Waterloo Region District School Board

Administrative Procedure 4070
RESPONSIBLE USE PROCEDURE FOR INFORMATION, COMMUNICATION AND COLLABORATION TECHNOLOGIES

Responsibility:	Associate Director and Executive Officer, IT and Digital Transformation
Legal References:	*Canada's Anti-Spam Legislation* *Copyright Act (RSC , 1985, c. C-42)* *Criminal Code (RSC , 1985, c. C-46)* *Education Act, R.S.O. 1990, c. E.2*
Related References:	*PPM 128 – The Provincial Code of Conduct and School Board Codes of Conduct* *Board Policy 6000 – Safe Schools* *Board Policy 6001 – Code of Conduct* *Board Policy 6008 – Student Discipline* *Board Policy 6009 – Student Bullying Prevention and Intervention* *Board Policy 2004 – Character Education and Social-Emotional Skills Development* *Board Policy 2012 - Network Access and Monitoring* *Board Policy 1014 - Privacy Protection and Access to Information* *Administrative Procedure 1260 – Student Discipline Procedure* *Administrative Procedure 3760 – Progressive Discipline* *Administrative Procedure 4110 – Selection & Reconsideration of Educational Resources* *Administrative Procedure 4580 – Technology and Audio-Visual Equipment Procedure* *Administrative Procedure 4115 - Online Educational and Business Tools* *Administrative Procedure 1375 – Student Use of Personal Mobile Devices* *Administrative Procedure 4050 – WRDSB Communication Systems* *Administrative Procedure 4060 – Board Email Protocol* *Administrative Procedure 4080 – Filtering System/Internet* *Administrative Procedure 4090 – Copyright* *Generative Artificial Intelligence (AI) Guidelines for WRDSB Staff*
Revisions:	September 2020, September 2024, January 2026
Reviewed:	June 2019

1. **Preamble**

1.1. The Responsible Use Procedure for Information, Communication, and Collaboration Technologies (RUP) outlines expectations related to the responsible use of Waterloo Region District School Board (WRDSB) information, communication and collaboration technologies, and accompanying resources, including emergent technologies.

1.2. Expectations in the RUP align with WRDSB's Character Development initiative concerning general conduct across the system. Character Development is the positive social and emotional development of students that is modeled by all staff, and is a key element in fostering a positive, inclusive system and school climate. All technology, information, and resources, and their use, must clearly support these WRDSB goals.

1.3. It is reasonable to expect that all individuals or groups who use WRDSB technology (includes but is not limited to: staff, trustees, students, parents/guardians, labour groups, volunteers) understand and comply with the expectations outlined in the RUP. As a WRDSB procedure, the RUP does not require individual or group signatures to indicate acceptance or compliance.

1.4. To achieve system awareness, the WRDSB will ensure a web link to the RUP is incorporated into all network logins. It is also understood that any user who attaches to our network understands and agrees to the RUP.

1.5. The WRDSB believes that the benefits of access to information, communication, and collaboration technologies and resources far exceed the disadvantages. Abuse of these services however, may lead to an individual's privileges being revoked. Misuse may be subject to disciplinary action and possibly civil or criminal action. Infractions of the RUP will be handled in a manner comparable to non-technology infractions that follow established WRDSB policies and procedures related to staff conduct and student discipline.

1.6. Canada's anti-spam legislation prohibits the sending of commercial electronic messages (CEMs) that encourage recipients to participate in a commercial activity, even if it is not-for-profit, unless they have the recipient's prior consent. Examples of CEMs include emails or text messages to inform parents and community members of promotions, advertising or offers for the sale of such things as student photograph packages, field trips, fun fairs, pizza or hot dog days, yearbooks or fundraising events. More information can be found at http://staff.wrdsb.ca/casl/.

1.7. Staff and students must only use educational and business tools that are approved by WRDSB and strictly follow applicable conditions of use.

2. Digital Citizenship

2.1. WRDSB strives to model and teach the safe, legal, ethical and responsible use of information, technology and resources, and expects all users to embrace the following conditions or facets of being a digital citizen:

- respect yourself;
- protect yourself;
- respect others;
- protect others;
- respect intellectual and technological property;
- protect intellectual and technological property.

2.2. Individuals are responsible for supporting personally-owned devices. As digital citizens, this includes, but is not limited to:

- knowing how to activate Wi-Fi on their devices and connect to a wireless service;
- maintaining virus and malware protection on personally-owned equipment;
- enabling personal firewall settings on personally-owned laptops and/or netbooks;
- disabling any internet sharing settings that would interfere with other users;
- operating in a manner consistent with Character Development and Digital Citizenship goals.

3. Responsible Use of Artificial Intelligence

3.1. WRDSB is committed to the responsible integration of Artificial Intelligence (AI) technology and tools in education and operations. AI technologies (e.g., generative AI systems such as Google Gemini or Microsoft 365 Copilot Chat) can provide innovative learning opportunities and have the potential to positively benefit creativity and productivity.

3.2. However, any use of AI technology or tools within WRDSB must be ethical, transparent, and in compliance with all legal standards and with the Board's values of privacy, equity, and academic integrity. This section outlines the expectations to employ AI in a manner consistent with existing policies and digital citizenship practices, ensuring all users uphold privacy, be mindful of the potential bias and misinformation, maintain academic integrity, and align with WRDSB's commitment to safe and inclusive learning environments.

3.3. **Students** must use AI tools responsibly and only for legitimate educational purposes under staff guidance. Students are expected to:

3.3.1. **Protect personal information:** Never input any personal details (such as names, addresses, account information, etc.) or sensitive data about yourself or others into AI systems, in order to safeguard privacy and data security of everyone.

3.3.2. **Maintain academic integrity:** May use AI resources only for educational purposes as directed by an educator. All AI use should support learning objectives and skill development adhering to the instructions from the teacher. AI assistance should be acknowledged or cited as required to avoid plagiarism.

3.3.3. **Think critically:** All AI tools hallucinate when preparing responses, make sure to evaluate AI-generated content carefully. Students should cross-check with reliable sources and be alert to potential biases or inaccuracies in AI output, rather than accepting information at face value.

3.3.4. **Respecting Code of Conduct:** Using AI to generate content to produce inappropriate, harmful, or discriminatory material that violates WRDSB's code of conduct is prohibited. AI should not be used to bypass rules or security or circumvent learning. Such misuse of technology will be treated as a RUP infraction under the Board's discipline policies.

3.4. **Staff** must ensure any integration of AI into teaching or work is conducted in an ethical, transparent, and pedagogically sound manner. Staff responsibilities include:

3.4.1. Board Approved AI tools only: Using only AI tools that have been vetted, reviewed, and approved by WRDSB. Educators should consult Board procedures, and the WRDSB Online Educational Tools and the applicable conditions of use prior to using these tools. Staff must not upload confidential or personally identifiable student or staff data into AI tools. They must adhere to the conditions of use and AI Guidelines.

3.4.2. **Use of AI Tools in Meetings:** Employees shall ensure all AI assistants, transcription tools, and generative AI applications are disabled prior to the start of meetings. Use of such tools is only permitted when explicitly authorized for collaboration with the Ministry of Education or other approved partner organizations or approved tools are being utilized, in alignment with Board privacy and security requirements.

3.4.3. **Promoting AI literacy:** Educating and guiding students on the safe, ethical, and critical use of AI. Including but not limited to, discussing AI limitations, potential biases, misinformation, irrelevant or outdated answers, etc. Teaching students skills to verify AI-produced facts with reliable sources.

3.4.4. Enhance, not replace learning: Only using approved AI tools where they are appropriate. They should be only used when it benefits, enriches, and augments learning outcomes or improves efficiency.

3.4.5. Monitoring and Support: Supervise student use of AI and intervene if misuse or academic dishonesty is suspected. Staff should rely on existing Board's policies and procedures to follow the process if the scenario of misuse or misconduct is confirmed.

3.4.6. Evaluation: AI technologies are advancing quickly and to stay up to date and responsive, relevant policies and procedures will be updated regularly. Educators and staff are encouraged to evaluate and suggest improvements to the RUP and WRDSB AI guidelines.

4. Access

4.1. WRDSB believes that individuals benefit from access to information and communication technologies for collaboration and discussion. WRDSB, by providing access, recognizes the potential to support curriculum and student learning expectations in order to promote educational excellence.

4.2. Technology users should have opportunities to:

- access internal, local, national, and international sources of information;
- collaborate and communicate across the WRDSB and with local and global communities;
- develop knowledge and skills that will be useful throughout their lives.

4.3. All equipment, information/data, and resources owned by WRDSB, regardless of the location, must be used for the purpose of carrying out the mandate of WRDSB.

4.3.1. It is at the sole discretion of WRDSB to decide who is given access to WRDSB equipment, information/data, and resources, and who retains, and who is denied access.

4.3.2. WRDSB has the right to access user content on any WRDSB system, or confiscate devices at WRDSB's discretion. Reasons for these actions may include, but are not limited to:

- engaging in technical maintenance, repair and management;
- meeting legal requirements to produce records;
- ensuring continuity of work processes;
- improving business processes and managing productivity;
- preventing misconduct and ensuring compliance with the law.

5. Responsibilities

5.1. WRDSB will make every effort to protect users of WRDSB technology from misuse and abuse, and will take reasonable steps to ensure information, communication and collaboration technologies are used only for purposes consistent with the WRDSB's corporate and learning expectations and Character Development and Digital Citizenship goals.

5.2. Staff are responsible for role modeling. In particular, teaching staff are responsible for the ongoing development of students and the review of the rules and responsibilities of being a digital citizen with them.

5.2.1. Staff also provide protection, by restricting access (within the technical limitations of products) to material that has no business or educational value or is inappropriate, such as material deemed to be racist, pornographic, dangerous or obscene.

5.2.2. Staff ensure a level of privacy and protection for all users (note that this level of privacy does not preclude the fact that approved support and administrative personnel may access mail, data, and software on systems).

5.2.3. Staff ensure a level of security by taking the steps to prevent electronic trespassing.

5.2.4. Staff ensure guidelines for the selection of appropriate equipment, learning resources and services are followed, and are in accordance with current WRDSB policies and procedures.

5.3. Supervisors in schools, sites and departments are responsible for ensuring the RUP is available in its entirety in prominent locations and in at least two of the following:

- student handbook;
- staff handbook;
- parent handbook;
- code of conduct or behaviour guidelines;
- school or department newsletter
- school website.

5.4. Additionally, supervisors provide, as appropriate and available, access to information, communication and collaboration technologies and resources and monitor these services for appropriate use and behaviour within their site/department.

5.4.1. Supervisors deal with abuse of privileges in a manner consistent with the Board's existing staff conduct and student discipline policies and procedures.

5.5. Individual users of information, communication and collaboration technologies and resources, must guard against inappropriate, unethical and illegal activity and are responsible for:

- understanding and adhering to the Board's Character Development, Digital Citizenship and RUP goals;
- promoting the acceptable use of information, communication and collaboration technologies and resources;
- using all WRDSB services, devices, and applications responsibly and for administrative and curricular purposes only, within the framework and standards set by the WRDSB;
- only sending commercial electronic messages using WRDSB approved tools and only to individuals who have provided their expressed consent to receive such messages;
- protecting the integrity of their account usernames and passwords (includes devices such as Smartphones) – this involves changing default passwords;
- all content held within their accounts;
- protecting the integrity and safety of their content by ensuring current WRDSB security measures and practices are followed;
- protecting equipment assigned to them from theft or damage and adhering to rules of hardware etiquette promoted by the WRDSB;
- respecting the integrity and security of the WRDSB's corporate (wired) network by using only approved and appropriately configured devices that are deployed by Information Technology Services.

5.6. Students must refrain from using personal mobile devices at all times during the instructional day, except under the following circumstances:

- For educational purposes, if explicitly permitted by the educator;
- For health and medical purposes;
- To support special education needs, as documented in the student's IEP;
- During breaks, lunch and spares, if the student is in Grade 7 to 12.

5.7. In accordance with PPM 128, students are responsible for their personal mobile device, how they use it and the consequences of not following the WRDSB's policy on personal mobile device use, which may include progressive discipline.

6. Infractions of the RUP

6.1. WRDSB believes that individuals benefit from access to communication and collaboration services and resources and computer technology. Adults, whether they are staff or students over the age of eighteen are responsible for their own use of these services. Parent(s) and/or guardian(s) are responsible for encouraging students under age eighteen in the appropriate use of technology in the school.

6.2. Violating the RUP may result in:

- restricted network access and/or access to computer technology;
- loss of network access and/or access to computer technology;
- surrender of personal mobile device to an administrator
- suspension and/or expulsion;
- fines
- civil or criminal charges.

6.3. Consequences for RUP infractions are determined by the supervisor, as they deem appropriate, using the applicable Board policy or procedure and/or involving:

- Information Technology Services staff to gather forensic evidence;
- the appropriate law enforcement agency if the infraction is deemed to be criminal.

6.4. To address incidents of inappropriate use of technology, supervisors and teachers should apply the strategies of:

- education;
- progressive discipline;
- early and on-going intervention strategies;
- restorative justice;
- character development and digital citizenship.

7. **Requesting ITS Assistance for Infractions**

7.1. WRDSB's Network and Data Security Analyst (519-570-0003, ext. 4595) is contacted:

- if an infraction of the RUP is suspected and staff at the site require assistance in collecting material evidence or identifying the scope of the incident;
- in situations where WRDSB technology infrastructure has been compromised or there is a major threat to students and staff or the system.

In these cases, supervisors or teachers should restrict access to those computers/devices and files related to the incident.

7.2. The Network and Data Security Analyst will involve and inform other Information Technology Services staff and supervisors as required.

8. **Violations of the RUP**

Inappropriate conduct includes, but is not limited to, the types of activities listed on the following pages. The chart outlines a series of incidents which contravene the RUP – the incident; the code of conduct violated; and the equivalent non-technology situation.

INCIDENT	CODE VIOLATION	EQUIVALENCE
Using WRDSB technological property for any illegal activity, including hacking.	**Respect Property**	● Theft
Placing unlawful information such as hate literature on the WRDSB's technological property or distributing it via the system.	**Respect Others**	● Bullying
Plagiarism or copyright violation.	**Respect Property**	● Plagiarism ● Theft
Developing or accessing programs that harass others, infiltrate a computer system or alter the software components of a system.	**Respect Property** **Respect Others**	● Bullying ● Moral Tone of School ● Theft
Degrading or disrupting equipment or system/network performance of WRDSB or other systems (e.g., introducing a virus, attaching personally owned or non-approved, non-standard devices to the network).	**Respect Property**	● Vandalism

Vandalizing equipment or the data of other users (e.g., opening up the equipment, changing data).	**Respect Property** **Respect Others**	● Vandalism
Sending messages that introduce a computer virus and are likely to result in the loss of a recipient's work or in the disruption of the system/network.	**Respect Property** **Respect Others**	● Vandalism
Sending "chain letters" or global messages or other types of communications which would cause congestion (spamming) of the system.	**Respect Property** **Respect Others**	● Vandalism
Purchasing an item other than the approved WRDSB standard.	**Respect Property**	● Not Following WRDSB Procedures
Attaching personally owned or non-approved, non-standard devices to the corporate network.	**Respect Property**	● Not Following WRDSB Procedures
Refusal to store personal mobile device out of view and powered off or set to silent.	**Respect Yourself** **Respect Others**	● Not Following WRDSB Code of Conduct

Inappropriate personal use, such as but not limited to:

INCIDENT	CODE VIOLATION	EQUIVALENCE
Downloading files that are not for educational purposes (e.g., games, movies and music).	**Respect Property**	● Theft ● Copyright Infringement ● Inappropriate Personal Use
Using WRDSB technological property for personal, political, financial or commercial gain.	**Respect Property**	● Inappropriate Personal Use ● Business Conduct Violation

Using WRDSB technological property to offer or provide goods or services or to advertise products.	**Respect Property**	● Inappropriate Personal Use ● Business Conduct Violation
Using WRDSB technological property to conduct political campaigns or advocate for or against candidates involved in municipal, provincial or federal elections.	**Respect Property**	● Inappropriate Personal Use ● Business Conduct Violation

Abuses of privacy and personal information, such as but not limited to:

INCIDENT	CODE VIOLATION	EQUIVALENCE
Invading the privacy of individuals, harassing others or personally attacking others with harmful intent.	**Respect Others** **Protect Others**	● Bullying ● Risk to Safety
Using WRDSB technological property to give out personal information such as home addresses, telephone numbers or credit card numbers.	**Respect Yourself** **Protect Yourself**	● Sharing Locker Combinations
Sharing or using others' access codes, account numbers, passwords and other authorizations which have been assigned to them.	**Respect Others** **Protect Others**	● Sharing Locker Combinations
Accessing email services which allow users to maintain anonymity.	**Respect Others** **Protect Others**	● Spreading Rumours

Abusive behaviour and defamatory activities, such as but not limited to:

INCIDENT	CODE VIOLATION	EQUIVALENCE
Downloading or posting inappropriate comments, defamatory remarks or pictures about the Board, or its schools, students, or staff.	**Respect Others**	● Bullying ● Inappropriate Behaviour ● Moral Tone of School
Using abusive, offensive, degrading or objectionable language in public or private messages.	**Respect Others**	● Bullying ● Inappropriate Behaviour ● Moral Tone of School
Establishing or accessing websites, links, postings or email messages which may imply a connection to the WRDSB and are criminal, degrading, defamatory or inappropriate.	**Respect Others** **Respect Property**	● Inappropriate Behaviour ● Moral Tone of School
Sending or receiving messages and/or images that are inconsistent with the WRDSB's curriculum and conduct procedures. These include messages and/or images which are racist, pomographic, dangerous, and obscene, or contain threats of violence.	**Respect Others** **Respect Property**	● Bullying ● Inappropriate Behaviour ● Moral Tone of School
Posting anonymous messages.	**Respect Others**	● Spreading Rumours

Circumventing security and integrity of technology, such as but not limited to:

INCIDENT	CODE VIOLATION	EQUIVALENCE
Gaining unauthorized access to resources, files, programs, other computer systems or technological entities through electronic trespassing.	**Respect Others** **Respect Property**	● Trespassing
Deliberately bypassing or attempting to bypass security provisions implemented by the WRDSB (e.g., content filter, firewall, etc.).	**Respect Property**	● Inappropriate Behaviour
Installing unauthorized, non-WRDSB approved operating systems.	**Respect Property**	● Inappropriate Behaviour
Installing tools intended to circumvent security measures (e.g., password hackers, network "sniffers").	**Respect Property**	● Vandalism

Appendix A – WRDSB Responsible Use Procedure and Mobile Device Use - Parent/Guardian Sign-Off