Policy Type: Information Technology
Policy Title: Employee Acceptable Use of Technology and Data Policy
Policy Number: IT-02

Purpose:
This policy governs the use of all technology and computer resources at Green River Community College including college computers, smart devices, college email, internet access and use of the college network by either college owned or personal equipment. Use of the college’s technology and computer resources signifies agreement to abide by this policy.

Scope:
All staff, faculty, administrators and students at Green River Community College.

Definition:
- College Technology Resources: any technology and computer resources owned by the college or by the employee.
- College Data: any email, electronic document, hardcopy document, facsimiles or voice mails stored on college technology resources.

Policy or Procedure:
1. Risk Statement
   The improper or illegal use of college technology resources may result in serious risk and liability to both the college and the individual employee. These risks include but are not limited to:
   - Violation of state law
   - Loss of public trust in the college
   - Interference with performance and services provided by the college
   - Loss of network or operational integrity
   - Financial loss
   - Personal and college liability

   All college employees are reminded that all college data, including email, are considered public records and may be subject to disclosure under the public disclosure laws.
2. Business and Limited Personal Use

College technology resources are provided to employees as a productivity tool for conducting college business and to perform their official duties. Employees may occasionally on a limited basis use college technology for purposes other than the conduct of official duties provided that the use conforms to the De Minimis Use of State Resources by State Employees (RCW 42.52.160 and WAC 292-110-010).

The permitted uses for a purpose other than the conduct of official duties must meet all of the following:

- Results in little or no cost to the college
- Is infrequent, and brief in duration
- Is the most effective use of time and resources
- Does not interfere with the performance of official duties
- Does not disrupt other state employees
- Does not obligate other state employees to make a personal use of college resources, and
- Does not compromise the security or integrity of college property, information or software

3. Prohibited Use

In the course of using college technology resources for either business or limited personal use, employees are prohibited from:

- Any activity that violates any college policy or city, state, or federal law, including hate speech, copyright violations, gambling, any malicious, threatening, or obscene matters.
- Discriminating against or harassing another person.
- Supporting, promoting or soliciting for an outside organization unless authorized by the college and permissible by law.
- Using college technology resources to gain unauthorized access to any computer, files, data, systems, or networks.
- Unauthorized access of college computer’s hard drives or college network drives. This includes, but is not limited to: accessing; downloading to; or modifying any network drives or the hard drive on any school computer; whether or not security is in place. Shared classroom/instructional drives are for school-related files only; personal files are not permitted.
- Unauthorized use of technology for the purpose of private or personal business. Computers may not be used for commercial purposes.
- Misrepresenting or forging the identity of the sender or the source of an electronic communication.
• Any activity which interferes with the work of others, including but not limited to, excessive printing; creation or propagation of computer viruses or other self-replicating or destructive programs; posting, mailing, or printing of obscene materials; or distributing unsolicited advertisements.

4. No Expectation of Privacy
The college has the right to access, inspect or monitor any college data, inclusive of electronic records. Employees cannot expect privacy in their use of college technology resources whether that use occurs in the conduct of official duties or is a use made for a purpose other than the conduct of official duties. While the college does not regularly monitor college data, employees are on notice that:
• The maintenance and operation of college technology resources may result in the observation of college data.
• Authorized college officers: President; Vice President of Human Resources; or designees may observe college data.

5. Reporting Misuse
Employees who discover misuse of college technology resources shall report such misuse to their supervisors. Retaliation on the basis of such a report will not be tolerated by the college.

6. Controlling Access to College Data
Employees are responsible for protecting college data from unauthorized access by securing communications devices and locking and securing hardcopy documents. Employees should not provide others access to their accounts by sharing passwords or leave their workstations unattended without securing the workstation.

7. College Data Retention
College data are public records. College data that contain information about college business and that can function as evidence of business transactions are part of the records of the college, and are subject to the guidelines in the Public Records Act, Chapter 40.14 RCW, which regulates the preservation and destruction of public records. College data should be kept for the retention period identified by the General Retention Schedule for the Washington Association of Community and Technical College System. In addition, there may be reasons to retain these records longer for ongoing operations, audits, legal proceedings, research or other known purpose. Managers and supervisors are responsible for providing retention guidelines and training to their staff. For more information on records retention matters, please consult the college records retention officer.
8. Public Records Disclosure

The intent of the Public Records Act is to provide public access to records and protect public records from damage or destruction. The college is required to make available for public inspection and copying all public records, unless the record falls within the specific exemptions of the Revised Code of Washington or other statute that exempts or prohibits disclosure of specific information or records. When a public records request is received, it should be forwarded to the College Relations office.

9. Violation Warning

Violations of this policy may result in disciplinary action up to and including dismissal and legal action. In addition, there may also be separate actions against the employee for violation of the state’s ethics law, criminal prosecution, and civil actions.

Specific Authority:

Use of persons, money, or property for private gain (RCW 42.52.160)
Use of State Resources (WAC 292-110-010)
General Retention Schedule for the Washington Association of Community and Technical College System (RCW 40.14)

Law Implemented:

WAC 292-110-010
RCW 40.14
RCW 42.52

History of Policy or Procedure

Draft: November 2, 2010
Adopted: December 1, 2010
Revised: April 24, 2013
Reviewed by: Camella Morgan, Executive Director of Information Technology
Contact: Camella Morgan, Executive Director of Information Technology
President’s Staff Sponsor: Camella Morgan, Executive Director of Information Technology