

RESPONSIBLE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT)

Administrative Procedures Cross Reference: Student Code of Conduct; Respectful Workplace; Use of Copyright Protected Work

Legal/Regulatory Reference: [Manitoba Education – Literacy with ICT Across the Curriculum](#); [The Freedom of Information and Protection of Privacy Act \(FIPPA\)](#)

1. Purpose and Philosophy

The Swan Valley School Division (SVSD) provides technology resources to support educational excellence and the efficient performance of professional duties. Access to these resources is a privilege, and all users—staff and students—are expected to act in a responsible, ethical, and legal manner.

2. Staff Section: Responsible Use of ICT

2.1. Professional Expectations

- **Mission Alignment:** Staff use of divisional telecommunication and network services must be consistent with the mission of the Division and used to perform assigned job duties or educational tasks.
- **Communication:** Employees are encouraged to use divisional email and tools for tasks associated with their assignments. Staff are responsible for checking and responding to emails regularly.
- **Security Training:** All staff are periodically required to participate in **online security** training provided by the Division to ensure the protection of student and staff data.

2.2 Privacy and Monitoring

- **No Expectation of Privacy:** Data stored on, or transmitted through, divisional equipment (computers, servers, networks) is the property of the Division.
- **Administrative Oversight:** The IT Department and Senior Administration reserve the right to monitor, audit, or intercept any information to maintain system integrity and ensure compliance with divisional administrative procedures.

2.3 Supervision of Student ICT Use

- **Guidance:** Teachers have a responsibility to help students develop skills to evaluate information sources and identify age-appropriate material.
- **Active Supervision:** Staff must supervise students while they are accessing the internet in the classroom.

2.4 Prohibited Actions

Staff shall not use divisional resources for:

- Commercial or profit-making ventures.
- Sharing personal passwords for any managed accounts.
- Installing unauthorized hardware or unlicensed software.
- Accessing, downloading, or displaying obscene, racist, or sexist material.

2.5 Consequences for Misuse

Violations of this procedure by staff may result in:

- Temporary or permanent removal of network and equipment privileges.
- Progressive disciplinary action, up to and including a recommendation for dismissal.
- Legal action or involvement of law enforcement if a violation of the law (e.g., copyright, criminal harassment) has occurred.

3. Student Section: Responsible Use of ICT

3.1 Access Requirements and Supervision

- **Parental Permission & Agreement:** To obtain network and internet access, all students must obtain parent/guardian permission, and both the student and parent/guardian must sign the Acceptable Use Agreement form.
- **Location and Hours:** Student divisional internet access is permitted only during school hours.
- **Mandatory Supervision:** K to Grade 8 Students may only use internet access under the active supervision of a staff member.
- **Web Awareness & Safety Instruction:** Teachers, as part of regular instruction, will provide students with orientation and information regarding web awareness, online safety, and acceptable use.

3.2 Student Responsibilities Students are expected to act in a responsible, ethical, and legal manner at all times. Specifically, students must:

- **Personal Accountability:** Take personal responsibility for their behavior while using division computers, networks, and internet access.
- **Safeguarding Access:** Take full responsibility for safeguarding and protecting their assigned account access.
- **Authorized Use Only:** Use local area networks and internet access solely in a manner assigned by network administrators and consistent with division administrative procedures.
- **Reporting Security Issues:** Disclose misuses of computing resources or potential system security problems to appropriate authorities and cooperate with school division administrators in investigations.
- **Website Creation Approval:** Obtain proper administrative approval before creating or posting a website on any division server.
- **Bandwidth Management:** Perform large file downloads or distributions during non-peak usage times where possible to prevent network congestion.

3.3 Prohibited Student Actions Students are strictly prohibited from performing any of the following actions on division systems or networks:

- **Offensive Content:** Sending, displaying, or soliciting offensive messages or images, including sexually explicit, hate-based, discriminatory, or sexist material.
- **Inappropriate Language & Harassment:** Using obscene language, or harassing, insulting, or attacking others.
- **Privacy Violations:** Re-posting personal communications marked as private without the original author's consent, or trespassing in others' folders, documents, or files.
- **Unauthorized Access:** Using or attempting to access others' accounts, or accessing and distributing others' passwords and private information.
- **System & Software Tampering:** Damaging computers, networks, or software; making unauthorized repairs, additions, software installations, or system reconfigurations; or installing/distributing files that may introduce a virus.
- **Non-Curricular Activity:** Downloading or using games, chat lines, or other tools not related to curricula or division administrative procedure.

- **Copyright Infringement:** Violating copyright laws by copying, installing, or distributing copyrighted programs or materials.
- **Unlawful or Commercial Use:** Employing the network for commercial purposes, political lobbying, or illegal activities.
- **Unauthorized Recording:** Recording or distributing in-class or virtual instruction without the explicit consent of all parties involved.
- **Resource Waste:** Intentionally wasting limited computing or network resources.

3.4 Consequences for Student Misuse Violations of these regulations by students will be considered grounds for disciplinary action, which may include:

- Loss of network and computer access privileges.
- Restitution activities.
- Suspension or expulsion.
- Appropriate legal action or involvement of law enforcement.

Swan Valley School Division: ICT Student & Parent Acceptable Use Agreement

Student Name: _____ School: _____

Student Agreement: I agree to follow the rules for computer and internet use as outlined in Administrative Procedure 234: Responsible Use of Information and Communication Technologies (ICT). I understand that technology is a privilege and that my files are not private and may be reviewed by staff to ensure responsible use.

Student Signature: _____ Date: _____

Parent/Guardian Permission: I have reviewed this agreement with my child. I understand that the Division uses content filtering but that keeping students safe is a joint responsibility. I grant permission for my child to access the school network and internet.

Parent/Guardian Signature: _____ Date: _____