

EMPLOYEE INTERNET USE POLICY

1. Purpose.

This policy establishes rules governing use of e-mail and internet services provided by the OBPA. E-mail and the internet are powerful communication tools and valuable sources of information and links to vendors, customers, competitors, technology, and new products and services. However, an employee's improper use of OBPA-provided e-mail or internet services can waste time and resources and create legal liability and embarrassment for both the OBPA and the employee.

2. Policy Scope.

This policy encompasses, but is not limited to, the internet, e-mail, telnet, FTP, web browsing, and Usenet or newsgroups. This policy applies to any services that are:

- Accessed on or from OBPA premises.
- Accessed using OBPA computer equipment or via OBPA paid access methods; and/or
- Used in a manner that identifies that individual with the OBPA.

3. Prohibited Activities.

Employees are strictly prohibited from using OBPA-provided services in connection with any of the following activities:

- Engaging in illegal, fraudulent, or malicious conduct, including sending or receiving copyrighted materials in violation of copyright laws or licensing agreements;
- Working on behalf of organizations without any professional or business affiliation with the OBPA, including profit-making activities that accrue to the employee;
- Use of internet or e-mail devices not authorized by the OBPA;
- Sending, retrieving, or storing offensive, obscene, or defamatory material;
- Annoying or harassing other individuals;
- Sending uninvited e-mail of personal nature or personal activities that incur additional costs to the OBPA or interfere with an employee's performance;

- Sending OBPA proprietary or confidential materials to anyone not entitled to know or possess them;
- Monitoring or intercepting the files or electronic communications of employees or third parties;
- Obtaining unauthorized access to any computer system;
- Using another individual's account or identity without explicit authorization;
- Attempting to test, circumvent, or defeat security or auditing systems of the OBPA or any organization without prior authorization;
- Distributing or storing chain letters, jokes, solicitations, offers to buy or sell goods, or other non-business material of a trivial or frivolous nature; or
- Downloading files or programs not authorized by the OBPA.

4. Personal Use.

All services are provided by OBPA for an employee's business use. Very limited or incidental use of services for personal, non-business purposes is acceptable. Personal use must be infrequent and must not:

- Involve any prohibited activity as defined by OBPA Disciplinary Policy;
- Interfere with the productivity of the employee or his or her co-workers;
- Consume system resources or storage capacity on an on-going basis; or
- Involve large file transfers or otherwise deplete system resources available for business purposes.

5. Employer Monitoring Rights.

Employees should not expect privacy with respect to any of their activities using the OBPA-provided services. The OBPA reserves the right to review all data on OBPA computers, related media, and seize all material pursuant to an investigation of possible criminal activities or non-compliance with OBPA policy.

6. Discipline.

Employees violating this policy are subject to discipline, up to and including termination of employment in accordance with OBPA Disciplinary Policy. Employees using OBPA computer systems for defamatory, illegal, or fraudulent purposes are also subject to civil liability and criminal prosecution.

7. Responsibility.

The Executive Director and department managers are responsible for their reports of adherence to this policy. Employees must be authorized in writing by their manager to use OBPA resources to access and use internet and e-mail services for limited personal use. Access to services may only be authorized after individuals agree in writing to abide by this policy.