**SECTION:** Administrative **Policy:** AD 07

**Policy Date:** July 2022
April 2021; March 2015



# COMPUTER and IT POLICY

## PREAMBLE

Contact Brant business relies on the use of internet technologies, resources, and systems including computers, laptops and other portable internet technologies (e.g., flash drives, cell phones, projectors, cameras, etc.), email, and databases. It is important to outline expectations regarding the use of these technologies and resources.

The equipment available for employees at the working place belongs to the company, and its management has all the rights to monitor the Internet activity of all workers. The data transmitted, created and received via the company's equipment can be monitored as well.

## POLICY

**Contact Brant employees, students and volunteers will ensure the security and confidentiality of all information in the agency's internet technologies information systems, as well as protect and respect Contact Brant IT equipment and resources.**

## PROCEDURE

1. **Appropriate use** of Contact Brant IT equipment, databases, and internet includes:
    - maintenance and storage of client, employee and agency records;
    - use of email for business-related communication;
    - web search for business-related information;
    - utilization of passwords to protect information from outside access;
    - professional development activities;
    - maintenance and storage of IT equipment;
    - personal use of the internet and IT equipment should be limited to breaks as outlined in the Hours of Work Policy.
2. **Inappropriate use** of Contact Brant IT equipment, databases, and internet includes but is not limited to:
    - misuse of confidential information;
    - theft or falsification of records;
    - neglect or wilful destruction of equipment and records;
    - personal use of IT resources during working hours; exceptions will be made for urgent family matters;
    - accessing obscene or gambling websites or any content that exceeds the bounds of good taste and moral values;
    - communicating through chat rooms or social media, other than by designated staff on the Contact Brant sites;
    - engaging in illegal activities;
    - copying, destroying, altering any data, documentation or other information that belongs to Contact Brant;

- emailing confidential information that is not covered under consent to share information;
- allowing unauthorized or third parties to access Contact Brant's network and resources.
- access of personal email accounts, personal Facebook and other social media sites, and radio via the internet.

3. All employees, students and volunteers using Contact Brant IT equipment must respect the agency's property, and use the equipment appropriately to avoid damage, loss or misuse of information.

4. **Passwords**: Access to Contact Brant server and databases is managed via individual user accounts and confidential passwords. Employees should take reasonable steps to protect the confidentiality and integrity of passwords to keep the information safe from unauthorized access.

    - Strong passwords are important to the security of the organization. Any password should have a minimum of 8 characters comprised of uppercase, lowercase, numbers, and symbols.
    - To keep passwords secure, employees will:
        - Keep passwords confidential and
        - Avoid use of the same password for multiple accounts or systems.
    - Employees will use the Password Manager provided by the agency to store passwords including 2-Factor Authentication.
    - Employees should not share credentials or use another user's login information to access any service.

5. **E-mails:** Emails generated from agency IT systems, including but not limited to computers, laptops, cellular phones and iPads, are considered official Contact Brant communication. As such, e-mails must conform to organizational standards and be created using a high level of professionalism in both language and tone. Emails create a permanent electronic record; whatever is written in an email will be on the record for all time.
    - Employees will ensure that all messages sent are appropriate and accurate in their content. Email communications must be polite and use appropriate language. Keep messages short, simple, clear and concise.
        - Employees are not permitted to share personal opinions in a capacity that would be recognized as being from the organization on any online service
    - Emails should include an appropriate Subject title and greeting. An email signature must be formatted for all emails being sent, and will include Name, Position, Organization Name, Address, Email, Phone, Website, logo, and a confidentiality statement.
    - Employees must proof-read emails and use the spell check function before sending.
    - Where confidential email communication is used, the document will be encrypted and a password sent to the recipient in a separate email. No identifying confidential information should be included in the body of the email.

- Employees will take every precaution to ensure emails are sent only to the intended recipients.
- Employees will check their emails frequently and respond in a timely manner, usually within one business day. Employees must never reply to Spam messages, and must file these messages appropriately in the Junk folder.
- Employees will alert IT support of any breach in email security or high volume of spam.

6. **Cell Phones/Portable IT Devices:**
   - Personal cell phones must be connected to the 'Guest' wifi network
   - Refer to the Cellular Telephones/Portable Electronic Devices Policy, AD 04.
7. **Downloading Programs and Software Installation:** Only Software approved and purchased by Contact Brant will be used on Contact Brant equipment.
   - Users are not permitted to attach external storage media to any organization-owned device
   - Users are not permitted to download or distribute copyrighted materials.
   - Employees, students or volunteers may not install any software or download any programs.
   - Contact Brant software may not be removed from the office or utilized for personal use.
   - Use of personal images/photos as backgrounds or screensavers may be used provided they are of an appropriate nature.
8. **Saving Files and Documents:** Employees, students, and volunteers should review the folders and files in their network drive and email folder at least quarterly, ensuring that outdated or unnecessary files are deleted.
9. **Internet and Intranet:** Internet and Intranet access at Contact Brant is managed via individual user accounts and confidential passwords.
   - Internet services on the organization's network should only be used for activities specific to the work duties of the user accessing online services.
   - Personal files stored on PC hard drives or network file servers must be minimal.
   - Employees must refrain from any online practices or procedures that would expose the network or resources to virus attacks, spyware, adware, malware, or hackers. This includes, but is not limited to, not accessing personal email accounts, radio, social media sites.
   - The use of social networking sites, e.g. Facebook, My Space, etc. and personal Blogs / Twitter shall not be accessed using Contact Brant equipment and internet. Employees that use these sites are prohibited from disseminating any private organizational information or any negative comments regarding Contact Brant, clients, employees, community stakeholders, or funders.
10. **Website:** Contact Brant strives to maintain a current and progressive online presence, by updating our website regularly, and maintaining the website in a consistent and

appropriate manner that provides our clients and the public at large with a professional and accessible resource.

- Website maintenance will be performed by (i) the Executive Assistant or (ii) Manager of Service Coordination; all content will be approved prior to posting by the Chief Executive Officer. These employees and the Chief Executive Officer are responsible for ensuring accurate and appropriate content.
- All employees should propose appropriate revisions and additions to the Chief Executive Officer.
- The Chief Executive Officer will ensure a monthly review of the website.

11. **Social Media:** Contact Brant will use social media (such as but not limited to Facebook, Instagram, and Twitter) accounts for the purpose promotion of the agency and to support the public in communicating with our agency. Contact Brant's social media accounts must be used appropriately within the following guidelines:

- Designated employee(s) will have 'administrative login' and will:
  - Ensure regular review of the social media accounts, at a minimum of once daily
  - Respond appropriately to all postings
  - If uncertain how to respond to a specific post or group, discuss the issue with the Chief Executive Officer or Manager of Service Coordination prior to posting.
  - Use good judgment when posting agency photos. Notify any employees who are in photos to be posted so that they may approve.
  - Always adopt a positive attitude when responding to comments on the company's pages, or comments about the company in general.
  - The Chief Executive Officer will work with employees to develop a social media plan for agency promotion.
- Employees will be held responsible for what they write or post on the Contact Brant social media pages.
  - Employees will not disclose confidential information on the Contact Brant social media pages. Inflammatory comments, disparaging remarks, or negative / inappropriate language or posts may result in disciplinary action.
  - Employees will not engage in discussions regarding partner agencies, personnel issues, clients, legal issues, or government issues.
  - Employees will not post text, images, or videos that were created by someone else without proper attribution and/or authorization.
- Social media is not a substitute for inter-agency communications. Important information should be transmitted within normal agency communication channels.
- Social media is not a substitute for customer service. Refer correspondents to contact the office instead of handling inquiries entirely through social media.
- Employees will relay all posts regarding the agency, employees or volunteers to the Chief Executive Officer or designate as soon as possible.

12. **Music:** Computers or other equipment may be used to listen to music provided the music is not offensive, does not disturb co-workers, and the volume is not audible outside of the workstation. The internet should not be utilized to listen to music.

13. **Games:** Playing of computer-based games during work time is not allowed.

14. **Technical Support:** Contact Brant retains professional IT support to maintain all computer equipment and the network, as well as maintain current anti-virus software and appropriate security measures. The IT support provider is authorized to access all systems as requested by employees.

    - When experiencing problems with IT equipment and networks, IT support should be requested by employees only after first problem-solving with the Administrative Assistant.

15. **Laptops and Other Portable Equipment**: Client related or confidential information is not to be permanently stored on the laptop or other portable equipment including flashdrives for the purposes of work out of the office – employees will instead use VPN functions to access and store information on the agency's server.

    Passcodes must be utilized on portable IT equipment.

16. **Security:**
    - If it is suspected that the confidentiality of passwords has been compromised, the passwords must be changed.
    - Upon request, employees will provide the Chief Executive Officer and/or Executive Assistant any passwords who will ensure appropriate security of this information.
    - To protect computer information, employees, students and volunteers must utilize screensavers, as well as log out of computers at the end of each work day.
    - Laptops, cameras, projectors, and other portable equipment must be secured in the locked cupboard in the photocopier area when not in use. The log must be completed when taking equipment out of the office; when transporting IT equipment out of the office, equipment must remain in the possession of the employee or be stored securely, such as the trunk of a vehicle.
    - Outside personnel will not be given access to computer information unless authorized by the Chief Executive Officer or Manager of Service Coordination.

17. The Executive Assistant will maintain a record of all Contact Brant IT equipment and the name of the employee provided with each resource.

18. The Chief Executive Officer, on behalf of the corporation, has the right to reasonably monitor employee use of IT resources including but not limited to business and personal use of agency equipment, emails, texting, social media, and records:
    - All communication over the agency's server can be monitored
    - All communication over the agency's server is property of Contact Brant
    - If policies are not followed and resources are used inappropriately, the Chief Executive Officer has the right to remove privileges for use of IT resources and/or remove access to the server for mobile devices.

19. Employees inappropriately using IT resources will be subject to discipline, up to and including termination, according to the Progressive Discipline Policy.