



## WASHINGTON COLLEGE POLICIES

### **USE POLICY FOR WASHINGTON COLLEGE INFORMATION TECHNOLOGIES RESOURCES**

Washington College (“the College”) provides computing facilities, an environment that encourages the sharing of information and access to local, national, and international information. The College provides its network, computing facilities, information databases, and Campus-wide information system in support of its academic mission and its administrative functions.

Within this document Washington College Information Technologies Resources (“WC IT Resources”) include, but are not limited to: all computer systems and software, interconnecting communications lines and hardware that are the property of Washington College, hardware that is privately owned when it is connected to the WC voice and/or data networks, all Internet Protocol (IP) addresses that are in the Washington College domain, the server computers and network systems, and voice and data networks provided by the College. Also included are the hardware and software associated with these systems and the information managed by these systems.

Approved uses of the WC IT Resources include, but are not limited to, educational applications, authorized electronic communications, administrative information exchange, presentation and promotion of the College to external audiences, research, faculty/staff professional development, and College-sponsored community outreach.

The following guidelines apply to ALL users of the WC IT Resources, including ALL of the Web and information servers operating on the Washington College Network. Infractions of these guidelines are to be reported to the Chief Information Officer for investigation and referral to the appropriate officers of the College. If one feels threatened, for example, by someone stalking or harassing by email or other technological means, immediately contact Public Safety.

#### **User Guidelines and Policies**

Use of WC IT Resources is a privilege, not a right. The WC IT Resources may not be used in any manner prohibited by federal, state, or local law or disallowed by licenses, contracts or College regulations, including (but not limited to) general College policies contained in the Faculty Handbook, the Student Handbook, and the Staff Manual.

Legitimate use of WC IT Resources is limited to those persons who have all of the following: proper authorization, a NetworkID (NetID), and a valid password to use the resources. Authorization to use any WC IT Resource is granted by the owner of the particular resource. Use of WC IT Resources is further limited by restrictions set forth in College policy. Legitimate use does not extend to whatever an individual is capable of doing with a College IT resource. Although some rules are built into the system itself, those restrictions cannot limit completely what an individual can do or can see. In any event, each member of the community is responsible for his/her actions whether or not specific rules are built in, and whether or not the rules can be circumvented.

Academic or administrative use of WC IT Resources always takes precedence over recreational and non-institutional use.

Washington College email is the property of the college. There should be no expectation of complete email privacy. Administrators will have access to an email account in the event of a legal subpoena, if an employee is terminated for cause, or for investigations of misconduct. Supervisors may request access, from the CIO or designee, to an employee's email if the employee is on an extended absence as determined by Human Resources. For confidentiality and personal privacy reasons personal email should be conducted on an outside account, such as Gmail, Hotmail at Live.com, or any of the many other free email services.

Members of the College community, as defined in the College's email policy, are expected to follow certain principles of behavior in making use of WC IT Resources. In particular they are to respect and to observe policies and procedures governing the Resources.

College community members must respect the privacy of, or other restrictions placed upon, data or information stored or transmitted across computers and network systems, even when data or information resources are not securely protected.

***Violations of this policy section include, but are not limited to:***

1. accessing, or attempting to access, data or information from any system, e.g., e-mail, LDAP, ellucian Colleague, a personal computer, without proper authorization regardless of the means by which this access is attempted or accomplished;
2. disseminating in any form, to an entity, data or information obtained from any system regardless of whether or not one is authorized to access said data or information;
3. giving someone else the means to access data or information that he or she is not authorized to access;
4. providing your own password, obtaining, sharing, using, or attempting to use passwords or other information that pertain to someone else's account;

5. without proper authorization: inspecting, modifying, distributing, copying, or attempting to do so, data, mail, messages, or software;
6. tapping or monitoring phone or data lines; or
7. accessing files by circumventing privacy, security, or other legal restrictions.

College community members must comply with the laws governing legally licensed software or shareware software, copyrighted materials, or other assets pertaining to computers or network systems, even when such software or assets are not securely protected.

***Violations of this policy section include, but are not limited to:***

1. making more copies of software than the license allows;
  - a. duplicating someone else's copy of proprietary software;
  - b. inspecting, modifying, distributing, or copying data or software without proper authorization, or attempting to do so;
2. giving another individual the means by which to inspect, modify, distribute, or copy proprietary data or software; or
3. stealing network or phone services.

The United States Department of Education's document number [DCL: GEN-10-08](#) addresses penalties for copyright infringement include civil and criminal penalties. Specifically, anyone who is found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages of not less than \$750 nor more than \$30,000 per work infringed. For information on other fees that might be assessed see [Title 17, United States Code, Sections 504 and 505](#).

College community members must respect the finite capacity of computers or network systems by limiting use of computers, game consoles, "gaming network activities" and network systems so as not to interfere unreasonably with the activity of other users. No level of user bandwidth is guaranteed.

***Violations of this policy section include, but are not limited to:***

1. knowingly tampering with, obstructing, or impairing the availability of WC IT Resources, using excess bandwidth, or attempting to do so;
2. knowingly sending a crippling amount of data around a network; introducing damaging, self-propagating, or otherwise harmful software (such as computer viruses or worms) into a computer or a network;

3. hoarding computer or network resources in ways that interfere with the normal operation of WC IT Resources;

a. removing or modifying computer or network equipment or software without proper authorization, or attempting to do so;

4. opening the College network to outside access by any means, for example by the connection of a personal wireless network access point or Ethernet switch;

5. altering WC IT Resources' equipment or software; or

6. altering telecommunications wiring, telephone sets, or associated equipment.

College community members must respect other policies, rules, or procedures established to manage computers or network systems, including those established to control access to, or the use of, computer data, files, or other information.

***Violations of this policy include, but are not limited to:***

1. using WC IT Resources without proper authorization or for unauthorized purposes, or attempting to do so;

2. using WC IT Resources to violate College, local, state, or federal regulations;

3. using copyrighted materials on WC IT Resources without the required authorization;

4. posting pictures, video, audio, or personal information of or about a person or persons on a computer system without the express permission of the subject(s);

5. posting or displaying material that is libelous or harassing in nature;

6. supplying false or misleading information or identification in order to access WC IT Resources, or attempting to do so;

7. deliberately trying to log on to an account that you are not authorized to use;

8. sending electronic mail, messages, or facsimile transmissions in a threatening or harassing manner or using campus phones to harass or threaten others;

9. using WC IT Resources for commercial purposes, political campaigning unrelated to academic or co-curricular activities, or any activity that would jeopardize the College's tax exempt status;

10. establishing of any type of network service, e.g. Web servers or music servers, not authorized by the College's Chief Information Officer; or

11. using campus phones for fraudulent purposes.

## **Violations**

In the event of violations of the provisions of this document, the Chief Information Officer may immediately terminate all services accessible through the use of the violator's WC Network ID. Violators of College policies may be referred to the Washington College Honor Board and/or the employee's supervisor for appropriate disciplinary action. Violators may also be subject to prosecution under local, state, and federal laws. Any decision to terminate service may be appealed to the President's Office.

REV 01/2009