SECTION: Administrative

Policy: AD 07

Policy Date: June 2023
July 2022; April 2021; March 2015

COMPUTER USE AND SOCIAL MEDIA POLICY

PREAMBLE

Contact Brant's 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, databases, agency's network, and social media.

This policy outlines the terms for the appropriate use of computers, email, intranet and internet at work as well as provides guidelines concerning the appropriate use of social media by employees, both while at work and outside of work hours and activities.

The equipment made available for employees belongs to the company. 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.

This policy outlines the terms for the appropriate use of computers, email, intranet and the internet at work; makes employees aware of their responsibility to maintain a positive image of the organization; and provides guidelines concerning the appropriate use of social media by employees, both while at work and outside of work hours and activities.

While Contact Brant respects the privacy and personal lives of our employees, our employees remain representatives of the company outside of work. As such, employees must be aware of their responsibility to maintain a positive image of the organization, including appropriate use of social media both while at work and outside of work hours and activities.

This policy applies to all employees, volunteers, students, and other authorized individuals who represent the organization.

POLICY

Employees are responsible for the appropriate use and security of agency computers, email accounts, and/or technology assigned to them. Employees shall use appropriate passwords and protections and ensure their computer is secured when unattended.

While Contact Brant respects the privacy and personal lives of employees, employees remain representatives of the company outside of work; as such, employees must be aware of their responsibility to maintain a positive image of the organization through the appropriate use of social media.

Contact Brant reserves the right to review and/or access employees' agency computers and emails at any time, as well as monitor employee company emails, computer use, and internet use.

PROCEDURES

1. Equipment and Technical Support
   - 1.1 When experiencing problems with IT equipment and networks, employees must first problem-solve with the Administrative Assistant, who will submit a ticket to IT Support when required.
   - 1.2 Contact Brant retains professional IT support to maintain computer equipment, appropriate security measures, and the network. IT support is authorized to access all systems as requested by the employer.
   - 1.3 Confidential information should be stored on the agency's client database or the server. Computers, laptops and other portable equipment (including flash drives) should never have client-related or confidential information stored on the hard drive or laptop.
   - 1.4 Employees should review folders and files in their network drive and email folder at least quarterly, ensuring that outdated or unnecessary files are deleted.
   - 1.5 Employees will use VPN functions to access and store information on the agency's server when working out of office.
   - 1.6 The Executive Assistant will maintain a record of all Contact Brant IT equipment and the name of the employee provided with each resource.
2. IT Security
   - 2.1 Employees are provided with a username and secured access to their computers and the agency's network and must protect this.
     - Any changes to an employee's password for computer log-in and email will be provided to the Executive Assistant; otherwise, this access is not to be shared with coworkers or people outside the organization.
   - 2.2 Employees are responsible for the use and security of the company computers including their email account and technology assigned to them.
     - To assist with security, Contact Brant provides a Password Manager program that must be used by employees.
     - Employees will use appropriate passwords and protections and ensure their computer is secured when unattended.
     - Passcodes must be utilized on portable IT equipment including company-provided cell phones.
   - 2.3 The CEO will assign user privileges as well as assign an administrator/ super user for each software and platform. Usually, this will be the Administrative Assistant responsible for IT coordination and data and/or the Executive Assistant.
   - 2.4 The employer reserves the right to monitor employee company emails and computer use, which includes intranet and internet use, as well as review and/or access employees' computers and emails at any time.

2.5 When transporting IT equipment out of the office, equipment must remain in the possession of the employee or be stored securely, such as in the trunk of a vehicle.

3. Appropriate Use of Computers, Email and the Internet
Employees are expected to use company computers, email, technology and access the internet for employment purposes which are the duties outlined in the employment agreement, job description and/or as directed by the CEO.

3.1 Restricted comments and/or behaviours may lead to discipline, up to and including termination, and could lead to criminal or civil action against an employee. Refer to the Sections on Restrictions.

3.2 Appropriate use of Contact Brant IT equipment, databases, email and internet include:
- Maintenance and storage of client, employee and agency records.
- Use of email for business-related communication.
- Web search for business-related information.
- Utilization of unique passwords to protect information from inappropriate access.
- Professional development activities.

3.3 Computers and Technology: Employees may use company computers and technology, as well as access the internet, for appropriate personal use on designated breaks, lunch and off-work times. This limited, occasional or incidental use of the agency's network for personal activities is acceptable, provided the privilege is not abused.

3.4 Emails: E-mails must conform to organizational standards and be created using a high level of professionalism in both language and tone. Emails are a permanent electronic record.

- An email signature must be formatted for all emails being sent and will include Name, Position, Organization Name, Address, Email, Phone, Website, Agency logo, a confidentiality statement, and an 'unsubscribe' option.
  Suggested confidentiality statement: This information is confidential and directed solely to the person named above and may not otherwise be distributed, copied or disclosed. If you have received this email in error, please notify the sender immediately via a return email. If you are the intended recipient of this email and no longer wish to receive emails from Contact Brant, please reply with the direction to remove your email from our contact list - please mark your email Subject as "Unsubscribe". Thank you.

- Employees must proofread emails and use the spell check function before sending.

- Where confidential email communication is used, documents must be encrypted, and a password sent to the recipient in a separate email. No identifying confidential information will be in email messages.

- If an inappropriate email or link is received, it must be deleted as 'Junk' immediately. The email must be reported to the Chief Executive Officer or alternate if sent internally. Employees will alert the Administrative

Assistant to inform IT support of any breach in email security or a high volume of spam.

- Company emails will be sent or received to and from people as required for employment purposes. Company emails are subject to the organizations' policies including workplace violence, harassment, discrimination, professional conduct and confidentiality; employees sending inappropriate emails will be subject to discipline.

4. Social Media

Social media refers to forms of electronic communication through which users create online communities to share information, ideas, personal messages and other content. Examples include but are not limited to Facebook, Linked In, Twitter, Instagram, etc.

4.1 Employee's Social Media: Employees are representatives of the company both during and outside of work hours, and it is a condition of employment that employees represent themselves and the company professionally (also refer to the *Professional Code of Conduct Policy*). As social media is a medium to exchange information, employees will be held accountable for what is written, portrayed or displayed on their social media. This is the case whether it be during or beyond work hours or activities.

- Social media content will be deemed to be that of the registered user/owner of the account.
- Employees are encouraged to use appropriate passwords and protections and ensure their social media accounts are secure.
- Where a staff member publicly associates with Contact Brant, all materials associated with their social media outlet may reflect on the company - the terms of this policy apply.

4.2 Contact Brant's Social Media Accounts: Contact Brant will use social media accounts for the purpose of promoting the agency and supporting the public in communicating with our agency. Contact Brant's social media accounts must be used appropriately by the designated employees who have the administrative logins and are assigned responsibility for managing accounts:

- Ensure regular review of the social media accounts and respond appropriately to all postings. If uncertain how to respond to a specific post or group, discuss the issue with the Chief Executive Officer.
- Employees will be held responsible for what they write or post on the Contact Brant social media pages. Use good judgment when posting agency photos and notify any employees who are in photos to be posted so that they may approve.
- The Chief Executive Officer will work with employees to develop a social media plan for agency promotion.

4.3 Contact Brant's 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 clients and the public at large with a professional and accessible resource.

- Website maintenance will be performed by the Executive Assistant. Content will be approved prior to posting by the Chief Executive Officer.
- 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.

5. <u>Restricted Use of Contact Brant Computers, Email and Internet</u>
Any *a*ctivity that reflects negatively on the organization; poses a danger to equipment, the organization or others; or conflicts with Contact Brant's policies will not be permitted. The following use of Contact Brant equipment, email, intranet and the internet is restricted and subject to discipline:

5.1 Personal use during work time, including personal emails, unless otherwise authorized to do so.

- On designated breaks/lunch and off-work times, provided the privilege is not abused, employees may make limited, occasional or incidental use of company computers and technology, and access the internet for appropriate personal use.

5.2 Internet sites which are deemed to be inappropriate are not to be accessed. Examples include pornographic websites, blocked websites, gambling websites, potentially harmful websites, etc.

5.3 Downloading files, music, videos, pictures, etc. not required for employment purposes.

5.4 Conducting unapproved business for any alternate sources of employment, compensated or otherwise, or for any home-based business at any time.

5.5 Installing or running security programs or utilities unless specifically instructed to do so.

5.6 Not complying with copyright and licensing restrictions on any information which has been downloaded or is protected by the organization.

5.7 Allowing others who are not authorized users to access and utilize company equipment or software.

5.8 Other inappropriate use of Contact Brant IT equipment, databases, and internet includes, but is not limited to:

- theft or falsification of records.
- neglect or wilful destruction of equipment and records.
- engaging in illegal activities.

6. <u>Restrictions regarding Social Media</u>
The following outlines the restrictions regarding employee's social media and will be subject to discipline:

6.1 Any comments and/or behaviour that is deemed to constitute discrimination, harassment, sexual harassment, or workplace violence, as outlined in the organization's policies.

6.2 Inappropriate comments or displays, disrespectful conduct about or towards the organization, another employee, client, or someone affiliated with the organization, as outlined in the organization’s policies.

6.3 Any other comments, displays or behaviours that would reflect, or ought to reasonably have known to reflect, negatively on the organization, another employee, client or someone affiliated with the organization.

6.4 Should the employee affiliate themselves with the organization on social media, any comments made will be required to include a disclaimer stating that any opinions expressed are the employee’s own and do not represent the company's positions, strategies, or opinions (this may be done via a general disclaimer on their social media outlet or page).

6.5 The employee must not speak on behalf or represent the organization in any way, release or disclose internal, confidential, or proprietary information of any kind, without express written authorization from the organization.

6.6 Employees are prohibited from using protected materials (copyright material, branding and/or logos) without prior express written permission.