ACCEPTABLE USE & SOCIAL MEDIA POLICY

Purpose: The purpose of this policy is to comply with the Weber State University Acceptable Use and Social Media policies.

Policy: WSU Charter Academy will use Weber State University PPM 10.2 as follows:

Acceptable Use Policy for Computing and Network Resources

No. 10-2	Rev. 12-14-10	Date: 10-11-05

I. PURPOSE

Weber State University provides students, faculty and staff with access to Information Technology (IT) Resources (as defined herein). Such access, used appropriately, legitimately advances the University's mission by supporting teaching, research, public service, and administrative activities. This Acceptable Use Policy, which reflects the University's mission, provides guidance for using IT Resources and protects the University, Users, and property.

II. REFERENCES

a. PPM 3-30, Personal Conduct
b. PPM 3-32, Discrimination and Harassment
c. PPM 3-33, Discipline
d. PPM 3-36, Conflict of Interest
e. PPM 5-41, Copyright Policy: Ownership
f. PPM 5-42, Copyright Policy: Copying of Copyrighted Works
g. PPM 5-43, Performance or Display of Copyrighted Works
h. PPM 6-22, Student Code
i. PPM 8-25, Reason for Dismissal of Tenured Faculty
j. PPM Section 9, Academic Freedom, Rights, Responsibilities and Due Process
k. PPM 10-1, Information Security Policy
l. PPM 10-4, Payment Card Handling Policy
m. R345, Information Technology Resource Security (Board of Regents Policy)
n. R343, Information Management (Board of Regents Policy)
o. PCI DSS

III. SCOPE

This Acceptable Use Policy applies to all Users of Weber State University's IT Resources whether affiliated with the University or not and to all use of these resources from on campus or in remote locations. Users accept personal responsibility for the appropriate use of IT Resources. Each year, Users will be required to review and accept the University's Acceptable Use Policy. Users accessing Weber State University IT Resources are responsible for maintaining a current understanding of the terms of this policy, which the University reserves the right to change without prior notice. The current version of this policy is available in the University's Policy and Procedures Manual. This policy also covers the use of all devices connected to the University IT Resources, whether owned by the University or private individuals.

While this policy deals specifically with issues involving the use of University IT Resources, it does not stand alone. All Users of University IT Resources are expected to abide by the rules and regulations contained in applicable University handbooks, the Student Code, guidelines and policy and procedure manuals, as well as the laws of the State of Utah and of the United States of America. We remind Users that state and federal laws apply to the use of campus networks and the Internet, including but not limited to those dealing with:

- copyright infringement
- defamation
- discrimination
- fraud
- harassment
- identity theft
- obscene materials
- records retention

IV. DEFINITIONS

A. IT Resources: Electronic processing, storage, and transmission systems, which include but are not limited to, the computers, terminals, printers, networks, modem banks, copy machines, fax machines, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by the University. IT Resources also include, but are not limited to, institutional and departmental information systems, faculty research systems, desktop computers, the University's campus network, and general access computer clusters.

B. Users: All faculty, staff, administrators, students, consultants, guests, and any person or agency employed or contracted by the University or any of its auxiliary organizations who have a legitimate need to access IT Resources.

C. Electronic Communication: Email, text-messaging, instant messaging, and social networks.

V. POLICY

A. General

1. IT Resources are the property of the University and shall be used only for legitimate University instructional, research, public service, administrative, and approved contract purposes, except as allowed in this policy. Additional policies may apply to IT Resources provided or operated by individual units of the University or to uses within specific units. Users are allowed to use IT Resources only to the extent authorized. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before using IT Resources. When demand for computing resources may exceed available capacity, priorities for their use will be established and enforced. Authorized faculty and staff may set and alter priorities for exclusively local computing/networking resources. Nothing in this policy guarantees that violations of this policy will not occur or imposes liability on the University for any damages resulting from such a violation.

B. Responsibilities of Users

1. Law and Policy

a. IT Resources must be used in compliance with applicable state and federal laws and University policies. IT Resources may not be used for any illegal purpose or activity or for any purpose which would violate University policy. Placing unlawful information or material on University systems is prohibited.
b. Downloading or disseminating copyrighted materials outside the provisions of "fair use" or without the permission of the copyright holder is prohibited. Illegally downloaded material may include, but is not limited to, music, movies, games, software, etc. Illegal use of peer-to-peer networking or other file-sharing technology is prohibited and may subject the User to civil or criminal penalties beyond penalties for violation of University policy. (See PPM 5-41, 5-42, 5-43 for the reference to copyright policy as well as IT Compliance Plan.)
c. Accessing or attempting to access computer systems through using IT Resources, including those external to the University, without authorization by the owner of that system, is specifically prohibited.
d. Sending electronic communication messages or creating web pages with fraudulent address or header information or containing misrepresentations in authorship or content in an attempt to deceive others is prohibited.
e. Using the University's official web site or email for partisan political purposes (with the exception of announcements of general public interest by university political clubs) is prohibited.
f. Using IT Resources in a way which would constitute a regular private business activity or which would violate the University's conflict of interest policies is prohibited.
g. Deliberately misusing trademarks in web pages and email, including University-owned marks such as the official logo or seal and trademarks owned by other entities is prohibited.
h. Providing false or misleading information in order to obtain access to computing or network facilities is specifically prohibited.

2. Accounts and Passwords

a. Users are responsible for any activity originating from their accounts which they can reasonably be expected to control.
b. Users may not divulge or make known their own password(s) to another person.
c. Unauthorized use of another User's account is prohibited.
d. Users who know another User's password, intentionally or unintentionally, must notify the account owner immediately.
e. Falsifying or corrupting data in others' accounts or in public directories is prohibited.
f. Falsifying identity while using e-mail or any other IT Resource is prohibited.

3. Respect for IT Resources, Users, and Information

    a. Users must respect the ability of other Users to utilize IT Resources in an efficient and secure manner. Use of IT Resources shall not disrupt, distract from or interfere with the conduct of University business (for example, due to nature, volume, or frequency).
    b. Using any device or software which interferes with the ability of others to access IT Resources is prohibited.
    c. Damaging or attempting to damage any portion of IT Resources is prohibited.
    d. Deliberately introducing computer viruses, worms, or similar technologies which would harm the integrity of IT Resources, as well as attempting to create or disseminate such technologies, is prohibited.
    e. Deliberately misusing of software or other techniques to degrade system or network performance or otherwise deprive authorized personnel of resources or access to University systems or networks, including techniques to disguise or obscure the source of data network traffic, is prohibited.
    f. Using IT Resources to release confidential, proprietary information, or information which has been classified as private, controlled, or protected under Utah Code Ann. § 63G-3-201 et seq, without appropriate authorization is prohibited. Refer to the Payment Card Handling Policy (PPM 10-4).
    g. Sending unsolicited bulk electronic communication (spam) unrelated to the University's mission or related bulk email without appropriate approval is prohibited.
    h. The privacy and rights of others must be respected. Monitoring or attempting to monitor another User's communications outside the scope of one's duties is specifically prohibited.

4. Incidental and Occasional Personal Use

    a. Users may engage in incidental and occasional personal use of University IT Resources provided that such use does not:

    - Violate applicable law, rules and policies;
    - Disrupt, distract from, or interfere with the conduct of University business (for example, due to nature, volume or frequency);
    - Involve regular private business activities; or
    - Contravene supervisor direction regarding personal use of University IT Resources.

C. Privacy

Providing and allowing access to University IT Resources to Users does not imply a guarantee of privacy. These systems can sometimes be breached by someone determined to do so. Also, there are some circumstances in which use of IT Resources may be monitored and in which records and information contained in electronic communications or other electronic formats may be viewed and/or copied by the University or other authorized officials. See Section E for further information. Users are encouraged to take appropriate precautions in use of IT Resources.

D. Remote Access

1. Remote access to the University Critical IT Resources or business systems requires the use of a VPN.
2. All Users must be authenticated to gain remote access into the University's network with at least a username and password.
3. Two-factor authentication is required for remote access to the cardholder data environment. Refer to the Information Security Policy (PPM 10-1).
    a. Accessing cardholder data via remote-access technologies, to copy, move, and store cardholder data onto local hard drives and removable electronic media is strictly prohibited.
    b. The remote-access end points must always be firewalled from the internal network and the VPN traffic subject to firewall rule sets.
    c. Split tunneling must be disabled.
    d. The remote-access session must be disconnected after 30 minutes of inactivity.
    e. Remote-access technologies for vendors must be activated only when needed by vendors, with immediate deactivation after use.

E. University Actions

1. The University reserves the right to take appropriate actions reasonably necessary to protect the integrity and security of University computing facilities and data networks. This includes the right to log and monitor network traffic and immediately disconnect any computer disrupting the University's data network; or being used for any activity in violation of this policy or other University policy or state and federal law. Users should be aware that logs are generated by the various IT Resources used on campus, including electronic communication and web access and network flows. Electronic information on University networks or equipment, including but not limited to electronic communication, is subject to review, monitor, copy, examination, and disclosure by the University as appropriate for legal, audit, or legitimate operational or management purposes. This includes, but is not limited to, the following:

    a. It is necessary to maintain or improve the functioning of University computing resources;
    b. There is reasonable cause for suspicion of misconduct under University policies or violation of state or federal laws;
    c. It is necessary to comply with or verify compliance with federal or state law, including but not limited to software licensing agreements;
    d. The requirements of maintaining a safe and secure network dictate the deployment of automatic security systems, such as host and network intrusion detection systems, and active protection firewall systems designed to intercept, examine, and block data that threatens the University or external networks;
    e. The University receives requests for information under state records law (Government Records Access and Management Act);
    f. The University receives subpoenas or other court orders requiring disclosure of information; and
    g. The University has notice of litigation or potential litigation.

2. The use of University IT Resources is a privilege that may be revoked at any time.

3. Violation of this policy may result in discipline, up to and including termination or expulsion, in accordance with Weber State University policies. Legal action may also be taken when warranted. Violation of applicable laws may result in civil or criminal penalties.
4. The system administrator has the right to delete any file(s) belonging to faculty or staff who are no longer employed by the organization.
5. The University makes no warranties of any kind, whether express or implied, with respect to the information technology services it provides; this includes but is not limited to the accuracy or quality of information obtained through its electronic communication facilities and services.
6. The University will not be responsible for damages resulting from the use or misuse of University computing and data network facilities and services, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, hacking, or service interruptions caused by the negligence of an organization employee or by the User's error or omissions.