

# **Acceptable Use Policy of Information Technology Resources at The University of Findlay**

This policy document is divided into five major sections:

- I. Guiding Principles** - provides background and relates the Policy to the University mission
- II. Acceptable Use Policy** - is the statement of the Policy itself
- III. Procedures** - provide specific detail for implementing the Policy
- IV. Policy on Faculty Access to Student Computer Files** - provides guidelines used to determine appropriate faculty access to student computer files
- V. OARnet Acceptable Use Policy** - provides guidelines for network use by the Ohio Academic Resources Network

## **Definitions of Terms Used in this Document**

*Information Technology (IT):* Any computer, telephony equipment, network equipment, peripheral, storage device or data file.

*Community:* Any UF employee, student or authorized guest.

*User:* Any person using any IT equipment or service, either locally or remotely.

## **I. Guiding Principles**

### **A. What The University of Findlay Provides and Why**

The University of Findlay provides access to a broad range of computing and network resources to members of the university community. These IT resources are in support of its mission to continuously improve student understanding and capabilities that lead to meaningful lives and productive careers. These resources are intended for university-related purposes, including direct and indirect support of the university's instructional, research and service missions; university administrative functions; student and campus life activities; and the free exchange of ideas among members of the UF community and between the community and the wider local, national and global communities.

### **B. Rights, Privileges, and Responsibilities Associated with Campus Network and Computing Resources**

The rights of academic freedom and freedom of expression apply to the use of university network resources. This philosophy is based on the belief that information has its greatest value when shared appropriately. Used appropriately, computing and network resources maintain and enhance the university's mission; used inappropriately, computing and network services can be used to break laws or infringe on the rights and beliefs of others. Thus, the rights of access to The University of Findlay's network resources are balanced by the responsibilities and limitations associated with those rights.

The privilege of access to The University of Findlay's network resources is conditioned on acceptance of the responsibilities and limitations associated with the Acceptable Use Policy. Users are bound by the terms of this policy whenever they utilize computing or network resources of The University of Findlay.

The use of UF's network resources, like the use of any other university-provided resource and like any other university-related activity, is subject to university policies and all requirements of legal and ethical behavior within the UF community. Thus, conduct that is illegal or inappropriate in the physical world or a violation of university policy is illegal, inappropriate, or a violation when conducted online. Uses of computers or network resources are not necessarily legitimate just because they are technically possible.

### **C. Applicability**

This policy applies to all users of UF's computing and network resources, whether affiliated with the university or not, whether the use or access itself is authorized or unauthorized, and to all uses of those resources, whether on campus or from remote locations, including those conducted over wireless networks.

## **II. Acceptable Use Policy**

**A. All users of The University of Findlay's computing and network resources must comply with the following statements:**

### **1. Compliance with Law and University Policies**

Users must comply with all federal, state, and other applicable laws; all generally applicable university rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; the university's policy handbooks; the university's sexual harassment and non-discrimination policies; and all applicable software license. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

## **2. Authorizations**

Users must access only those computing resources they are authorized to use and use them only in the manner and to the extent authorized. This provision applies to digital, printed or written data. Ability to access computing resources does not, by itself, imply authorization to do so. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned. Users who share access to accounts with third parties will be held liable for consequences caused by the third parties' use of their accounts.

## **3. Privacy**

Users must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Again, ability to access another person's account does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and obtaining them before proceeding.

## **4. Consumption of Resources**

Access to University computing and network resources is granted for purposes consistent with The University of Findlay's mission and for limited personal use. Use of IT resources for personal or recreational activities may be limited depending on the capacity of computing and network resources. Users must limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. UF may require users of the resources to limit or refrain from uses of specific resources in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

## **5. Non-commercial uses only**

Users must refrain from using computing and network resources for personal commercial purposes. Personal use of university computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other university responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

## **B. Enforcement and Sanctions**

Users who violate this Policy may be denied access to The University of Findlay's computing and network resources and may be subject to other penalties and disciplinary action, both within and outside of the university.

Violations will normally be handled through the university disciplinary procedures applicable to the relevant user. For example, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed, by the Office of Student Affairs. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

The University may temporarily suspend or block access to an account prior to the initiation or completion of such procedures when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of university or other computing resources, or to protect the university from liability. Under carefully arranged circumstances, UF reserves the right to limit access to network resources and to access data stored on university owned systems in order to ensure the stability and availability of network resources for the common good of the university community.

### **C. Security and Privacy**

The University of Findlay employs various measures to protect the security of its computing and network resources and of their users' accounts. Users must be aware, however, that the university cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

Users must also be aware that their uses of UF's network resources cannot be considered completely private. The normal operation and maintenance of the university's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service.

The university may specifically monitor the activity and accounts of individual users of university computing and network resources, including individual login sessions, content and communications, without notice, when

- (a) the user has voluntarily made them accessible to the public, as by posting to a web page, public file sharing application, etc.;
- (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of university or other computing resources or to protect the university from liability;
- (c) there is reasonable cause to believe that the user has violated, or is violating, this Policy or another written university policy;
- (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or
- (e) it is otherwise required or permitted by law.

Any such individual monitoring of content or communications, other than specified in "a", required by law, or necessary to respond to perceived emergency situations, must be authorized in advance in writing or email by a member of the UF senior staff or their designee.

The university, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate university personnel or law enforcement agencies under the direction of a court of law and may use those results in appropriate university disciplinary proceedings.

### **III. Procedures**

#### **A. Reporting Suspected Violations of the Acceptable Use Policy**

If a potential violation occurs in a UF classroom or lab, violations should be reported to the faculty or staff monitoring the facility, or to the Information Technology Officer. If a potential violation occurs in a non-instructional area, the situation should be reported to the supervisor of the area. Alternatively, complaints may be filed with the Office of Security or the Office of Student Affairs.

Where appropriate, whoever is notified first shall review the activities and, if merited, notify the user that they are in violation of this Policy and request that they take immediate remedial action to bring their conduct into compliance. The violation should then be immediately reported to the Information Technology Officer so damage to data or system integrity may be assessed. University's IT personnel may take immediate action, as needed, to abate ongoing interference with network and system operations, or to insure system integrity.

The details of all reports, including the identity of the complainant, will be handled in the strictest of confidence. Anonymous reports may be investigated but are not likely to result in judicial action or resolution.

#### **B. Procedures For Gathering and Reporting Evidence**

Any office receiving a complaint about a suspected violation of the Acceptable Use Policy will report this to the Information Technology Officer in writing or email. The Information Technology Officer will ensure that the report is forwarded to the most appropriate IT staff member for initial investigation.

Authorizations are required before specific evidence can be gathered about an individual's activity unless required by law or necessary to respond to a perceived emergency situation. Authorization for monitoring an individual's use of resources or the gathering of evidence from an individual's assigned account, network storage space or a University-owned computer must be granted by the appropriate authority. In the case of student accounts, authorizations come from the Vice President for Student Affairs or his/her designee. In the case of members of the faculty, authorizations come from the Vice President of Academic Affairs or his/her designee. In all other cases, authorizations come from the Director of Human Resources or the Vice President of Finance. Authorizations must be specific and delivered in writing or by email to the Information Technology Officer before any evidence is gathered from an individual's accounts.

### **C. Negligent Computer Use**

It is a violation of the Acceptable Use Policy for anyone to continue to operate any computer on The University of Findlay network that is known to propagate any potentially disruptive software code. Ignorance of technical methods to update, patch or disinfect a computer is not justification for continued use. It is the responsibility of the computer user to take all reasonable steps to ensure that any vulnerable or infected computer on the network is restored to proper operating condition.

### **IV. Policy on Faculty Access to Student Computer Files**

Faculty members may have access to a student file if the student specifically requests their assistance and grants access to the file. Faculty members may also have access to academic course-related files created by a student only if all of the following conditions are met:

1. The file or files are related to the course requirements of the particular course taught by the faculty member, and the student is registered for that course;
2. The faculty member announces, in advance of the access, when that access to the files meeting Condition 1 will occur;
3. The student specifically grants permission and access to the faculty member for those files that meet Condition 1 with the student understanding that not granting permission and access to the files to be reviewed could have an impact on his/her grades;
4. The faculty member will only access programming or programming-related files meeting the above conditions for the purpose of grading or monitoring the student's progress in the course, testing course work software to ensure it functions properly or assist in determining why it malfunctions and maintaining a dialogue with the student relative to the student's progress in the course.

Access to student files created by students at any correctional facility must be done within the confines of each institution and may be limited or changed after mutual agreement has been reached by the Information Technology Officer, the Vice President of Academics and the Director of Correctional Education Programs.

### **V. OARnet Acceptable Use Policy**

The University of Findlay is connected to state, national, and international resources through the Ohio Academic Resources Network (OARnet). OARnet provides access to these resources to its clients through connections with networks outside OARnet. In general, it is the responsibility of those networks to enforce their own acceptable use policies. OARnet will inform its clients of any restrictions on use of networks to which it is directly connected. OARnet accepts no responsibility for traffic which it originates which violates the acceptable use policy of any directly or indirectly connected networks

beyond informing the client that they are in violation if the connected network so informs OARnet.

**Specific Policies of OARnet:**

1. Use of OARnet must be consistent with the goals of facilitating and disseminating knowledge, encouraging collaborative projects and resource sharing, aiding technology transfer to Ohio businesses, fostering innovation and competitiveness within Ohio and building broader infrastructure in support of education and research.
2. It is not acceptable to use OARnet for illegal purposes.
3. It is not acceptable to use OARnet to transmit threatening, obscene or harassing materials.
4. It is not acceptable to resell OARnet provided services.
5. It is not acceptable to use OARnet so as to interfere with or disrupt network users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms or viruses and using the network to make unauthorized entry to any other machine accessible via the network.
6. It is assumed that information and resources available via OARnet are private to those individuals and organizations which own or hold rights to those resources and information and unless specifically stated otherwise by the owners or holders of the rights. It is therefore not acceptable for an individual to use OARnet to access information or resources unless permission to do so has been granted by the owners or holders of rights to those resources and information.
7. OARnet will review violations of its Acceptable User Policy on a case-by-case basis. Clear violations which are not promptly remedied by the client organization may result in termination of OARnet network services.

Please click on yes if you agree with the above agreement