University of Wisconsin – Whitewater CyberGirlz Camp Computer Acceptable Use Policy

Please read the following excerpts from the UW-Whitewater Acceptable Use Policy and indicate your agreement to the policy by signing at the end of the document.

Appropriate Use

Listed below are the policies that govern data network access and usage for students, staff and faculty at the University of Wisconsin Whitewater.

1. Authorized users

Authorized users are (1) current faculty, staff, and students of the University; (2) individuals connecting to a public information service supported on the Campus network and (3) others who are specifically authorized to use a particular computing or network resource by the campus unit responsible for the resource.

2. General Guidelines

Those who use the campus network resources are expected to do so responsibly, that is, to comply with state and federal laws, with this and other policies and procedures of the University, and with normal standards of professional and personal courtesy and conduct.

3. Security

Information security at UW-Whitewater is everyone's responsibility. To maintain security in using the campus network services, it is important to adhere to the following guidelines:

Protect your login ID and password. Computer accounts, passwords, ids and other types of authorization are assigned to individual users and should not be shared with others.
Be aware that the person to whom an account is assigned will be held accountable for any activity originating from that account.
Do not access data or systems for which you have not been given specific authority.
Take reasonable steps to ensure that your desktop or laptop computer system does not create a security risk when connected to the network, including keeping anti-virus software and operating patches up-to-date.
Report security violations.

4. Confidentiality

Information stored on computers is considered confidential, whether protected by the computer system or not, unless the owner intentionally makes that information available to other groups or individuals. The University of Wisconsin Whitewater takes the position that computer users desire that the information that they store on central and/or campus shared computing resources remain confidential.

While all efforts will be made to ensure confidentiality, users should be aware that data (including e-mail) might, due to software or hardware failure, become accessible to those who are not explicitly authorized for that access. iCIT personnel may also on occasion have access to such data while performing routine

operations or pursuing apparent systems or user problems. No guarantee of complete privacy is made or implied by this policy.

Requests for the disclosure of confidential information will be governed by the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA) and the Wisconsin Open Records Statutes (Chapter 19, ss. 19.31 - 19.39, Laws of 1992). All such requests will be honored only when approved by University officials who are the legal custodians of the information requested, or when required by state or federal law, or court order. Users found to be copying, modifying, or otherwise accessing information for which they have not been granted permission may be liable to disciplinary action.

Unacceptable Use

Network resources at UW-Whitewater may not be used for unlawful activities, commercial purposes not associated with the University, or uses that violate other University policies or guidelines. The following activities are NOT acceptable use of the campus network resources:

- Damaging or performing unauthorized removal of networking equipment, software or data
- Tampering with network hardware, wiring, or software
- Disrupting or interfering with the normal operation of network communications, generating excessive network activity or performing unauthorized monitoring of network traffic
- Willfully introducing computer viruses or other disruptive programs into the university network, which are intended to damage or create excessive load on network resources
- Intentionally violating or attempting to bypass network security strategies
- Using unauthorized accounts, passwords, IP addresses or other network access information
- Accessing or modifying any software, files, data or other university information for which an individual has not been given authorization
- Using network resources to harass or intimidate others
- Using network resources to impersonate others or to forge another's identity
- Interfering with the computing activities of others.
- Setting up network services or equipment without knowledge or involvement of iCIT.
- Violating state, federal or copyright laws
- Using network resources for commercial activity or financial gain which does not conform to UW-W rules and regulations.

I have read the above policy and agree to abide by the terms listed.

_____ _____

Student Date

_____ _____

Parent/Guardian Date