



OLLEISN Best Practice

Policy Title: Use of Internet, Email and Other IT Resources
Policy Number: OLLEISN-BP-001
Policy Date: 01/14/2005
Effective Date: MM/DD/YYYY

1.0 Purpose

The purpose of this policy is to ensure that (agency name) Email, Internet and other Information Technology (IT) resources are used for official law enforcement purposes to carry out the duties of the organization.

2.0 Scope

This policy applies to all individuals who have access to Email, Internet, and other IT resources of the (agency name) (hereinafter referred to as "Department") including sworn law enforcement officers and non-sworn civilian employees (hereinafter referred to as "Employees").

3.0 Background

Employees must have access to Internet, Email, and other IT resources to carry out their official duties for the Department. The purpose of these resources is to support the agency in achieving its mission and goals, and resources must be used as a tool to efficiently and effectively manage the operations of the agency. Inappropriate use of these resources results in lost productivity, workplace lawsuits, public relation concerns, security breaches, disciplinary action and misused computer resources. IT resources are not intended for personal use by Employees of the Department.

4.0 Policy

This policy establishes acceptable and unacceptable use of Internet, Email, and other IT resources. All Employees are responsible for appropriate and responsible use of these resources.

4.1 Acceptable Use. All agency Employees shall use Internet, Email, and other IT resources to carry out their official duties for the Department.

- 4.2 Personal Use. A minimal amount of personal use of Email is authorized for important brief communications for personal family issues that must be addressed while on duty. Employees are encouraged to limit this use to break and lunch times.
- 4.2.1 The Department reserves the right to revoke any Employee's privilege of personal use of Email at its discretion.
- 4.3 Unacceptable Use. Use of IT resources for any of the following **personal** reasons is strictly prohibited. It is understood that circumstances will exist that result in the need to use IT resources in one or more of the activities included below for investigative purposes to carry out the mission of the Department. Prior to such use, such access shall be reported to a supervisor.
- 4.3.1 Illegal Use. IT resources shall not be used for or in support of any violation of local, state, or federal laws.
- 4.3.2 Commercial Use. IT resources shall not be used for commercial purposes, product advertisements, or "for profit" personal activity.
- 4.3.3 Accessing Sexually Explicit Materials. IT resources shall not be used to view, transmit, retrieve, save or print for personal reasons any electronic messages or images which may be deemed sexually explicit.
- 4.3.4 Lobbying. IT resources shall not be used for any form of lobbying, such as using Email to circulate solicitations for money or advertisements for charities, political reasons or religious purposes.
- 4.3.5 Copyright Infringement. IT resources shall not be used to duplicate, transmit, or use copyrighted materials such as software, documents, music, graphics, and other materials in violation of copyright laws.
- 4.3.6 Junk Mail. IT resources shall not be used to distribute chain letters, advertisements, or unauthorized solicitations for personal reasons.
- 4.3.7 Harassment. IT resources shall not be used to distribute harassing statements which disparage others based on race, national origin, sex, sexual orientation, age disability, or political or religious beliefs.
- 4.3.8 Incite Violence. IT resources shall not be used to incite violence or to describe or promote the use of weapons or devices associated with terrorist activities.
- 4.3.9 Gambling or Wagering. IT resources shall not be used to observe or participate for personal reasons in any gambling or wagering activities.
- 4.3.10 Software. IT resources shall not be used to maintain, copy, or transfer unauthorized software or software that is not licensed by the Department.

4.4 Reporting Requirements. Any employee who has knowledge that another employee is inappropriately using IT resources, must report this to his/her supervisor immediately.

4.5 Security violations. Use of IT resources to compromise the security of the Department or any other organization is strictly prohibited.

4.5.1 Unauthorized Access. Accessing accounts within or outside the agency's computers and communications facilities for which an Employee is not authorized or does not have a business need is strictly prohibited.

4.5.2 Unauthorized Dissemination. Disseminating confidential information or personal information of another is strictly prohibited.

4.5.3 Misrepresentation. Employees shall not represent themselves as someone else, fictional or real, for personal reasons.

4.6 No Personal Privacy. Internet, E-mail, and other IT resources are provided to carry out the mission of the Department. The materials, files, information, software usage, communications, and other content transmitted, received, copied, or stored using agency Internet, E-mail, or other IT resources may be monitored, reviewed, and copied by the Department at any time without notice to the sworn officer or civilian employee. Personal privacy of material transmitted, received, copied, or stored through these resources does not exist. Only authorized individuals will have the ability to monitor electronic communications.

4.7 Misuse. Any violation of any provision of this policy shall result in progressive discipline as defined by the Department's disciplinary policy.

5.0 Definitions

5.1 IT Resources. Any mechanism used for electronically acquiring, filing, storing, distributing, and retrieving data. It can also include any equipment or interconnected system or subsystems used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

6.0 Revision History

Date	Change
04/14/2005	Original policy.

7.0 References

None.

8.0 Inquiries

Direct inquiries regarding this policy to:

(Agency Name)
(Designated Contact Person)

**Acceptable Use of Email, Internet and Other IT Resources
Policy Acknowledgement**

I acknowledge that:

I have received, read, understand, and agree to abide by this policy for acceptable use of
(Police Department Name) Internet, Email, and other IT resources.

I understand that a copy of this signed Acknowledgement will be placed in my personnel file.

Authorized User - Signature

Supervisor – Signature

Date: _____

Authorized User (print): _____

Supervisor (print): _____

Department: _____