



# Acceptable Use Policy

Last Update Status: *November 2024*

## 1. Overview

The Information Technology Department's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Bloomfield Township's established culture of openness, trust and integrity. Bloomfield Township is committed to protecting Bloomfield Township's employees, partners and the Township from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Bloomfield Township. These systems are to be used for business purposes in serving the interests of the Township, and of our Residents during normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Bloomfield Township employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

## 2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and other electronic devices at Bloomfield Township. These rules are in place to protect the employee and Bloomfield Township. Inappropriate use exposes Bloomfield Township to cyber risks including virus attacks, ransomware, compromise of network systems and services, data breach, and legal issues.

## 3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Bloomfield Township business or interact with internal networks and business systems, whether owned or leased by Bloomfield Township, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Bloomfield Township and its subsidiaries are responsible for



exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Bloomfield Township policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Bloomfield Township, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Bloomfield Township.

## 4. Policy

### 4.1 General Use and Ownership

- 4.1.1 Bloomfield Township proprietary information stored on electronic and computing devices whether owned or leased by Bloomfield Township, the employee or a third party, remains the sole property of Bloomfield Township.
  - 4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Bloomfield Township proprietary information.
  - 4.1.3 You may access, use or share Bloomfield Township proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- 1.1 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.
  - 1.2 For security and network maintenance purposes, authorized individuals within Bloomfield Township may monitor equipment, systems, and network traffic at any time, per the Information Technology Department's *Audit Policy*.
    - 4.1.4 Bloomfield Township reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

### 4.2 Security and Proprietary Information

- 4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.
- 4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- 4.2.3 All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 30 minutes or less. You must lock the screen or log off when the device is unattended.
- 4.2.4 Postings by employees from a Bloomfield Township email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Bloomfield Township, unless posting is during business duties.



- 4.2.5 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

### **4.3 Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Bloomfield Township authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Bloomfield Township-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

#### **4.3.1 System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or Township protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Bloomfield Township.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Bloomfield Township or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting Bloomfield Township business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
6. Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Bloomfield Township computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.



8. Making fraudulent offers of products, items, or services originating from any Bloomfield Township account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Information Technology Department is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the Bloomfield Township network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Bloomfield Township employees to parties outside Bloomfield Township.

#### **4.3.2 Email and Communication Activities**

When using Township resources to access and use the Internet, users must realize they represent the Township. Whenever employees state an affiliation to the Township, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the Township". Questions may be addressed to the Information Technology Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.



6. Use of unsolicited email originating from within Bloomfield Township's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Bloomfield Township or connected via Bloomfield Township's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

#### **4.3.3 Posting and Social Media**

1. Posting to social media platforms by employees, whether using Bloomfield Township's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Bloomfield Township's systems to engage in other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Bloomfield Township's policy, is not detrimental to Bloomfield Township's best interests, and does not interfere with an employee's regular work duties. Posting from Bloomfield Township's systems is also subject to monitoring.
2. Employees shall not engage in any posting that may harm or tarnish the image, reputation and/or goodwill of Bloomfield Township and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by Bloomfield Township's *Non-Discrimination and Anti-Harassment* policy.
3. Employees may also not attribute personal statements, opinions, or beliefs to Bloomfield Township when posting. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Bloomfield Township. Employees assume any and all risk associated with posting.
4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Bloomfield Township's trademarks, logos and any other Bloomfield Township intellectual property may also not be used in connection with any social media activity

## **5. Policy Compliance**

### **5.1 Compliance Measurement**

The Information Technology Department will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

### **5.2 Exceptions**

Any exception to the policy must be approved by the Information Technology Department in advance.



### 5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 6. Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

## 7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: <https://www.sans.org/security-resources/glossary-of-terms/>

- Proprietary Information
- Spam
- Ransomware

## 8. Revision History

Date of Change	Responsible	Summary of Change
November 2024	Incident Response Team	Review and update format

Print Name:

Sign:

Date: