Scappoose School District
Acceptable use of District Computing Resources and Networks

Introduction

This document constitutes the Scappoose School District ("the District") policy for the management of computer networks, personal computers and the resources made available thereby. The policy reflects the ethical principles of the District community and indicates, in general, the privileges and responsibilities of those using District computing resources.

Acceptable Use

Institutional Purposes

District computing resources are to be used exclusively to advance the District's mission of education and public service. Faculty, staff and students may use them only for purposes related to their studies, their responsibilities for providing instruction, the discharge of their duties as employees, their official business with the District, and other District-sanctioned or authorized activities. The use of District computing resources for commercial purposes including any sort of solicitation is prohibited, absent prior written permission of the appropriate District official(s). Unauthorized commercial uses of District computing resources jeopardize the District's relationships with network service providers and computer equipment and software vendors.

The District acknowledges that occasionally faculty, staff and students use District computing resources assigned to them or to which they are granted access for non-commercial, personal use. Such occasional non-commercial uses are permitted by faculty, staff and students, if they are not excessive, do not interfere with the performance of any faculty, staff member or student's duties, do not interfere with the efficient operation of the District or its computing resources, and are not otherwise prohibited by this policy or any other District policy or directive. Decisions as to whether a particular use of computing resources conforms to this policy shall be made by the individual school principal or the Superintendent.

Impermissible Use

Computing resources may only be used for legal purposes and may not be used for any of the following purposes or any other purpose which is illegal, immoral, unethical, dishonest, damaging to the reputation of the District, inconsistent with the mission of the District, or likely to subject the District to liability. Impermissible uses (some of which may also constitute illegal uses) include, but are not limited to, the following:

- Harassment;
- Libel or slander;
- Fraud or misrepresentation;
- Destruction of or damage to equipment, software, or data belonging to the District or others;
- Disruption or unauthorized monitoring of electronic communications;
- Unauthorized copying or transmission of copyright-protected material;
- Use of the District's trademarks, logos, insignia, or copyrights without prior approval;
- Violation of computer system security;
- Unauthorized use of computer accounts, access codes (including passwords), or network identification numbers (including e-mail addresses) assigned to others;
- Use of computer communications facilities in ways that unnecessarily impede the computing activities of others (such as randomly initiating interactive electronic communications or e-mail exchanges, overuse of interactive network utilities and so forth);
- Development or use of unapproved mailing lists;
- Use of computing facilities for private business purposes unrelated to the mission of the District or to District life;
- Academic dishonesty;
- Academic Honor Code violations;
- Violation of software license agreements;
- Violation of network usage policies and regulations;

- Violation of privacy;
- Posting or sending obscene, pornographic, sexually explicit, or offensive material;
- Posting or sending material that is contrary to the mission or values of the District;
- Intentional or negligent distribution of computer viruses;
- Use of any network sniffer or tool designed to monitor or decode passwords, network traffic, or utilization;
- Participation in any chat rooms, except as specifically provided for by District policies; or
- All Internet access is subject to content filtering. Any attempt to bypass or disable filtration systems is expressly prohibited.

Cooperative use

Computing resource users can facilitate computing at the District in many ways. Collegiality demands the practice of cooperative computing. It requires:

- Regular deletion of unneeded files from one's accounts on shared computing resources;
- Refraining from overuse of connect time, information storage space, printing facilities, processing capacity, or network services;
- Refraining from use of sounds and visuals which might be disruptive or offensive to others;
- Refraining from use of any computing resource in an irresponsible manner; or
- Refraining from unauthorized use of departmental or individual computing resources.

General policies

Computer use has become an integral part of many District activities. While much computing occurs on individual computing resources, most information and communication systems reside on central computers and use networks. Distributed resources, such as computer clusters, provide additional computing tools. Access to these computing resources is contingent upon acceptance of the policies and procedures governing such use.

Responsibilities of Users

The user is responsible for correct and sufficient use of the tools available for maintaining the security of information stored on each computer system. The following precautions are strongly recommended:

- Computer accounts, password and other types of authorization that are assigned to individual users should not be shared with others.
- The user should assign an obscure account password and change it frequently.
- The user should understand the level of protection each computer system automatically applies to files and supplement it, if necessary, for sensitive or confidential information.
- The computer user should be aware of computer viruses and other destructive computer programs and take steps to avoid being a victim or unwitting distributor of these processes.
- Ultimate responsibility for resolution of problems related to the invasion of the user's privacy or loss of data rests with the user.
- The computer user should consider whether information distributed using District resources should be protected from unauthorized use by the use of copyright notices or by the restriction of distribution of certain materials to the District users.

Security

The District will assume that users are aware that electronic files are not necessarily secure.

Users of electronic mail systems should be aware that electronic mail in its present form is generally not secured and is extremely vulnerable to unauthorized access and modification. The Data System Specialist or NWRESD Technology technician will make available to interested persons information concerning reasonable methods for attempting to protect information on central computing resources from loss, tampering, unauthorized search, or other access. Levels of obtainable security will vary depending upon the system involved. Information on procedures appropriate to each resource will be available from the Data System Specialist.