8.5 INTERNET AND IT DEVICE USAGE POLICY

Policy Overview
Access to the Internet and BACI's IT Devices is provided to increase productivity and efficiency and to gain access to information, which is relevant to the work of supporting people with disabilities. BACI expects you to use your Internet access and IT Devices principally for business-related purposes only. Any personal use, should be restricted to non-working time (e.g. lunch breaks) and be conducted in compliance with this Policy.

Note: Whenever the word ‘Device’ is used in this policy from now on, it means 'BACI Device.'

The Internet and the use of Devices gives each individual an immense reach to propagate messages. Because of that power we must take special care to maintain the clarity, consistency and integrity of BACI communications. Thus we insist that you conduct yourself honestly and appropriately on the Internet and in using Devices, and to respect the copyrights, licenses and privacy of others.

Furthermore, all existing BACI policies apply to your conduct on the Internet and your use of Devices, especially those that deal with privacy, the use of resources, harassment, information and data security and confidentiality.

While our connection to the Internet and the use of Devices offers many potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. The overriding principle is that security is to be everyone’s first concern.

All BACI Staff must read and sign this Internet and IT Device Usage Policy – Statement of Compliance.

Definitions

Document covers any kind of file that can be read on a computer screen or Device as if it were a printed page.

Graphics includes photographs, pictures, videos, animations, movies, or drawings.

IT Device(s) means any device used to access BACI's computer, data, and electronic communications systems, and includes computers, laptops, tablets or smartphones;

BACI refers to the Burnaby Association for Community Inclusion.

Internet and IT Device Policy Provisions

A) Management and Administration

1. With existing software and systems, BACI may monitor and record Internet, e-mail and Device usage. BACI reserves the right to do so at any time in connection with any investigation where there are reasonable grounds for suspicion or wrongdoing. Employee expectations of privacy regarding Internet usage are therefore limited.
2. BACI reserves the right to inspect any and all files stored on our network or on any Devices in order to ensure compliance with BACI policies.
3. The display of any kind of sexually explicit Graphics or Document on any Device is a violation of BACI's policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using BACI's network, computing resources or any Device.
4. BACI may use independently-supplied software and data to identify and block access to inappropriate or sexually-explicit Internet sites. If you find yourself connected to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.
5. BACI's Internet facilities and Devices must not be used knowingly to violate any laws and regulations of any nation, province or other local jurisdiction.
6. Any software or files downloaded via the Internet into BACI's network or onto any Device may be used only in ways that are consistent with their licenses or copyrights.
7. No employee may use Devices knowingly to download or distribute pirated software or data.
8. No employee may use BACI's Internet access or any Device to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
9. No employee may use BACI's Internet access or any Device knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
10. Each employee using BACI's Internet access or any Device shall identify himself or herself honestly, accurately and completely (including their BACI affiliation and function where requested) when participating in chats or when setting up accounts on outside computer systems.
11. Only those employees or officials who are duly authorized to speak on behalf of BACI may speak/write in the name of BACI to any newsgroup or chat room. Other employees may participate in newsgroups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves.
12. Employees are reminded that online communication platforms are public forums where it is inappropriate to reveal confidential BACI information.
13. Since a wide variety of materials may be deemed offensive, it is a violation of BACI policy to store, view, print or redistribute any Document or Graphics that are not directly related to the user's job or BACI's business activities.

14. Employees may not use BACI Internet access or any Device to download entertainment software or games, or to play games against opponents over the Internet or to download images or videos unless there is a legitimate business-related use for such material.
15. Employees may not use BACI Internet access or any Device for excessive or inappropriate streaming of content. BACI will monitor bandwidth and data usage though our monthly data plan. In cases of misuse or excessive use, BACI may change internet and data settings without notice and provide usage records to BACI's HR department for follow up. Employees may be held responsible for excessive costs and be subject to disciplinary action.

B) Technical

1. User IDs and passwords help maintain individual accountability for Internet and Device access and resource usage. Any employee who obtains a password or ID forInternet access or use of a Device must keep that password confidential. BACI policy prohibits the sharing of BACI user IDs or passwords.
2. Any file that is downloaded to a Device must be scanned for viruses before it is run or accessed.
3. Video and audio streaming and downloading technologies represent significant data traffic which can cause local network congestion. Video and audio downloading to Devices should be avoided.

C) Security

1. BACI has installed a variety of firewalls and other security systems to assist in protecting the safety and security of BACI’s networks and Devices. Any attempts to disable, defeat or circumvent any BACI security systems are prohibited.
2. Files containing confidential or sensitive information that are transferred across the Internet must be encrypted. Until encryption is in place, confidential information should not be transferred electronically.
3. Internet services and functions that are deemed inappropriate or offensive by the Privacy Officer and Manager of Technology will be disabled at the Internet firewall.

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 being taken.

____
Employee name & position

____
Employee signature

____
Supervisor name - program