NIAGARA UNIVERSITY	Acceptable Use of Electronic Resources	Date: 9/2009	No.
		Replaces: P-26	

COVERAGE:

All who access or use the university's Electronic Resources, including students, trustees, employees, volunteers, and community members.

OBJECTIVE:

To further establish rules, ethics and standards for the use of university Electronic Resources.

POLICY:

The university maintains and provides access to a wide and ever-expanding array of "Electronic Resources" for the use of students and facilitation of work by employees. Such resources include but are not limited to: computers, computer equipment, software, networks, servers, websites, internet access, intranet access, library databases, fax machines, scanners, PDA's, university-owned cellular phones and pagers, telephones, voicemail, and e-mail. Electronic Resources may only be used for purposes authorized by the university; these purposes generally comprise work, study, research, service, or student residential activities consistent with the university's mission, operations, and priorities.

The university's general policies and codes of conduct, including in particular policies related to harassment, discrimination, and intellectual property, apply to this electronic environment, just as they apply in all university settings. This Acceptable Use Policy supplements, not overrides, these existing standards. As specific Electronic Resources can come with their own typical scenarios for misuse and abuse, all who use electronic resources should familiarize themselves with the specific policy requirements below.

Username and Password for Electronic Resources; Preventing Unauthorized Access

User IDs and passwords are the primary method used to authenticate users of the university's Electronic Resources. All users must protect the university's Electronic Resources from unauthorized access. This includes:

- Taking responsibility for the security and integrity of information stored on any Electronic Resource;
- Logging out of Electronic Resources when you leave them unattended, even for a brief moment;
- Changing passwords routinely as recommended by IT (cycles vary based on the Resource);
- Cooperate with Supervisors, System Administrators, and Law Enforcement during investigations of improper use;
- Reporting the compromise or potential compromise of passwords and account information to IT;
- NEVER disclosing your username and password to a third party, including IT staff (who have other sanctioned means of accessing accounts and equipment for maintenance).

E-mail

E-mail is an official means of notification between the university and its students and employees. To ensure that the university has a static address with which to communicate, the university provides a name@niagara.edu e-mail address for each student and employee (hereinafter, "NU E-mail Address"). Every NU E-mail Address has a unique username and password, which should not be disclosed to a third party. Employees with NU E-Mail Addresses should use them solely for university business and are cautioned to avoid using them as the contact points for private communications, including those conducted over social network and other non-university resources. **Employees may not use alternate e-mail addresses for university business.**

The university does not routinely monitor a user's email, data, software, or other online activity. But the university does reserve the right to access, monitor, remove, and disclose a user's communications or other data on Electronic Resources that are owned and/or controlled by the university under the following circumstances: 1) after a university officer, dean, or department head requests HR to act per the procedure below; 2) when required by a court order or other legal authority; or 3) when the university, at its discretion, determines that there is an operationally important reason for doing so (examples include but are not limited to: productivity concerns, reputation-related concerns, trade secret or confidentiality concerns, or the substantiation of otherwise unrelated investigations).

Cell Phones

There are two broad categories of cell phones used by the University:

1) cell phones owned by the university; and,
2) cell phones owned by employees, but partially used for professional purposes. NOTE: *If the phone bill is in the employee's name, then the phone and service is the employee's personal property, regardless of who pays (or partially pays) the bill.*

Cell phones owned by the university must be used for business purposes only.

Cell phones owned by employees but paid or partially paid for by the university: May be used for a mixture of business and personal purposes. Per IRS regulations, university employees whose personal cell phones are paid for in full by the university are imputed 25% of this bill as income, while the other 75% is considered a business expense. University employees whose bills are no more than 75% partially paid by the university will not have this income imputed to them.

An annual usage form regarding the billing breakdown will be sent from the Controller's office to each employee with a personally owned cellular phone paid for in whole or in part by the university.

Prohibited Actions Using Electronic Resources

Without authorization, no user may:

- Extend the network by introducing a hub, switch, router, wireless access point, or any other service or device that permits more than one device to connect to any university network;
- Register any domain name or host content associated with the university (for further information, see the IT Department's Domain Registration Procedure);

- Provide any other person with Electronic Resources or access to them;
- Send e-mail chain letters or mass mailings for purposes other than authorized university business;
- Alter, remove, or forge e-mail headers, addresses, or messages, or otherwise impersonate or attempt to pass oneself off as another;
- Obtain or access Electronic Resources beyond the scope of your authority;
- Unless during a duly authorized investigation per this policy & procedure, eavesdrop or otherwise access communications of which you are not the intended recipient;
- Use Electronic Resources to access in a malicious manner or to alter or destroy any material you are not authorized to alter or destroy;
- Tamper with, modify, damage, alter, or attempt to defeat restrictions or protection placed on Electronic Resources.

Copyright and Other Proprietary Material

Users are expected to respect copyrights and other proprietary information when using the University's Electronic Resources. All use of content, including text, images, music, and video must comply with copyright and other applicable laws. Users with questions about Fair Use may contact the Director of Libraries or the General Counsel.

Work product

Saving particular arrangements controlled by contract, including but not limited to the NULTA Collective Bargaining Agreement, work product generated by employees in the general course of business is the intellectual property of Niagara University.

University Web Pages

Materials submitted by employees who maintain, update, and otherwise provide content for the Niagara University website are the property of Niagara University.

Data Preservation and Recovery

Users should be aware that electronic communications may be copied, backed up, and/or stored long after they were created or last accessed. Data believed to have been deleted may still be preserved in some storage medium and retrieved if necessary, however, CRITICAL DATA SHOULD ROUTINELY BE BACKED UP ON THE UNIVERSITY'S SERVER.

Disclaimers

The University's Electronic Resources are available "as is" and "as available." The university makes no guarantee that any Resource will be free of objectionable matter, defects, errors, or malevolent software. The university is not responsible for any harm arising from the use or access of Electronic Resources, nor the User's reliance upon them.

Changes to This Policy

The university reserves the right to change this Policy at any time. The university will post the most up-to-date version on myNU.

NIAGARA UNIVERSITY	Acceptable Use of Electronic Resources PROCEDURE	Date: 9/2009	No.
		Replaces: P-26	

Person	Action
Employee, student, or community member	Notices or suspects an employee violation and informs Officer, Supervisor, Department Head, or Dean, as appropriate; if uncertain, consults the Director of Human Resources. Notices or suspects a student violation and informs the Dean of Students. Notices or suspects a volunteer or community member violation and informs the Department Head of the unit coordinating the volunteer.
Officer, Supervisor, Academic Dean, or Department Head	Assesses potential violation; if it would be a serious violation, a repeat violation, or potential violation of the law, alerts the Director of HR to determine if investigation is warranted. If the potential violation is minor, addresses the matter informally per Employee Discipline Policy. If the potential violation could be criminal, alerts Campus Safety and General Counsel. Resolved matter per the Employee Discipline Policy.
Dean of Students	Assesses potential violation for violation of student rules, including the Rules of Student Conduct, Student-Athlete Code of Conduct, and Academic Integrity Policy. If investigation is warranted, works with IT Director (or designee) to ensure proper backup and authentication of Electronic Resource prior to access. If the potential violation could be criminal, alerts Campus Safety and General Counsel. Refers or addresses matter as warranted to Student Judicial, Athletics, Assistant Director of Financial Aid (student employees) or Academic Integrity Board.
Director of HR	After notification, confers with functional officer or EVP to determine if investigation and access to Electronic Resource(s) is warranted. If investigation is warranted and approved by functional officer, works with IT Director (or designee) to ensure proper backup and authentication of Electronic Resource prior to access. If there is a suspected violation of the law, immediately alerts both the Director of Campus Safety and the

	General Counsel. Works with Officer, Supervisor, Department Head, or Dean to properly document and respond per the Employee Discipline Policy.
IT Director	If alleged violator is employee, ensures proper permission from functional officer is in place, and cooperates with HR Director or corporation officer to ensure investigation is conducted and content is backed up as necessary. If alleged violator is student, informs necessary personnel, and works with Dean of Students to conduct investigation and backup as necessary. If an alleged violator is community member, works with Campus Safety and any other necessary or affected parties to ensure the proper resolution.
Campus Safety	Will document occurrences and coordinate institutional cooperation with law enforcement as necessary.
General Counsel	Will assist with determining if there is a potential violation of the law, and facilitate employee cooperation with law enforcement as necessary.