

Sunrise School Division

Sunrise Procedure

Procedure Number - 3300

Procedure Title	ICt Acceptable Use		
Date of Issue	March 2005	Related Procedure	Online Publishing 7300
Revision Dates		Related Forms	<ul style="list-style-type: none">Online Publishing Permission FormOnline Photograph Permission Form
Review Date	March 2007	Originator	Superintendent

ICt Acceptable Use Procedure

Rationale

- Information and communications technologies are increasingly part of the fabric of everyday life. Access to these valuable learning resources will greatly enhance the ability of teachers to provide new and exciting learning opportunities for students.
- Material made available on the Internet is not governed or regulated in any way. It is impossible to predict with certainty, the accuracy and age-appropriateness of material that students may access.
- The use of the Internet has created new ethical challenges for schools related to appropriate use, privacy and security, and copyright/intellectual property issues. It is the responsibility of administrators, teachers, parents, and students, to ensure that access to telecommunication networks and computers provided by the division are not abused; and that everyone continually works together to maintain, enforce, and reinforce a culture of academic and technological integrity.

Procedure

- Sunrise School Division will develop and maintain an ICt infrastructure that includes computers, a WAN, connectivity to the Internet, and web filtering capabilities, and site based websites.
- The Sunrise School Division will endeavor to provide appropriate safeguards to provide for staff and student privacy and safety.
- In order to have access to divisional ICt's, all staff, parents, and students need to acknowledge and then exercise appropriate, respectful, and responsible use of divisional ICt's.
- As a result of the inappropriate use of ICt's, staff and students can have their access to divisional ICt's restricted.

Practices

Provision of Computer and Network Privileges

- Any divisional use of the Internet must be in support of education and consistent with the educational objectives of the Sunrise School Division.
- Sunrise expects staff and students to exercise appropriate, respectful, and responsible use of computers.
- Students and appropriate staff (administrators, secretaries, managers, business and education center staff, and teachers) will be provided an account on an annual basis for as long as they are a staff member or student of Sunrise.
- In connection with inquiries into possible abuses, Sunrise School Division reserves the right to examine files, programs, passwords, accounting information, printouts or other computing material without notice. Privacy of any electronic or printed material examined during an investigation of abuse that is not relevant to the investigation is guaranteed.
- Inappropriate use, by staff or students, can result in a cancellation of these privileges and other disciplinary action as determined by the Sunrise School Division.

Responsibilities

- Every user is expected to adhere to this policy whether division network access is gained from in or out of school settings.
- Application for Network and/or Internet accounts indicates the applicant will comply with the attached use policies and will be a responsible, efficient and ethical user. Failure to adhere to the policies and guidelines will result in the revocation of use privileges.
- It is expected that users will inform appropriate staff of misuses of computing resources or potential loopholes in computer systems security. It is also expected that they cooperate with the ICt staff in their investigation of abuses.
- All users are to have valid, authorized accounts and may only use those computer, network, and Internet resources that are specifically authorized. Users may only use their account in accordance with its authorized purpose. It is expected that all staff maintain compliance with the rules and regulations of the Sunrise School Division ICt Acceptable Use Policy.
- Users are responsible for safeguarding their own account. Users should not let another person use their account unless authorized by the system administrator for a specific purpose. Passwords should be changed often to ensure that private and secure files are kept that way.
- A user may not change, copy, delete, read or otherwise access files or software without permission of the owner of the files or the system administrator. A user may not bypass accounting or security mechanisms to circumvent data protection schemes. A user may not attempt to modify software except when intended to be user customized and permission for that specific purpose has been given.
- A user may neither prevent others from accessing the system nor unreasonably slow down the system by deliberately running wasteful jobs, playing games, or sending mass mailings or chain letters.

- Users should assume that any software they did not create is copyrighted. They may neither distribute copyrighted or proprietary material without the written consent of the copyright holder nor violate copyright or patent laws concerning computer software, documentation or other tangible assets. Not all information on the Internet is free, appropriate, and available for any type of use—the perception that the Internet is part of the “public domain” in this way is incorrect.
- Attempts to log into the system as any other user will result in cancellation of user privileges. Attempts to log into any system as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access.

Etiquette

Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- Be respectful. Do not write or send abusive, defamatory, offensive, or harassing messages to others. The same moral and ethical behavior that applies in the non-computing environment applies in the computing environment.
- Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
- Keep personal home addresses and phone numbers, and those of students or colleagues, strictly confidential. For personal safety, it is very important that this information is not disclosed to anyone on the Internet.
- Refrain from posting a student’s picture without parental consent or a staff member’s photo without their permission.
- Obtain the permission of the site administrator before using diskettes, other magnetic media such as compact disks (CDs), or any USB port devices such as memory sticks.
- Abstain from installing software that is not legally licensed for use (e.g. pirated software) and abstain from installing software that is not supplied or approved for use by the Division without administrator authorization.
- Be aware that electronic mail (e-mail) is not guaranteed to be private, nor is there such a thing as an anonymous sender.
- Note that messages relating to or in support of illegal activities may be reported to the authorities.
- Use the Internet in such a way that prevents any disruption of Internet use by other users (e.g. downloading huge files during prime time; sending mass e-mail messages).

Security

- Users who identify a security problem on the system must notify a system administrator. Users must not demonstrate the problem to other users.

Vandalism

- Vandalism is defined as any attempt to harm or destroy data of another user, or any connections that are part of the Internet. This includes, but is not limited to, any damage either physical or logical to hardware and/or software, or by uploading,

downloading or creating computer viruses. Vandalism can result in cancellation of privileges and the perpetrator will be referred for discipline.

Privacy

- Investigating or reading another user's files is considered the same as reading papers on someone's desk – a violation of their privacy. Reading unprotected files is rude; reading protected files, by whatever mechanism, is considered the same as "breaking and entering." Violations include:
 - Attempting to access another user's computer files without permission.
 - Supplying or attempting to supply false or misleading information or identification in order to access another user's account.
 - Deliberate, unauthorized attempting to access or use Sunrise School Division computers, computer facilities, networks, systems, programs or data.
 - Unauthorized manipulating of Sunrise School Division computer systems, programs or data.

Theft

- Theft includes the stealing of any property of Sunrise School Division by teachers, students, other staff, visitors or any other person or organization that uses Sunrise School Division facilities. Unauthorized use of Internet on-line time, whether billable or not, is also considered to be theft. Violations include:
 - Using subterfuge to avoid being charged for the use of computer resources
 - Deliberate, unauthorized using of another user's account to avoid being billed for computer use.
 - Abusing specific computer resources, or removing any computer equipment (hardware, software, data, etc.) without authorization.
 - Copying, or attempting to copy, data or software without proper authorization.

Harassment

- Harassment of other users may be the sending of unwanted messages or files. Violations include:
 - Interfering with the legitimate work of another user.
 - Sending abusive or obscene messages via computer.
 - Using computer resources to engage in abuse of computer personnel or other users.

Miscellaneous

- Transmission of any material in violation of any law or regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secrets. ICT use for commercial, advertisement, or political lobbying, or gambling is prohibited. Illegal activities are strictly prohibited. Other prohibited activities include:
 - Unauthorized and time-consuming recreational game playing.
 - Using computer accounts for work not authorized for that account.
 - Sending chain letters or unauthorized or unwanted mass mailings—"spamming".

- Using the computer for personal profit or other illegal purposes.
- Posting personal advertisements
- Pretending to be someone else in an e-mail message or chat room—"spoofing".

Consequences

Abuse or misuse of Sunrise School Division computing services may not only be a violation of this policy or user responsibility, but it may also violate the criminal code. Therefore, Sunrise School Division will take appropriate action in response to user abuse of ICT's. Action may include, but not necessarily be limited to:

- Suspending or revoking computing privileges
- Denying access to all computing facilities and systems
- Requiring reimbursement to Sunrise School Division, or the applicable Institution, of resources consumed
- Pursuing other legal action including action to recover damages; referral of computer users (faculty, staff and/or students, or authorized guests) for disciplinary action, or referral to law enforcement authorities.

School Websites

Practices

Educational Value:

- All use of ICT resources must have sound educational merit and/or support the Division guidelines, goals and policies.
- Published materials must not display, access, or link to sites deemed offensive according to Divisional policy.

Publishing Agreement:

- Only materials authorized by the sponsoring administrator will be published on Sunrise online servers.
- All publishers of material must have on file, at their site, an Online Publishing Agreement signature page.
- Student work may not be published on a web site unless both the student and the parent(s) or guardian(s) have signed the Online Publishing Agreement.

Privacy and Student Safety:

- At no time shall any student's personal information (full name, home address, e-mail address, or phone number) appear on Sunrise online published materials.
- All contact information should identify a webmaster or content sponsor.
- As a matter of practice, student pictures will not be published on divisional websites. On the rare occasion that they are (recognition for awards, etc.) written parental permission will be required.
- To assure student safety, full names will not be published. When student work is published, the first initial, last name can be provided.
- Permission must be obtained from any staff member prior to displaying his/her photograph or information.

Copyright Laws:

- Adhere to all copyright laws. Please pay particular attention to the copyright information in the Sunrise Online Publishing Guidelines (below).

Content Monitoring/Auditing:

- The sponsoring administrator should regularly "visit" online accessible content to monitor appropriateness, quality and educational value. All published content is ultimately her / his responsibility.

Sunrise School Division Administration and members of the ICT Team reserve the right to audit and/or adjust materials and/or activity on any Online Server publishing content sponsored by a Sunrise organization.

Responsibilities

For uniformity across the school division, the following terms will be used:

- WAN (Wide Area Network) Manager
- Administrator (school and division levels).
- School Webmaster (administrator, teacher or secretary).
- Content Contributors (staff and students).

Sunrise School Division WAN Manager

The WAN Manager will manage the Division Wide Area Network and Internet Server(s).

Responsibilities:

- establish Online Publishing guidelines and procedures;
- provide Online Publishing access for designated webmasters;
- ensure that all files are up-to-date;
- ensure the accuracy and appropriateness of all materials published so that they adhere to the division goals, guidelines and policies. (Refer to SUNRISE Online Publishing Guidelines).

Administrator

All Sunrise School Division Senior Managers, Principals, and Managers have responsibility for content information published by their organizations online.

Responsibilities:

- develop site-based publishing procedures; who does what and how?
- ensures content and materials meet Sunrise standards for quality and excellence before they go public;
- designates a site webmaster who manages procedures;
- annually, shares Divisional Online Procedures with staff;
- submits a site contacts and server locations of all their online accessible content to the Division WAN Coordinator;
- ensures site Webmasters, Content Sponsors and/or Content Contributors understand their procedures, and;
- ensures that all content fits the Division goals, guidelines and policies. (See SUNRISE Online Publishing Guidelines below.)

School Webmaster

A webmaster is the person responsible for publishing content on an Online Accessible Server. This could be any staff member. All content published by a webmaster shall follow Sunrise Online Publishing Guidelines.

Responsibilities:

- develop his / her organization's online procedures;
- ensure that all materials published have been approved by the organization administrator;
- ensure accuracy and appropriateness of all materials published;
- practice effective file management so only current materials are on the Wan / Internet Server;
- ensure all active materials on servers are backed up;
- ensure Content Sponsors and/or Content Contributors understand Division goals, guidelines and policies, and;
- ensure content adheres to the Division goals, guidelines and policies. (Refer to SUNRISE Online Publishing Guidelines).

Content Contributors

- Include individuals (staff, students, parents) who contribute content materials to an online accessible server.
- Staff is responsible for content prepared by their students and should ensure the accuracy and appropriateness of all of the materials they provide so that they adhere to the Division goals, guidelines and policies. (Refer to Sunrise Online Publishing Guidelines).
- All published content is ultimately the responsibility of the sponsoring administrator.