school course or school club structure and at least one other staff member has administrative access to the social media group. This excludes family and close family friends.

9. Websites

9.1 Web pages and software applications of a personal nature or from an association or committee shall not be hosted on RCDSB computers or servers without the expressed consent of the RCDSB and the individual or group.

9.2 Any web page attributed to a school, department, RCDSB-approved committee or association, shall be approved by the principal, department manager or committee/association chairperson.

9.3 Web pages attributed to a school or a department shall be hosted by the RCDSB.

9.4 Web pages attributed to a school council shall be approved by the school council and the school principal and be hosted by the RCDSB as part of the school website.

9.5 Individuals wishing to display or execute applications or web pages on RCDSB servers which have been developed outside the scope of RCDSB influence or of personal interest will first request approval from their manager/principal and the supervisory officer of information technology. The individual will assign the RCDSB the right to use, display or execute these web pages or applications in a manner consistent with existing RCDSB policies and procedures.

9.6 Web pages developed by, or representative of, a school or department will first be approved by the manager/principal before being made available for web access. Such web pages will only be hosted on the RCDSB's web server.

9.7 Pictures of students included on school web pages must NOT include student names. Similarly, schools should not use filenames for pages and images which include student names. First names can be used for samples of student work. When posting images of students to a school or RCDSB webpage, student names will not be used.

9.8 When using pictures of persons on the school website, the school should obtain written permission.

9.9 No school page content should provide the means for people to contact any student directly. If communication back to the school is needed, it should be directed to the appropriate staff member.

9.10 All school websites must contain a link back to the RCDSB home page. This link must be prominent and displayed on the school's main page.

9.11 Schools hold many different types of personal information. Due to the nature of certain types of personal information, **some information should never be included on any websites**. This would include:

- Student's report card and academic transcript/individual student marks
- Student's Ontario Student Record (OSR)/Ontario Education Number
- Student's telephone number, home address, personal email address
- Parent's telephone number, home address, personal email address
- School and/or school RCDSB/authority staff's home address, telephone number, personal email address

9.12 Some students may not be concerned about their personal information being posted on the school website, and hence the web, while others are apprehensive. Types of personal information, which RCDSB's may decide to post, provided the proper consent is obtained, in advance, include:

- Photographs of students (individual and/or group)(with or without a name)
- Students' work (e.g., essays, projects, etc., with or without a name)
- Names of students participating in extracurricular activities and student council

- Names of students award-winners/prize/scholarship winners
- School yearbooks (names and photographs)

Some information may be considered "non-personal" when used alone but, when combined with a second piece of information, becomes personally identifying. A picture or a name on its own may not be considered "personal information," but together will form an identity that can be recognized.

9.13 **Information that may be personal information, depending on its content**

It should be noted that certain types of information may not appear to be personal information, but depending on the content, may contain personal information.

Examples of types of information, which may contain personal information are:

- School newsletters
- Minutes of meetings, including those of school councils
- Information on school events, such as fundraisers, drama productions, athletic competitions, science fairs

The above records need to be reviewed on a page-by-page basis. If they contain personal information, they should only be posted to the website if the personal information is edited out, or if the individuals to whom the personal information relates have consented to its posting.

9.14 **Guidelines for Teacher Websites**

A teacher website, under the direction of the principal, should be self-administered.
A teacher website should be directly related to the classroom curriculum.
Examples of classroom curriculum-related/educational material(s) are:

- Assignments
- Upcoming events or trips – being careful that posting time and place information may have impact on issues of custody.
- Sample lessons
- RCDSB-recommended educational sites
- RCDSB-recommended curriculum projects

Examples of non-classroom curriculum material, and therefore not permitted for posting, are:

- Individual student marks
- Attendance
- Personal information (non-classroom-related)
- Links to commercial websites

9.15 Information related to one's professional capacity or individual professional responsibilities do not constitute "personal information" as cited in MFIPPA legislation, Section 2.1 and may be posted on RCDSB/school websites. Examples of this type of information are:

- Staff lists with staff members' names, titles, contact information, department, and grade taught
- Names of staff members responsible for extracurricular activities
- Names of volunteers/community members/schools
- Photographs of staff members (individual and/or group photos)
- Photographs of volunteers/community members (individual and/or group photos)

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
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