OFFICE OF INFORMATION TECHNOLOGIES (OIT)

The Office of Information Technologies (OIT) is Washington College's Central IT organization. OIT advocates for information technologies that foster and support the enduring values of Washington College by providing technologies that enhance the learning and teaching experience and empower communications for the community. Some of what we do:

- Provide guidance in the development of IT standards and policies that facilitate and govern the College's access and use of IT resources.
- IT Infrastructure, building and maintaining IT services, including email, Wi-Fi, networking, authentication, telecommunications, and other IT systems that the community depends upon.
- Enterprise Applications, maintaining the College's database of records for financial information, human resources, donors, and students.
- IT Acquisitions, purchasing all College-owned computers, mobile devices, and other IT-related hardware and supplies.

Responsive, professional IT services result in the campus community's ability to access and use information technology effectively. **Learn more about OIT services**.

Authentication Service

The authentication service provides password security for email accounts, Wi-Fi, and other networked IT services. Do not give your Washington College UserID or password to anyone. The Washington College OIT, including the email administrators or anyone affiliated with management of your UserID, password, and accounts do not send emails asking for your password.

Password and account management for your Washington College UserID that enables access to email, Wi-Fi, network, and other IT resources is done through the **Washington College Account Password Management website**. Be sure to complete the steps necessary to set up your account so you can complete password recovery if you forget your password.

Please do not fall for scam emails that appear to be from Washington College webmail administrators asking for your UserID, password, or other personal information. These emails, referred to as phishing, are illegal attempts to acquire sensitive information such as your UserID and password. They are designed to look convincing, but no legitimate business or government agency will **ever** ask you to provide password and personal information in an email.

If you believe that your UserID/password combination has been compromised, change your password. If you are ever in doubt about an email that appears to be from a Washington College department, please contact the HelpDesk (ext. 7777, or 410-778-7777 from off campus or using a cell phone). You can also email the HelpDesk at helpdesk@washcoll.edu.

WC-Wireless Wi-Fi and Ethernet Network Service

Ethernet and WC-Wireless Wi-Fi network access are available in each dormitory room. Because Wi-Fi coverage is a shared network medium and is subject to interference and performance issues during high use, if your computing device has an Ethernet port, use the in-room Ethernet jack to connect for improved connection reliability and speed.

Network access control is provided by captive portal for both the Ethernet and Wi-Fi services. Connect and use your Washington College UserID and Password to login. If you need additional assistance using this service, contact the HelpDesk by telephone (ext. 7777, or 410-778-7777 from off campus or using a cell phone). You can also email the HelpDesk at helpdesk@washcoll.edu. Additional information **may be found here**.

Campus Telephone Service

Policy on Release of Telephone Numbers, Campus Directory Information, and 1-800 Numbers

The College strives to protect students' safety and privacy. It is against policy for anyone in the College community to distribute a student's telephone number, room assignment, or personal information to any outside entity. An outside entity includes anyone who is not a verified current employee of Washington College. While a student can choose to share his or her personal information, students may not share someone else's (another student's) personal information. Only current employees of Washington College can receive this information.

The information in the Washington College Campus Directory is for internal use only. It is against Washington College policy to distribute the directory off campus or to share its content with anyone other than a current employee of Washington College.

Computer-Related Policies

The general nature of a network is an open access, high-speed connection to the world through the use of technology. Because of the capabilities that result from such a powerful tool, users of the Washington College Network should be aware of several policies. The purpose of these policies is to preserve the integrity and accessibility of our network communications. Infractions of these policies and guidelines must be reported to the Office of Information Technologies' (OIT) Executive Director for investigation and referral to appropriate departments in the College. The OIT website directs users to the College's network policies and guidelines that apply to all users of the College's IT Resources, including all web and information servers

operating on the Washington College Network. Any questions or concerns about these policies and guidelines should be addressed to the Library and Information Technology HelpDesk at ext. 7777. Policies posted on the OIT website are considered an integral part of the Student Handbook.

Acceptable Use Policy for Information Technologies Resources

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** the Web and information servers operating on the Washington College Network. Infractions of these guidelines are to be reported to the Executive Director for investigation and referral to the appropriate department of the College. If there is an immediate threat, for example, someone stalking or harassing by email or other technological means, or threat of harm or violence, contact Public Safety immediately.

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 Handbook.

Legitimate use of WC IT Resources is limited to those persons who have all of the following: proper authorization, a UserID, 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, regardless of whether specific rules are built in, or whether 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 Executive Director 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.

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):

- accessing, or attempting to access, data or information from any system (e.g., email, LDAP, Ellucian Colleague, a personal computer) without proper authorization, regardless of the means by which this access is attempted or accomplished;
- disseminating in any form, to any entity, data or information obtained from any system, regardless of whether one is authorized to access said data or information;
- giving someone else the means to access data or information that he or she is not authorized to access;
- providing your own password, obtaining, sharing, using, or attempting to use passwords or other information that pertain to someone else's account;
- without proper authorization: inspecting, modifying, distributing, copying, or attempting to do so, data, mail, messages, or software;
- tapping or monitoring phone or data lines; or
- 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):

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

The United States Department of Education's document number **DCL: GEN-10-08** addresses penalties for copyright infringement, including 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, 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):

- knowingly tampering with, obstructing, or impairing the availability of WC IT Resources, using excess bandwidth, or attempting to do so;
- 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;
- hoarding computer or network resources in ways that interfere with the normal operation of WC IT Resources;
- removing or modifying computer or network equipment or software without proper authorization, or attempting to do so;
- 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;
- altering WC IT Resources' equipment or software; or
- 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):

- using WC IT Resources without proper authorization or for unauthorized purposes, or attempting to do so;
- using WC IT Resources to violate College, local, state, or federal regulations;
- using copyrighted materials on WC IT Resources without the required authorization;
- 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);
- posting or displaying material that is libelous or harassing in nature;
- supplying false or misleading information or identification in order to access WC IT Resources, or attempting to do so;
- deliberately trying to log on to an account that you are not authorized to use;
- sending electronic mail, messages, or facsimile transmissions in a threatening or harassing manner or using campus phones to harass or threaten others;
- 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;
- establishing of any type of network service (e.g., web servers or music servers) not authorized by the College's Executive Director; or
- 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 UserID. 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.

Terms and Conditions Governing the Use of the Washington College Network
Network ID

A WC UserID provides access to a variety of facilities and services managed by Washington College Information Technologies. Any use of a WC UserID constitutes acceptance of the terms and conditions in this document. The College reserves the right to modify the provisions of this document and will announce all such modifications in appropriate College publications.

The facilities and services accessible by a WC UserID will vary over time, depending on changes in WC's IT Resources and depending on the user's relationship with the College. Some examples of these facilities and services are electronic mail, research databases, and access to certain information from the College's databases, such as viewing grades. In addition, many College administrative systems rely on the WC UserID and passwords for security and access.

Once an individual is granted access to data, that person is responsible for maintaining the security and confidentiality of that data.

Authorized Use

Use of a WC UserID is subject to the following limitations:

- WC UserIDs may not be used for the solicitation of business, to conduct business, or for political campaigning unrelated to academic or co-curricular activities, candidate endorsement, or illegal activities;
- Outside resources directly or indirectly accessed using a WC UserID may have their own regulations or restrictions. It is the responsibility of the WC UserID user to be aware of and abide by these regulations or restrictions;
- The use of a WC UserID by more than one person is prohibited. Users are responsible for any consequences arising from the use of their WC UserID, either directly or indirectly attributable to their actions. User passwords must never be shared.

Violations

In the event of violations of the provisions of this document, the Executive Director 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.

Limitation of Liability

Although Washington College tries to provide a stable and accurate computing environment, hardware and/or software errors may arise from time to time. The College does not warrant the accuracy of its computers, network systems, documentation, or advice and consultation. Neither Washington College nor or any of its agents shall be liable for any incidental or consequential damages, even if advised of the possibility thereof. In no event shall Washington College or any of its agents be liable for failure to deliver WC IT Resources' services.