<Company Name>
SOCIAL MEDIA USE POLICY

1 Overview

Social networking is increasingly becoming a standard component of work and personal life. While companies are increasingly embracing social media technologies as a way of promoting products and services and improving employee retention, the potential for confidential data leakage or employee abuse is ever present.

2 Purpose

The purpose is to outline for employees, contractors and other individuals performing work for <Company Name>, acceptable use of social networking applications both on the job and in personal usage situations.

3 Cancellation or Expiration

The policy in this document does not have an expiration date. However, this policy will be subject to periodic review and updated accordingly.

4 Scope

For the purposes of this document Social Media is defined as any service or application facilitating the sharing of information and participating in public conversations over the internet.

The Social Networking Policy applies to all individuals performing work on behalf of <Company Name> including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors.

5 Policy

5.1 Speaking on Behalf of <Company Name>

Some individuals performing work on behalf of <Company Name> will, by the nature of their position, be knowledgeable about certain aspects of <Company Name> and may be authorized to speak on the behalf of <Company Name>.

- You must not speak on behalf of <Company Name> unless you are authoritative on the subject and have been authorized, in writing, to speak on behalf of <Company Name> by your manager or responsible <Company Name> executive.
- **Follow the Code of Business Conduct and other Company Policies.** As a representative of the Company you must act with honesty and integrity in all matters.

- **You must not share information that is confidential or proprietary.** Only publicly available information or information which you have been authorized to share may be disseminated. Do not refer to the products or services of vendors, clients, customers or partners without obtaining their consent. When in doubt, do not post, and seek guidance from your manager.
- **Fully disclose your affiliation with the Company.** The company requires all employees who are communicating on behalf of the company to always disclose their name, affiliation, and role within the company. It is never acceptable to use aliases or otherwise deceive people. State your relationship with the Company from the outset. This disclosure is equally important for any agency/vendor/partner/third party who is representing the Company online. They must disclose the work with **[**INSERT BRAND OR COMPANY NAME HERE**]**
- **Be mindful that you are representing the Company**. This includes being honest, respectful, and factual at all times. As a company representative, it is important that your posts convey the same positive spirit that the Company instils in all of its communications.
- **Be respectful of all individuals, races, religions cultures.** How you conduct yourself within social media online not only reflects on you – it is a direct reflection on the Company.
- **Keep Records.** It is critical that we keep records of our interactions in the online social media space and monitor activities of those whom we engage.
- **Give credit where credit is due and don't violate others' rights.** DO NOT claim authorship of something that is not yours. If you are using another party's consent, make certain that they are credited for it in your post and that they approve of you utilizing their content. Do not use the copyrights, trademarks, publicity rights, or other rights of others without the necessary permissions of the rightsholder(s)
- **Know the Internet is permanent.** Once information is published online, it is essentially part of a permanent record, even if you "remove/delete" it later or attempt to make it anonymous. If your complete thought, along with its context, cannot be squeezed into a character-restricted space (such as Twitter), provide a link to an online space where the message can be expressed completely and accurately.

5.2 Social Media Corporate Responsibilities

- Daily posting and engagement- who exactly is responsible, with performance metrics; ie amount of posts, responses, is it pre-scheduled and content approved by C level? By who? Detail this out in case of incidence there is folks accountable for each aspect.
- Daily customer service - who responds; eastern / western time zone?
- Strategy and planning- who leads up overarching brand strategy
- Advertising- who manages and has access to paid social and reporting analytics
- Security and passwords- ideal to limit to 3 or under personnel (plenty of ppl can generate and schedule content through scheduling software, however limiting the amount of folks who know the password is ideal.
- Having a system to wipe mobile devices and hardware that are lost or stolen & have the password saved.
- Monitoring and listening - who has access to that metadata
- Approvals (legal, financial, IT security, HR or otherwise)- who is involved for each department in relation to social media decisions and or guest content / access
- Crisis response plan of contact

- Social media training for other employees beyond the marketing dept who plan to use their personal profiles to promote the company or be a subject matter expect.

5.3 Personal Use of Social Media Activities

- Be aware of the implications of engaging in forms of social media and other online conversations that reference the Company and/or the associates' relationship with the Company and its brands, and that everyone recognizes when the Company might be held responsible for their behaviour.
- Always remember who we are and what role we play within the social media community.
- Do not post sensitive, private or confidential company information (e.g. unannounced launches and promotions, internal sales results, company strategy, pricing information or comparisons).
- Respect customer privacy. Never give out personal customer information (e.g. personal addresses, phone numbers or credit card information) or add information you receive from social networking to company records.
- Do not post photos of or make negative comments about our customers and do not share details about customer visits – both private and public figures – without their permission (unless it is a marketed personal appearance for the Company).
- Do not post comments about a co-worker, customer or vendor that could be perceived as harassing, threatening, retaliatory or discriminatory.
- Ensure your posts do not create a real or perceived conflict of interest. A conflict of interest exists if you have an interest outside of your work that interferes with your job responsibilities or affects your judgment.
- The Company will not tolerate discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender identity, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations or ordinances).

5.4 Social Media Use Guidelines

- The Company does not condone manipulating the social media flow by creating "*fake*" destinations and posts designed to mislead followers and control a conversation.
- When you are posting on the internet, your integrity is on display for the entire world to see, so strive to be ethical, truthful and decent.
- When you are posting about the company or its products, include the hashtag #IamCompanyname. This lets people know that you are affiliated with the Company (disclosure is required by the Federal Trade Commission). Just putting the Company name in your biography is not enough!
- We are committed to ensuring that our sponsored social media practitioners (including blogs, microblogs, forums, and any other social media) clearly and conspicuously disclose their relationship to our Company, including incentives and sponsorship. Please be sure this information is readily apparent to the public and readers of each of your posts. For tweets or other written posts on platforms such as Facebook as well as descriptions of photos on platforms like Instagram, start your post with *"#Paid or #Ad*".
- If you are posting a video on a platform such as YouTube use *"#Company name Ad*" on the actual video footage in the top corner of the screen, preferably at the beginning of the video, as well as including "*Sponsored by Company name*" above the line in the description of the video.

- If you are creating a podcast, in the opening line of the podcast, you should disclose the relationship, an example of wording you should use would be: "*This episode is a paid sponsorship by Company name*". If you use alternative language please ensure you use the word "*paid*" in your wording.
- By stating that disclosures be clear and conspicuous, practitioners should make claims that are close to the claims to which they relate, in a font that is easy to read, and in a shade that stands out against the background. For video ads, disclosures need to be on the screen long enough to be noticed, read, and understood. Audio disclosures need to be read in a cadence that is easy to follow and with understandable words.
- If you talk about the company on any website or any form of social media, please use a disclaimer like, "*All opinions are my own*".
- You should avoid posting content that might contain legal conclusions, intellectual property that belongs to other companies, and defamatory language. Everything you post online can be traced back to you, so be sure what you post is appropriate before you post it.
- All Company employees, from the CEO to interns, are subject to the Company's Code of Business Conduct in every public setting. In addition, other policies, including the Information Protection Policy and the Insider Trading Policy, govern everyone's behavior with respect to the disclosure of information. These policies are applicable to your personal activities online.
- Anything you post that can potentially tarnish the Company's image or reputation will ultimately be your responsibility. We do not encourage you to participate within the social media community, but urge you to do so properly, exercising sound judgment and common sense.
- Respect Copyrights, Trademarks, Rights of Publicity, and other Third-Party Rights within the social media community, including with regard to User-Generated Content (UGC). How exactly you do this may depend on your particular situation, so work with other teams within the Organization to make informed, appropriate decisions.
- You may come across negative or disparaging posts about the Company or its brands, or see third parties trying to spark negative conversations. Unless you are a certified online spokesperson, avoid the temptation to react yourself. Pass the post(s) along to the official company spokesperson who are trained to address such comments.
- Online, your personal and business persons are likely to intersect. The Company respects the free speech rights of all employees and associates, but you must remember that customers, colleagues and supervisors often have access to the online content you post. Keep this in mind when publishing information online that can be seen by more than friends and family, and know that information originally intended just for friends and family can be forwarded on. Remember NEVER to disclose non-public information about the Company (including confidential information) and be aware that taking public positions online that are counter to the Company's interests might cause conflict.

6 Social Media Use Checklist

The following points should be considered when creating and using accounts within social media networks. Any answers of yes should be remediated.

Social Media Question	Answer	Description
DO YOU USE A BUSINESS EMAIL ACCOUNT ON PERSONAL SOCIAL MEDIA ACCOUNTS OR PERSONAL EMAIL FOR BUSINESS SOCIAL MEDIA ACCOUNTS?		When using social media NEVER use your business email account to create personal social media profiles. This also applies if creating a business profile, NEVER use your personal email to create this account. Separation of business and personal social media accounts is crucial to maximise your online safety.
DO YOU USE THE SAME PERSONAL EMAIL ADDRESS FOR MOST OR ALL ONLINE ACCOUNTS?		The most frequently compromised information today is typically online services and social platforms. You should always have a personal email address that is only used between close family and friends and critical services such as banking, medical, etc. Keep one or two “throw-away” email accounts that you use for signups and other online services.
DO YOU USE A SINGLE EMAIL ADDRESS FOR PERSONAL COMMUNICATIONS, FINANCIAL, AS WELL AS REGISTERING FOR APPLICATIONS, PURCHASES, OR OTHER ONLINE ACCOUNTS?		If this is for personal use NEVER use a business email to register for these applications or accounts. If it fulfils a business need then always use your business email address.
DO YOU USE THE SAME PASSWORDS ON MULTIPLE ACCOUNTS?		Password recycling across multiple accounts is NEVER considered best practice due to the fact that if you are compromised on one of your accounts an attacker can then potentially gain access to more sensitive accounts such as accounts linked to financial institutions.
HAVE YOU CHANGED YOUR PASSWORDS RECENTLY		Changing passwords regularly is always recommended. With respect to these passwords consider using “passphrases” as the key to a good password is not only its complexity but its character length. Consideration should be given to having passwords/passphrases in excess of 14 characters. Consideration should also be given to adding unique special character symbols such as ‘ [‘, ‘ } ‘, ‘ ~ ‘ or ‘ ^ ‘
HAVE YOU ENABLED TWO FACTOR (2FA) OR MULTI-FACTOR AUTHENTICATION (MFA) FOR YOUR ACCOUNTS AND PROFILES?		Whilst it might be regarded by many as an inconvenience having some form of added authentication for your accounts and profiles is definitely considered best practice and will greatly reduce the potential of your accounts and profiles being compromised. MFA is considered by many as the best option but if you cannot follow these steps then 2FA is better than nothing.

DO YOU USE SIMILAR USERNAMES ACROSS SOME OR MOST OF YOUR SOCIAL MEDIA AND OTHER ONLINE ACCOUNTS?		Similar usernames across social media accounts makes it easier for attackers to discover social media accounts across platforms and develop a clearer picture about your total social media footprint.
DOES YOUR PERSONAL EMAIL ADDRESS SHARE SIMILARITIES WITH YOUR USERNAMES ACROSS SOCIAL MEDIA OR OTHER ONLINE ACCOUNTS		Sharing commonalities across social media usernames and passwords makes it very easy for an attacker to discover one if they have the other.
DO YOU USE YOUR LIKENESS AS YOUR PROFILE IMAGE ON YOUR SOCIAL MEDIA?		Refrain from using your personal likeness on all social media accounts. If required/desired limit the use of your personal likeness to your business related accounts only. Not only does this provide an attacker with an image to search the internet with but it also allows them to identify you in the real world should they be conducting reconnaissance on either yourself or your organization. Generic images of pets, landscape, cars etc as long as they themselves do not have any distinguishable marks are preferable.
DO YOU USE YOUR FULL NAME ON YOUR SOCIAL MEDIA ACCOUNTS?		For personal social media accounts, which are primarily designed to allow you to engage with family and friends, consideration should be given to displaying a nickname or a variation of your full name in order to obfuscate the potential for attackers to link you to your personal profiles. In combination with a generic profile image this is ideal to provide extra security regarding these profiles.
DO YOU ACCEPT FRIEND REQUESTS FROM PEOPLE YOU DON'T PERSONALLY KNOW?		You should NEVER accept requests from individuals you do not know or can not validate as genuine. This primarily applies to Facebook and LinkedIn and is necessary for both personal and business accounts.
DO YOU SHARE INFORMATION REGARDING YOUR EMPLOYMENT PUBLICLY ACROSS SOCIAL MEDIA?		Often the starting point for an attacker is searching for employees of a specific company in order to attack individuals that they identify as having key information and access to an organization of interests network.
DO YOU SHARE INFORMATION REGARDING YOUR TITLE PUBLICLY ACROSS SOCIAL MEDIA?		Some attackers go after key job titles of individuals that have access to specific types of company information.
DO YOU SHARE CHECK-INS AND LOCATIONS PUBLICLY FROM YOUR SOCIAL MEDIA ACCOUNTS?		If you need to post locational information within social media then this key intelligence should be restricted to individuals that are within your trusted network and should not be publicly visible. This provides not only a cyber risk to you but a physical security risk. Limiting sharing of information can be controlled via your platform settings.

ARE YOUR FRIENDS LISTS PUBLICLY ACCESSIBLE ON ONE OR MORE OF YOUR SOCIAL MEDIA ACCOUNTS?		Having friends lists publicly accessible allows an attacker to look at patterns of relationships to determine attributes and interests about you.
ARE POSTS AND CONVERSATIONS PUBLICLY ACCESSIBLE ACROSS YOUR SOCIAL MEDIA ACCOUNTS?		Having posts publicly accessible is one of the single largest vulnerabilities. Posts reveal interests, locations, centrality of relationships and a host of other personal information that can easily be used by an attacker.
DO YOU HAVE CONTROVERSIAL CONTENT PUBLICLY ACCESSIBLE ACROSS YOUR SOCIAL MEDIA ACCOUNTS (CONTENT THAT IS OVERLY SEXUAL, VIOLENT, DEROGATORY, OR DRUG RELATED		Controversial content can not only cause problems for you personally but can also cause issues for your employer. Be judicious about what you say and how you say it.
DO YOU HAVE RESTRICTIONS IN PLACE ACROSS YOUR SOCIAL MEDIA THAT LIMIT FRIENDS FROM SHARING YOUR CONTENT OR TAGGING YOU IN CONTENT.		On social media platforms you not only have to control the information you are exposing about yourself but the information your relationships may be exposing about you. Tagging you to a post on an interest page as an example now exposes your association to a specific interest.
DO YOU HAVE PERSONAL ATTRIBUTES THAT ARE PUBLICLY ACCESSIBLE ACROSS SOCIAL MEDIA ACCOUNTS (INTERESTS, EDUCATION)		Exposing personal attributes such as interests, education history, employment history provides valuable context about you that an attacker can use against you. As an example, just knowing what city you live in provides a host of services specific to a town or city that can be used as conduits for spear phishing.

7 Enforcement

Any individual found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contract and potentially legal action.

8 Definitions

Limited personal use – A philosophy that employees are permitted limited personal use of <Company Name> computing resources when that use does not:

- Interfere with business usage of <Company Name> resources.
- Is performed on non-work time.
- Does not violate acceptable use policies or standards of ethical conduct.

Social Networking - A variety of applications, usually web-based, which allow users to share content, interact with each other and develop communities around similar interests. Some examples of social networking applications are Facebook, Blogger, Twitter, LinkedIn, Flickr, and numerous other similar sites.

9 Revision History

Version	Date of Revision	Author	Description of Changes
1.0	July 15, 2020	Aaron Barr / Darren Millar	Created