8.5 INTERNET AND IT DEVICE USAGE POLICY

Purpose
The purpose of the BACI Internet and Device Usage Policy is to establish acceptable practices regarding the use of BACI IT devices and information resources to protect the confidentiality, integrity, and availability of information created, collected, and maintained. This policy ensures that our IT resources are used responsibly to support high-quality, secure, and ethical services for the individuals and families we serve.

Audience

The Internet and Device Usage Policy applies to anyone who interacts with BACI IT Resources. This includes:

- All BACI Employees
- Contractors and Consultants
- Volunteers
- Board Members
- Interns or co-op students.
- Service Providers
- Third-party vendors and partners with access to BACI systems or data
- Individuals supported by BACI who use BACI devices or resources
- Visitors to BACI locations.

Policy

Internet Use

Internet access is provided to support staff with their work duties. While we recognize that occasional personal use is reasonable, all internet activity must be appropriate, legal, and consistent with BACI's values and policies.

Personal Use

Limited personal use of BACI’s internet resources is permitted during breaks or outside work hours.

- Personal use must not interfere with work responsibilities or productivity.
- Personal use must not consume excessive bandwidth or network resources.
- Personal use must comply with all sections of this policy, particularly the prohibited activities section.

Network Security

Protecting organizational data and systems requires proper network security practices. Different networks present different levels of risk, and staff must take appropriate precautions based on where and how they connect. Using secure connections, especially when accessing sensitive information, is critical to preventing data breaches and protecting client privacy.

- Staff must connect and use BACI Wi-Fi networks when working in BACI homes and program locations.
- When working remotely or from public locations, staff should ensure the network they are using is secure and password protected or use a mobile hotspot before accessing BACI systems.
- Confidential information, client data, and personal health information must only be accessed and transmitted through secure, encrypted connections.
- Staff home Wi-Fi networks should be password-protected with WPA2 or WPA3 encryption.

IT Device Use

Personal Use

Limited personal use of organizational devices is permitted provided that such use:

- Does not interfere with work responsibilities or productivity.
- Does not compromise device security or organizational systems.
- Does not generate significant costs to the organization (e.g., excessive data usage).

Device Assignment and Accountability

All BACI devices are assigned by the IT Department.

- The IT Department maintains an inventory of all organizational devices, including:
    - Device type, make, model, and serial number.
    - Assigned user and department.
    - Date of assignment and expected replacement date.
    - Device configuration and installed software.
- Users who are assigned BACI owned devices are responsible for:
    - Maintaining the device in good working condition.
    - Protecting the device from loss, theft, damage, or unauthorized access.
    - Using the device in accordance with this policy and all related organizational policies.
    - Reporting any loss, theft, damage, malfunction, or security incident to the IT Department immediately.
- Users must return organizational devices:
    - Upon termination of employment or contract.
    - When changing roles if the device is no longer required.
    - When the device is no longer needed for work purposes.
    - Upon request by the IT Department or Senior Management.

Security Requirements

Staff should make all efforts to:

- Create strong passwords/passphrases meeting organizational standards (minimum 12 characters) and use a password manager where applicable.
- Enable multi-factor authentication on all accounts where available.
- Never share passwords or login credentials with others.
- Log out or lock devices when leaving them unattended

When using BACI issued IT Devices staff should make all efforts to:

- Install security updates and patches promptly when notified.
- Allow automatic updates configured by IT.
- Not defer or disable automatic updates.
- Restart devices as required to complete updates.
- Critical security patches may be deployed automatically by the IT Department without user intervention.

All BACI IT Devices will have approved antivirus and endpoint protection software installed and active. Staff should not:

- Disable, uninstall, or interfere with security software

Personal Devices or Bring Your Own Device (BYOD)

The use of a personally owned mobile device to connect to the BACI network is a privilege granted to employees and should adhere to the additional guidelines:

- All personally owned laptops and/or workstations must have virus detection/protection software along with firewall protection active.
- Mobile devices that access BACI systems must have a PIN or other authentication mechanism enabled.
- All mobile devices must maintain up-to-date versions of their operating systems and software.
- Jailbroken or rooted devices must not be used to connect to BACI networks or systems.
- Confidential information must not be stored on any personally owned mobile device outside of the approved microsoft applications. (Outlook, OneDrive, SharePoint).
- Theft or loss of any mobile device that has been used to create, store, or access confidential or internal information must be reported to the BACI IT Team immediately so that organizational data can be removed.
- BACI reserves the right to revoke personally owned mobile device use privileges if staff do not abide by the requirements set forth in this policy.
- If there is a suspected incident or breach associated with a personally owned mobile device, it may be necessary to remove the device from the staff's possession as part of a third-party legal investigation.

Prohibited Use

Staff will not use BACI Internet, Networks, or IT Devices for any of the following activities:

- Accessing, creating, storing, transmitting, or distributing illegal content.
- Violating copyright, trademark, or intellectual property laws.
- Engaging in fraudulent activities or misrepresentation.
- Hacking, unauthorized access, or any other cybersecurity offense.
- Accessing, creating, or distributing sexually explicit, or obscene material, creating or sharing content that is harassing, discriminatory, threatening, or hateful, distributing content that violates the organization's workplace policies including bullying & harassment, discrimination, code of ethics.
- Installing unauthorized software, applications, or hardware without IT approval.
- Circumventing or disabling security controls, including antivirus software, firewalls, encryption, or authentication mechanisms.
- Using personal cloud storage services (e.g., personal Dropbox, Google Drive) to store organizational data.
- Inappropriate communication with supported individuals.

Monitoring and Privacy

- BACI reserves the right to monitor internet usage and device activity to ensure policy compliance, investigate security incidents, and protect organizational resources.
- Monitoring will be conducted in accordance with applicable privacy legislation and with respect to employee privacy.
- The CEO's will be notified if monitoring identifies a potential policy violation.
- Monitoring logs may be used as evidence in investigations.

Linking Policies

1.8 Code of Ethics
1.12 Corporate Responsibility Policy
1.18 Social Media Policy
8.1 Privacy Protection for Individuals
8.2 Privacy Policy – Plain Language
8.3 Privacy Protection for Employees

Statement of Compliance

I have read BACI's Internet usage policy. I fully understand the terms of this policy and agree to abide by them.

I realize that BACI's security software may record for management use the Internet address of any site I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive may be recorded and stored in an archive file for management use.

I know that any violation of this policy may lead to disciplinary action.

_____

Employee name & position

_____

Employee signature

_____

Supervisor name - program