

Universal Companies Internet Policy and Procedures

Purpose:

To provide guidance for acceptable use for Internet to company employees.

Policy:

The Internet will provide employees with a fast and convenient resource for the exchange of information. The equipment necessary to access the Internet is the exclusive property of Universal Companies, and therefore any access is to be used for official business purposes only. Access to the Internet will be at the sole discretion of Management.

The Company will actively monitor use of the Internet, to ensure that anyone using Company access to the Internet does not engage in any unethical, illegal or unacceptable activity.

Examples of unethical, illegal or unacceptable activities include, but are not limited to:

1. Seeking to gain or gaining unauthorized access to information resources.
2. Gaining, communicating, or using passwords belonging to the users.
3. Using the Internet to access, process, distribute, transmit or display inappropriate media; obscene, or defamatory material, or any material, the access to which might undermine the integrity of Universal Companies.
4. Participating in chat-rooms.
5. Submitting, publishing or display any defamatory or obscene material.
6. Using the Internet for personal gain or profit.
7. The use of "Web Radio", "Web Shots", "Weather Bug", "LimeWire" (or the equivalent), or any other real-time connections, which occupies continuous bandwidth (resources) in the network.

If an employee is found to have engaged in any unacceptable activities, such activity will subject the user to discipline consistent with any applicable labor agreement or policy including revocation of rights to Internet access and may lead to termination.

All employees using County access to the Internet are expected to comply with the following:

1. All files downloaded from the Internet must be scanned with anti-virus software pre-loaded by Universal Companies.
2. No computer used for Internet access can be connected to another Internet Service Provider other than what is provided by the company.
3. Any employee that feels he or she can identify a security concern or feels that his or her system may be infected with a computer virus should perform no further work on the computer and immediately contact the Tech Department.

Procedure:

- A. It is the policy of Universal Companies to require any employee, contractor or consultant who has access to, or is required to use the Internet or Internet services using company equipment, to read, sign and abide by the Universal Companies Internet Policy.

- B. Upon hiring, each new employee will receive a copy of the Internet policy from the companies Personnel Department. Each new employee, at the request of his/her elected official or department head, will be given a computer account for Internet access only if the employee has signed a copy of the Internet Policy.

- C. Employees will be notified by e-mail and through elected officials and department heads when changes to this policy are made. It is the responsibility of each employee to review and adhere to this policy.

- D. After 30 days from the employee's hire date, if an employee has not reviewed and signed the policy, or if an employee refuses to review and sign a copy, the Technology Department will disable that employees user account and that employee will no longer be authorized to use any data processing equipment that is attached to the companies computer network.