# ADMINISTRATIVE REGULATION 3720

**COLLEGE OF THE REDWOODS**

## INFORMATION SECURITY-ACCEPTABLE USE

### 1. Purpose and Scope

The objective of this administrative regulation is to outline the acceptable use of electronic assets at **COLLEGE OF THE REDWOODS**. Inappropriate use exposes the district to risks including compromise of network systems and services, human resources or legal issues.

This is one of a series of information security Administrative Regulations maintained by the Information Technology (IT) department designed to protect the district information systems.

#### 1.1 Applicability of Assets

The scope of this Administrative Regulation includes all electronic assets that are owned or leased by the district*,* regardless of funding source. Assets may include but are not limited to:

* Desktop and Laptop Computers
* Servers
* Network Infrastructure
* Mobile Computing Devices
* Electronic Media
* Non-electronic media (paper and other)

#### 1.2 Applicability to All Employees and Volunteers

This Administrative Regulation applies to all Board of Trustees, authorized/ratified full-time and part-time regular Academic and Classified employees, Substitutes, Short-term (Temporary) staff, Professional Experts, College Work Study students, Student Help and Volunteers who are employed at the college for the purpose of meeting the needs of students.

#### 1.3 Applicability to External Parties

This Administrative Regulation applies to all external parties, including but not limited to the district business partners, vendors, suppliers, outsource service providers, and other third party entities with access to the district networks and system resources.

#### 1.4 References and Related Documents

Please refer to the following Administrative Regulations for additional information and references including definitions:

* AR 3720: Acceptable Use
* AR 3721: Change Control
* AR 3722: Disaster Recovery
* AR 3723: Network Security
* AR 3724: Secure Operations
* AR 3725: Security Incident Response
* AR 3726: Data Classification
* AR 3727: Physical Security
* AR 3728: Logging and Monitoring
* AR 3729: Remote Access

### 2. Acceptable Use

#### 2.1 Acknowledgement of User Responsibilities

All users must review and acknowledge their understanding of the district Acceptable Use Administrative Regulation and other job appropriate information security Administrative Regulations on an annual basis. Human Resources (HR) will provide the Administrative Regulation and acknowledgement links to new staff and contractors upon hire or contract establishment.

#### 2.2 Personal Use

Computers and computer accounts given to users are provided to assist district employees and volunteers in the performance of their jobs. All computer systems belong to the district and are intended for business and instructional use. Users are expected to exercise good judgment regarding the reasonableness of personal use of the district information systems and assets. Personal use should not conflict in any way with business objectives or interests, organizational values, or standards of business conduct. The district reserves the right to limit or prohibit the use of any software not licensed or approved by district IT. If unlicensed software is found to reside on a district computer, it mustbe removed. If unapproved software is found, it may be removed by IT personnel*.*

The district considers all information transmitted through or stored in its business system, including e-mail, instant messaging (IM) or chat data, and voice mail messages, as district business information. All files and other business information stored on district systems, even if considered “personal” by an employee, are and remain the property of the district. The district may review or use such business information as it deems appropriate.

Where allowed by law, the district IT department reserves the right to monitor activities that occur on its systems in order to troubleshoot system problems, disruptions or outages. For this reason, users should not have an expectation of privacy for anything they store, create, send, or receive on a district system. Suspected inappropriate use of systems by individuals may also be investigated in order to protect the organization.

#### 2.3 Confidentiality

**COLLEGE OF THE REDWOODS** has implemented a Data Classification Administrative Regulation 3726 which categorizes different types of information and how it will be protected based on its value and sensitivity. Sensitive, personally identifiable, and customer information are classified as *Restricted*, and must be kept confidential at all times. This information is accessible only to those district staff who need such access in order to perform their jobs, or to others who have been expressly authorized by the district for specific limited purposes. Unauthorized disclosure of information that has been classified as *Restricted* could cause great harm to the district, and may be protected by law.

*Restricted information* must be protected from disclosure to third parties (non-employees) by default. Third parties may be given access to district information only when a demonstrable need-to-know exists. Such disclosure may be authorized by district management or by contract, such as with a temporary worker, consultant, or service provider. A non-disclosure agreement may be required as directed by the relationship and district legal requirements.

*Restricted* information may be stored in designated locations only andmust be securely deleted when it is no longer required. If stored online, on portable devices or on tape, *Restricted* information requires encryption so that it cannot be read by unauthorized persons. *Restricted* information that is on paper or other media must also be stored securely. Refer to the Data Classification Handling Procedures for additional information on this topic.

Specific information about the district’s computer network, information system security, security controls, or potential vulnerabilities may not be distributed to persons who do not have a demonstrable need-to-know, and without prior approval from the district administration and district IT management.

All information systems assets provided by the district remain the sole property of the district. Any data or intellectual property created by the user, including voicemail and electronic messages, remain the property of the district and should not be removed, copied or shared with any person or entity except as part of the user’s normal job responsibilities.

#### 2.4 Electronic Messaging

**COLLEGE OF THE REDWOODS** has an electronic mail (e-mail) network and provides instant messaging (IM) services. Users are responsible for using these technologies responsibly and within the following policies:

* The district e-mail system is not to be used to solicit for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations.
* Sending unsolicited e-mail messages is prohibited, including the sending of junk mail or other advertising material to individuals who did not specifically request such material.
* Creating or forwarding chain letters or pyramid schemes of any type is prohibited.

* Users must not create any messages that may be considered offensive or disruptive. Examples of messages deemed to be offensive are any which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
* District business communications transmitted by e-mail must use the appropriate district or college e-mail address (@redwoods.edu) and employ the standard e-mail signature for external communications. Falsifying e-mail headers or routing information so as to obscure the origins of the e-mail or identity of the sender is a violation of this Administrative Regulation.
* Because e-mail records and computer files may be subject to discovery in litigation, users must avoid making statements in e-mail that would not reflect favorably on the district if disclosed in litigation or otherwise. Delete unnecessary e-mail promptly.
* Unauthorized access to others’ e-mail accounts is prohibited.
* Information classified as *Restricted* (sensitive, personally identifiable, or student information) must not be e-mailed over **public** networks or stored on portable devices without encryption. Refer to the Data Classification Administrative Regulation 3726 for additional information.
* Caution must be used when opening e-mail attachments or following hypertext links received from unknown senders, which may contain malware or viral code.

#### 2.5 Social Networking Technologies

Social networking tools (blogs, online social networks, Facebook, Twitter, etc.) provide an open exchange of information and a means to establish relationships with colleagues and members of the public. These tools represent a communication model where a fine line exists between business and personal statements. Employees who choose to participate in social networking technologies must know and follow the district’s guidelines.

The district’s or another person or company's confidential or proprietary information is not to be shared. Users must ask permission to publish or report on conversations that may have intended to be private or internal to the district. Check with the appropriate PIO or the Legal department if you have any questions about what is appropriate to publish or say online.

#### 2.6 Use of COLLEGE OF THE REDWOODS Assets

Using district electronic assets for abusive, unethical, or inappropriate purposes will not be tolerated and may be considered grounds for disciplinary action, including termination of employment. Unacceptable use of electronic assets includes, but is not limited to:

* Illegal activities
* Revealing or publicizing district intellectual property or proprietary information for unapproved or non-business-related reasons
* Use or distribution of unlicensed software
* Unauthorized use of copyrighted materials
* Sharing of user names and/or passwords
* Leaving *Restricted* or any confidential or sensitive materials in plain sight without taking protective measures
* Transferring or storing information on untrusted third party servers. Contact IT for approved locations / services.
* Presenting your own viewpoints or positions as those of the district, or attributing them to the district
* Effecting security breaches or disruptions of network communications
* Circumventing user authentication or security of any computer, network or account
* Facilitation of the compromise of district information security controls
* Disabling software designed to prevent viruses or malware, or disabling screen savers or encryption methods
* Providing information about, or lists or organizational charts of district employees to external parties.

### 3.0 Enforcement

Those detecting violations of this Administrative Regulation must report the violation to their direct manager immediately, who will verify the nature of the violation and report it to District IT or Local College IT and/or Human Resources as appropriate. District management will determine the extent of risk that any non-compliance condition presents and remediation activities that are required.

Users who deliberately violate information security Administrative Regulations will be subject to disciplinary action up to and including termination from employment or association with the district.