



PROCEDURE

Title: **INFORMATION TECHNOLOGY APPROPRIATE USAGE AND ELECTRONIC MONITORING PROCEDURE**

Procedure No.: **5017b**

Effective Date: **2013 Nov 12**

Department: Organizational Support Services

Reference(s):

- Canadian Charter of Rights and Freedoms
- Equity and Inclusive Education Policy
- Information Technology Policy
- Information Technology Security Procedures
- Municipal Freedom of Information and Protection of Privacy Act
- Employment Standards Act, 2000
- Ontario College of Teachers Professional Advisory: Maintaining Professionalism
- Use of Electronic Communication and Social Media
- Ontario Human Rights Code
- Privacy and Records Information Management Policy
- Privacy and the Management of Personal Information Procedure
- Privacy Breach Protocol Procedure
- Records Information Management Procedure
- Harassment Policy
- Harassment Procedure
- Employee Code of Conduct Policy
- Employee Code of Conduct Procedure
- Off duty Code of Conduct Procedure
- Video Surveillance Policy
- Video Surveillance Procedure
- Policy/Program Memorandum 128

1.0 **Background**

This policy governs the use of “Information Resources”, which include Information Technology (IT) services, facilities, networks and equipment that the Board owns, operates, or sources from external parties for the use of students, employees and other authorized users. It is important for **all users** of Board-owned equipment to practice responsible and ethical behaviour in their computing activities.

Administered By: **Information Technology Services**

Amendment Date(s): 2012 Sept. 11, 2012 Dec. 18, 2022 October 3, 2024 June 10

Most Recent EIE Review Date:

Many staff have access to private and sensitive information that could injure

other persons and/or diminish the reputation of the Board if lost or disclosed inadvertently. All staff members and trustees are required to complete an annual declaration acknowledging awareness of and compliance with the Information Technology Policy and underlying procedures. Also, see Information Technology Letter for New Employees, regarding the use of technology in TVDSB.

Expectations for the appropriate use of technology by students are also incorporated in each school's Code of Conduct, as outlined in Section 4 of this document.

2.0 Principles

Information Resources and data owned by the Board are to be used solely for the furtherance of the Board's objectives and to be consistent with all laws, including the Canadian Charter of Rights and Freedoms, the Ontario Human Rights Code, the Ontario Occupational Health and Safety Act, the Municipal Freedom of Information and Protection of Privacy Act, the Employment Standards Act, 2000, Policy/Program Memorandum 128 and the applicable Board policies, including the Thames Valley District School Board Information Technology Policy #5017, the Information Technology Security Procedure #5017a, the Privacy and Records Information Management Policy #2014, and the Records Information Management Procedure #2014a, Privacy and the Management of Personal Information Procedure #2014b, Privacy Breach Protocol Procedure #2014c, Harassment Policy #3004, Harassment Procedure #3004a, Employee Code of Conduct Policy #3017, Employee Code of Conduct Procedure #3017a, Off Duty Conduct Procedure #3017c, Video Surveillance Policy #2017 and the Surveillance Procedure #2017a.

3.0 Online Publishing, Websites and Social Media

All web pages hosted on the Board's corporate site or paid for by the Board are considered the property of the Board and must comply with the principles and standards set out in the Information Technology Security Procedures. Online publishing must respect the Board's policies and procedures and be consistent with copyright and other laws, the Canadian Charter of Rights and Freedoms and the Ontario Human Rights Code. All school websites are to be created within the Board's system webpage. See Guidelines for TVSDB School and Teacher Websites.

TVDSB will restrict access to social media platforms on school networks and Board devices. Exceptions to permit the use of social media platforms by students for pedagogical or work-related purposes will be determined by the Board.

4.0 Appropriate Use of Technology

- 4.1 Every school is required to have a Code of Conduct that communicates to all members of the school community the types of behaviour expected of them. The Code of Conduct should include expectations with respect to computer use and mobile device use (see Sample Page for School Code of Conduct). Responsible use of computer resources helps ensure that they are used for educational benefit and that no harm or damage occurs to others or to data or equipment as

a result of misuse.

- 4.2 Handheld audio and video devices (e.g., cameras, MP3 players) may be used in the classroom and other designated areas of the school for instructional purposes with the permission of the school administration and teaching staff under certain conditions and in specific grades. Additionally, no one is to use their portable handheld device to audiotape or videotape other individuals (staff, student, parent/guardian or community members) without their permission while on school property, or at any school events. The appropriate use of Information Resources, mobile devices, network and licensed software at Board sites as well as access to the Internet using Board or personal equipment by both staff and students must be in support of education and educational research, and be consistent with the educational objectives of the Thames Valley District School Board. Unacceptable use includes, but is not limited to:
- activities which may damage equipment;
 - downloading, copying or transmitting any material which is in violation of any Federal or Provincial regulation such as copyrighted material; threatening or obscene material; hateful, racist or discriminatory material;
 - any breach of security on local and remote sites including use or attempted use of another user's account; unlawful entry or attempted entry into any network system; any attempt to gain unauthorized access to view, alter, copy, share or destroy data and the creation and/or willful transmission of computer viruses or virus hoaxes; and
 - activities supporting private business, personal interests (including political) or commercial ventures.
- 4.3 Network etiquette is expected to be followed including using appropriate and respectful language, the avoidance of the distribution of nuisance or junk mail and the efficient use of online time.
- 4.4 Students must follow personal safety measures including but not limited to the following: reporting to school staff any unusual or suspicious communication with others, not divulging any personally identifying information over the Internet and never agreeing to meet with strangers with whom they have communicated on the Internet.
- 4.5 Use of the Internet is an integral part of the educational experience in many school programs with a focus on education of appropriate usage and supervision of student work by staff. To supplement this supervision and education, Internet filtering is done on both the TVDSB wired and wireless networks to reduce the chance of accessing inappropriate material. Potentially inappropriate sites are blocked on personal devices using the wireless network. Parents/guardians will be advised, through the Parent Portal or school documentation, that their child will have access to the Internet.

- 4.6 Inappropriate use of the Board's assets and/or information resources will result in disciplinary action that may include dismissal. In the event of actions which may violate the law, the police will be informed.
- 4.7 Use of individually-assigned Board owned equipment by Board employees must be consistent with the educational objectives and practices of the Thames Valley District School Board.

5.0 **Electronic Monitoring**

- 5.0 The Board provides Information Resources to enable productive work, and has a duty to uphold the security of its Information Resources. This gives the Board a critical interest in having access to information related to the use of Information Resources.
- 5.1 Information resources must be used appropriately and inappropriate use is not permitted. Users of the Board's Information Resources should have no reasonable expectation of privacy. For greater certainty, the Board has the right, and without the consent of the employee, student, or other user, to monitor any and all of the aspects of its Information Resources, including, without limitation, reviewing documents created and stored on its computer system, deleting any matter stored on its Information Resources, monitoring websites visited by users, monitoring chat and news groups, reviewing all material downloaded or uploaded by users from the Internet, reviewing email sent and received by users, as well as social media activity if concerns warrant such attention. If privacy is required, a personal device that is not connected to the Board's network should be used. Users of the Board's Information Resources should also be aware that a password allows the Board to identify how Information Resources are being used, and does not preclude the Board from accessing information about its users.
- 5.2 The Board monitors its Information Resources and accesses accounts and information for its legitimate purposes, which include:
 - performing maintenance and repair;
 - upholding security and safety;
 - complying with a legal obligation;
 - supporting work and work continuity; and
 - conducting research to support business planning and other objectives.
- 5.3 The Board collects information about how Information Resources are used through a variety of tools, including the tools set out below. Information may be logged for subsequent inspection, may generate alerts that are sent to IT staff or may be actively monitored by IT staff who have access to a dashboard and other reports.

Type of monitoring	Explanation
Tools for filtering and logging traffic in and out of the Board's network	Network monitoring provides data on who is communicating in and out of the Board's network, what type of application they are using to communicate, when they are using it, and whether the traffic may indicate a security problem.
Tools for managing how applications and systems are used	Applications and systems (e.g. phone systems, student information system, financial system) monitoring typically provides data on who has used an application and when. Applications and systems may also track user actions, though this varies depending on the application or system.
Tools for managing and detecting anomalous events on devices – i.e., Board owned devices, personal devices connected to the Board's network or using Board account credentials	Device monitoring (e.g. anti-malware software, anti-virus software, device management software and configuration tools) provides data to determine if a device is being used without authorization or if there is another problem on a device.
Video surveillance systems	The Board employs video surveillance at some facilities for security purposes. For information about how and in what circumstances the Board uses video surveillance please see the Board's <i>Video Surveillance Policy & Procedure #2017</i> .
Access control systems	The Board employs electronic systems for controlling access to its facilities. If a Board facility is accessed using a Board access card, these systems will record the user identity, the point of entry and the time and date of entry.
Vehicle telematics (GPS) systems	The Board employs telematics in several Board owned and leased vehicles. These systems collect location data when vehicles are being used. The Board uses this data to manage its vehicle fleet and uphold driver safety and security.

- 5.4 The Board collects the above information routinely and accesses it on an as needed basis. The Board reserves the right to employ special monitoring tools or change settings or parameters of existing monitoring tools as part of a reasonable investigation, to address a changing threat environment or for other operational needs.

- 5.5 A copy of this policy will be retained by the Board until three years from the date on which this policy is no longer in effect. Similarly, if the Board revises this policy, a copy of the previous version of this policy will be retained until three years from the date of such revision.

Supporting Document for Information Technology Appropriate Usage Procedure

Information Technology Letter for New Employees

(Board Logo)

(Date)

Dear _____

Welcome to the Thames Valley District School Board (the "Board"). I am pleased to have the opportunity to write to you as you begin your employment with our Board. As part of your work responsibilities as a Board employee or trustee, you will have access to the Board's computer networks and data, email and the Internet.

So that the interests and well-being of students, other employees and the Board can be protected, Technology Security Procedures have been developed. Like other Board policies and procedures, these are available on the Thames Valley District School Board website. Your attention is drawn to the Policies and Procedures and you are required to read the Information Technology Policy, Information Technology Security Procedure and Information Technology Appropriate Usage Procedure carefully. Current copies of these documents are attached for your reference.

A basic principle is that information technology and equipment and data owned by the Board are to be used solely for the furtherance of the Board's objectives. In the procedures you will find stated the responsibilities of employees regarding the use of the Board's equipment and networks, appropriate use and protection of data, licensing of software and other copyright protection, protection of hardware from damage and responsibilities regarding Internet and email.

As with all Board policies and procedures, your compliance is expected. Failure to comply with these will result in disciplinary action that may include dismissal.

Questions or concerns about the Information Technology Policy and Procedures should be addressed through your supervisor or the Manager of Information Technology Services. It is my hope that this notification will ensure that you have all the information you require to ensure your understanding of this issue.

Yours truly,

Associate Director
Organizational Support Services

Supporting Document for Information Technology Appropriate Usage Procedure

Guidelines for TVDSB School and Teacher Websites

The Principal has the final responsibility for the content of the school website. Each Principal should work with appropriate, interested staff in creating the school website, ensuring that these guidelines are adhered to and that the content of the school website meets the Principal's approval.

- For consistency, maintainability, URL management, site security, and other related issues, all organizations of the school board, including schools and teachers must host their sites on the TVDSB web server. This enables system important information and emergency messages to be included on school websites. As well, with the connection to the teacher websites, the Principal is also able to remove the link, if necessary. There shall not be links to personal web pages or private businesses on these pages.
- The content of the school website and associated links must be consistent with the educational aims of the school board.
- School web pages shall not contain any commercial or promotional advertising. School web pages may contain acknowledgements of school partnerships or sponsorships.
- All school websites must contain a link back to the TVDSB home page. This link must be prominent and displayed on the school's main page.
- External site links should be credible, operating and checked on a regular basis.
- All website content must be AODA compliant. Content means any information that may be found on a web page or web application, including text, images, forms, documents and sounds.
- No school page content shall 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.
- Pictures of students included on school web pages must NOT include full 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 using pictures of students on the school website, the school shall obtain written permission, annually, on the registration/update forms.

Supporting Document for Information Technology Appropriate Usage Procedure – cont'd

- All student pictures must be removed after the end of the school year for which permission was given.
- School web pages must not use copyrighted materials without permission.
- All schools must include School Profile information on the “About Us” tab.
- Schools and teachers are encouraged to keep their website current, AODA compliant, and to periodically check to ensure that links are still valid.

Adapted from Privacy & Information Management, PIM Toolkit, 2008

Supporting Document for Information Technology Appropriate Usage Procedure

SCHOOL AND CLASSROOM GUIDE TO USING SOCIAL MEDIA BACKGROUND

Over the years, schools have employed a variety of strategies for communicating with parents/guardians and students – school newsletters, classroom monthly calendars, digital announcements – to name a few.

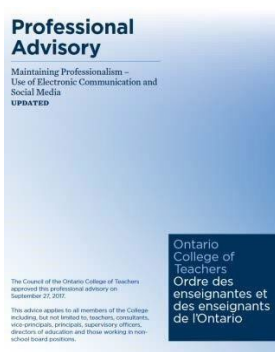
As the Internet grew in popularity, websites and email became additional tools available for sharing information with various audiences.

Supporting Document for Information Technology Appropriate Usage Procedure

GUIDING PRINCIPLES

As educators using social media, it is important to remember that we are bound by statutory and regulatory frameworks including the Education Act: Statutes and Regulations, the Ontario College of Teachers Act: Statutes and Regulations and the Teaching Professions Act (Section 18).

Use of social media by teachers as a learning tool or as a method of communicating with students, parents/guardians or colleagues should first and foremost be guided by standards of professional conduct outlined by The Education Act, collective agreements and the Ontario College of Teachers (OCT).



- OCT's Professional Advisory: Maintaining Professionalism – Use of Electronic Communication and Social Media:
http://www.oct.ca/publications/PDF/Prof_Adv_Soc_Media_EN.pdf “This professional advisory is intended to help Ontario Certified Teachers (OCTs) understand their professional boundaries and responsibilities in the appropriate use of electronic communication and social media.”

Canada. Ontario College of Teachers. Professional Advisory Maintaining Professionalism - Use of Electronic Communication and Social Media. Ontario College of Teachers 2017 Print.

In addition, the use of social media will be guided by the ethical and professional principles outlined in existing TVDSB Board guides, policies and procedures, notably:

- Information Technology Policy and Procedures
- Equity and Inclusive Education Policy_
<http://www.tvdsb.ca/files/filesystem/EquityandInclusiveEducationPolicy1.pdf>
- TVDSB Corporate Guide to Social Media, as posted on the TVDSB Facebook Page

Supporting Document for Information Technology Appropriate Usage Procedure – cont'd

WHAT IS SOCIAL MEDIA?

Social media is an ever-changing landscape consisting of websites and other online means of communication that are used by large groups of people to share information and to develop social and professional contacts.

SOCIAL MEDIA – THE POTENTIAL

“Electronic communication and social media tools provide exciting opportunities to learn, teach and communicate with students, parents/ [guardians] and your colleagues. They serve a range of purposes from helping students and parents access assignments and resources to connecting with communities all over the world.”

Canada. Ontario College of Teachers. Professional Advisory Maintaining Professionalism - Use of Electronic Communication and Social Media. Ontario College of Teachers, 2017 Print.

“Members also use the Internet and social networking sites as instructional tools, seeking resources to develop lesson plans and information to enhance their teaching practice. These tools provide powerful new ways for members to collaborate and dialogue with others, expand their professional network and continue their professional learning.”

Canada. Ontario College of Teachers. Professional Advisory Maintaining Professionalism - Use of Electronic Communication and Social Media. Ontario College of Teachers, 2017 Print.



<http://www.youtube.com/watch?v=8iMLjqlptBc>

"Professional Advisory: Electronic Communication, Social Media from Ontario College of Teachers - YouTube." YouTube - Broadcast Yourself. Ontario College Teachers, 05 Dec. 2011. Web. 05 Dec. 2011. <<http://www.youtube.com/watch?v=8iMLjqlptBc>>.

PRIVATE VERSUS PROFESSIONAL

There is a distinction between the professional and private life of a teacher. Ontario Certified Teachers are individuals with private lives; however, off-duty conduct matters and sound judgment and due care must be exercised. Teaching is a public profession. Canada's Supreme Court ruled that teachers' off-duty conduct, even when not directly related to students, is relevant to their suitability to teach. Members must maintain a sense of professionalism at all times – in their personal and professional lives. This level of professionalism is expected of all TVDSB employees.

Canada. Ontario College of Teachers. Professional Advisory Maintaining Professionalism - Use of Electronic Communication and Social Media. Ontario College of Teachers, 2017 Print.

PROFESSIONAL VULNERABILITY

- Staff can be vulnerable to unintended misuses of electronic communication and social media.
- Electronic messages are not anonymous.
- The use of the Internet and social media, despite best intentions, may cause staff to forget their professional responsibilities and the unique position of trust and authority given to them by society.
- Staff should never share information with students in any environment that they would not willingly and appropriately share in a school or school-related setting or in the community.
- Online identities and actions are visible to the public and can result in serious repercussions or embarrassment.

Adapted from Canada. Ontario College of Teachers. Professional Advisory Maintaining Professionalism - Use of Electronic Communication and Social Media. Ontario College of Teachers, 2017 Print.

MINIMIZING THE RISKS: ADVICE TO STAFF

- Interact with students appropriately
- Understand privacy concerns
- Act professionally
- Pause and ask yourself important questions

For more details on each of these points, please refer to: [Ontario College of Teachers Professional Advisory - Maintaining Professionalism - Use of Electronic Communication and Social Media](#)

Supporting Document for Information Technology Appropriate Usage Procedure – cont'd

Frequently Asked Questions (FAQs)

Do I need to have approval from my administrator before using social media in my classroom?

Yes, before engaging your students with social media, teachers must seek the approval, advice and input of their school administrator. Administrators will always be interested in hearing about the learning that is happening throughout the school. Your principal may have important suggestions and questions for you to consider as you make plans to bring social media into your classroom.

How can I start my own website?

Teachers within the Thames Valley District School Board are provided with the ability to create and maintain a teacher website that is affiliated with the websites of their current school of placement and the system website for the Thames Valley District School Board. If teachers wish to have a website, they must use this site, which is intended for classroom or system-related instructional or informational communications with students, parents/guardians, and the community. Teachers should consult the [Guidelines for TVDSB School Websites](#) for information on creating and maintaining their teacher website.

As a teacher, am I permitted to have a professional Facebook page or a Twitter account (or any other social media platform) in order to support student learning and classroom instruction?

Teachers may choose to design and provide unique and engaging learning experiences through social media sites and services (like Facebook or Twitter). If one does so, one must provide a clear understanding of the purpose behind its use as an **instructional tool** and be knowledgeable about how to facilitate its use to ensure safety for all students. Furthermore, online teacher conduct should reflect the same standards of professionalism that are expected within our schools. Teachers need to be aware of the risks of dealing with students one-on-one through messaging, emailing, casual online dialogue etc., and as such should message students as a group wherever possible.

How should I set my privacy settings on my social media sites? How often should I check my privacy settings?

Teachers need to familiarize themselves with and stay apprised of changes in the provider's Terms of Service. Check within the provider's documentation as social media sites often reserve the right to change and modify privacy measures for the end user at any time. Although it is good practice to constantly check and revise the privacy settings of your social media, it is best to proceed from the notion that everything you post, contribute or create online is never truly private, cannot be retracted, and will exist forever.

What do I do if I find inappropriate online content created by or directed towards my students?

As with all inappropriate conduct that can potentially impact the learning environment of a school and the safety of its students and staff, it is important to address online behaviour that does not comply with TVDSB and school policies, and codes of conduct. It is important to work

with your administration to uphold and apply disciplinary measures and standards that are in line with current interventions and supports at the classroom, school, and system level. In addition, teachers are reminded of their obligation under the duty of care to report issues regarding student and staff safety. Where possible, teachers may wish to minimize the possibility of inappropriate content being posted by using the option of approving messages/information before content is posted publicly (e.g., using notification services).

Sample Parent/Guardian Letter

(School Logo)

(Date)

Dear Parent or Guardian:

The purpose of this letter is to inform you that as part of our class this year, I am planning to make use of electronic communication and social media tools including, but not limited to (list the tools you will be using here).

The use of social media tools such as Facebook, Twitter, YouTube, Wikipedia, Edmodo, blogs, etc., provides students with a wider audience with whom they can share their ideas. At all times, students are expected to use the social media tools in a responsible manner and in support of the curriculum expectations being addressed. When students are able to safely share their ideas with an audience broader than just our classroom, they can often discover their voice and become even more motivated to learn, communicate, and share their ideas effectively with others. An additional outcome of our use of electronic communication and social media is to help students learn through experience, ways to safely use the Internet to share information and to collaborate.

To protect student privacy I will:

- Use only first names of students, if names are used at all, in identifying student work and ideas.
- Ensure that release forms have been signed if any pictures or videos are posted of your son/daughter as part of the work we are doing with the social media site.
- Engage students in a conversation about the importance of maintaining their own privacy and being aware of the risks and responsibilities when posting names and information related to other students.
- Familiarize myself with the provider's Terms of Service.

The Ontario College of Teachers provides the following statement regarding the use of electronic communication and social media tools in Ontario classrooms:

Electronic communication and social media tools provide exciting opportunities to learn, teach and communicate with students, parents/[guardians] and colleagues. They serve a range of purposes, from helping students and parents/guardians access assignments and resources to connecting with communities all over the world.

Canada. Ontario College of Teachers. Professional Advisory Maintaining Professionalism - Use of Electronic Communication and Social Media. Ontario College of Teachers, 2017 Print.

The school's Code of Conduct outlines expectations for students, including behaviour with respect to use of computers. Inappropriate use of the social media tools that we will be using could result in denial of computer privileges, suspension and/or legal action.

Information Technology Appropriate Usage and Electronic Monitoring Procedure

Inappropriate use includes, but is not limited to: (i) downloading, copying or transmitting any material which is in violation of any Federal or Provincial regulation such as copyrighted material; threatening or obscene material; hateful, racist or discriminatory material (ii) any breach of security including an attempt to gain unauthorized access to view, alter, copy, share or destroy another individual's work.

Please contact me at _____ if you have any questions

or concerns. Sincerely,

Teacher's Name

Sample Page for School Code of Conduct

Students are expected to use computer equipment, access to networks and the Internet responsibly for educational goals. So that all students can benefit from using computers for learning in a safe environment, the following rules apply.

Personal safety:

1. Students shall not give out personal information about themselves or others (such as address, phone number, pictures of themselves) to strangers met through the Internet/Social Media
2. Web pages/Social Media shall not contain personal information about students unless parents/guardians have given consent (e.g., address, phone numbers, pictures).
3. Students shall report to a teacher or other school staff member any computer or Internet/Social Media related activity (e.g., threats, abusive language) that gives them concern or appears to threaten the safety of people or places.

Use of equipment, software and networks:

1. All equipment, including cables and network drops shall be used in ways that do not cause damage.
2. Use of computer resources including the Internet/Social Media shall respect the safety and rights of others. Information shall not be accessed, downloaded, stored or distributed that is illegal, abusive, threatening, obscene, harassing or otherwise inappropriate.
3. Students shall not share passwords or use the passwords of others nor should they try to hack into computer systems.
4. Computer files or the data in files shall not be deleted, modified, moved or copied unless permission has been given to do so by a school staff member.
5. Creating and transmitting computer viruses, hoaxes, email worms, or sending junk mail or similar nuisance behaviour or related threats to computer security is not permitted.
6. Software used shall be properly licensed unless it is made available free by the creator ("freeware"). Licensed software shall not be copied illegally.
7. Email, conferencing, on-line chat and content of web pages shall respect the safety and rights of others.
8. Students shall report to a teacher or other school staff member any inappropriate use of computer equipment, software or networks, including the Internet/Social Media.

9. Students shall not pretend to be someone else.
10. Students shall not intentionally access Internet sites with inappropriate content of no educational value.
11. If using the work of others, credit must be given and permission obtained if copyright materials are used.
12. Handheld audio and video devices (e.g., cameras, MP3 players, cell phones) may be used in the classroom and other designated areas of the school with the express permission of the school administration.
13. No one is to use their portable handheld device to audiotape or videotape other individuals (staff, student, parent or community members) without their permission while on school property, or at any school events.

Inappropriate use of the Board's computer resources will result in consequences. If the actions of a student appear to break the law, the police will be informed.

(Toronto District School Board's Internet Acceptable Use Guidelines used as a resource)