

CARTERS

BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CARTERS CHARITY & NFP WEBINAR SERIES 2019

April 17, 2019

LEGAL CHALLENGES IN SOCIAL MEDIA FOR CHARITIES AND NFPS

By Terrance S. Carter, B.A., LL.B., TEP, Trade-mark Agent
tcarter@carters.ca
1-877-942-0001

© 2019 Carters Professional Corporation

CARTERS PROFESSIONAL CORPORATION
BARRISTERS . SOLICITORS . TRADEMARK AGENTS
TOLL FREE: 1-877-942-0001

Toronto (416) 594-1616 Orangeville (519) 942-0001
Ottawa (613) 235-4774
www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca

CARTERS

BARRISTERS
SOLICITORS
TRADEMARK AGENTS

Carters Charity & NFP Webinar Series 2019 Wednesday, April 17th

Legal Challenges in Social Media for Charities and NFPs

By Terrance S. Carter, B.A., LL.B., TEP, Trade-mark Agent

tcarter@carters.ca
1-877-942-0001

© 2019 Carters Professional Corporation

CARTERS PROFESSIONAL CORPORATION
TOLL FREE: 1-877-942-0001

Toronto Ottawa Orangeville
www.carters.ca www.charitylaw.ca www.churchlaw.ca

2



Terrance S. Carter, B.A., LL.B., TEP, Trade-mark Agent – Managing Partner of Carters, Mr. Carter practices in the area of charity and not-for-profit law, and is counsel to Fasken on charitable matters. Mr. Carter is a co-author of *Corporate and Practice Manual for Charitable and Not-for-Profit Corporations* (Thomson Reuters), a co-editor of *Charities Legislation and Commentary* (LexisNexis, 2019), and co-author of *Branding and Copyright for Charities and Non-Profit Organizations* (2014 LexisNexis). He is recognized as a leading expert by *Lexpert*, *The Best Lawyers in Canada* and *Chambers and Partners*, and is a Past Chair of the Canadian Bar Association and Ontario Bar Association Charities and Not-for-Profit Law Sections. He is editor of www.charitylaw.ca, www.churchlaw.ca and www.antiterrorismlaw.ca

www.charitylaw.ca

www.carters.ca

A. OVERVIEW

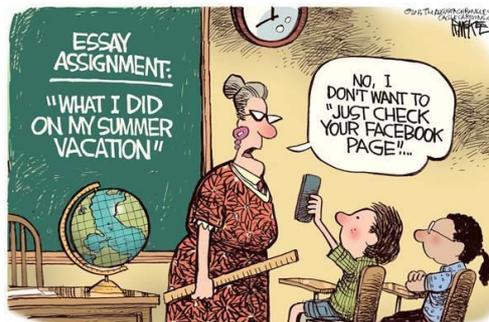
- What is Social Media?
- Legal Challenges in Social Media
 - Terms of Use Challenges
 - Privacy and Data Challenges
 - CASL Challenges
 - Intellectual Property Challenges
 - Defamation Law Challenges
 - Crowdfunding Challenges
 - CRA Regulatory Challenges
 - Employment Challenges
- Managing the Legal Challenges
- For more, see *Charity & NFP Law Bulletin* No. 441 at:
<http://www.carters.ca/pub/bulletin/charity/2019/chylb441.pdf>



B. WHAT IS SOCIAL MEDIA?

1. Setting The Stage

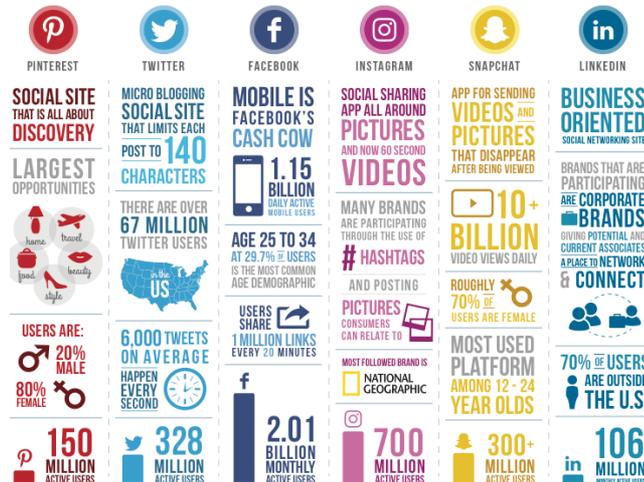
- Social media consists of websites and Internet applications that enable users to create online communities where they can share content, including user-generated content, or network with others, subject to the platform's terms of use



2. Social Media Enables Social Networking

- Social media builds on and encompasses the full breadth of online communication, creating new business models and can become a key method for building a brand for charities and NFPs
- Social media is an advertising, marketing and public relations tool, that is in an ongoing state of flux
- Charities and NFPs typically use social media to:
 - promote their brand directly or encourage followers (and “influencers”) to share their customer or supporter experience with their own followers (*i.e.*, friends, family and others)
 - promote a campaign to raise funds for a particular project or cause (*e.g.*, crowdfunding)

Examples of popular social media platforms:



Others are: Instagram, Youtube, Reddit, Google+, Tumblr, Flickr, WhatsApp, Digg, Vimeo, Delicious, Yelp, etc.

C. LEGAL CHALLENGES IN SOCIAL MEDIA

1. Terms of Use (Contracts of Adhesion)

- Each social media or crowdfunding platform unilaterally establishes its own terms of use as a “take-it-or-leave-it” contract (contract of adhesion)
- Terms of use generally cover: the collection, use and storage of personal information, including pictures and videos; the use of intellectual property, including the content created by the charity or NFP; liability for representations made by the charity or NFP and the exclusion of the platform’s liability; the jurisdiction in case of a dispute; the treatment of refunds and withdrawal of funds from an account; any service fees as a percentage of each donation; and the assignment of the contract by the platform to a third party

- Charities and NFPs need to review all terms of use carefully before agreeing to those terms
- While online terms of use do not allow for the charity or NFP, or any user, to negotiate the terms of service, knowing the limits imposed by these agreements will allow the charity or NFP to make better decisions with regard to the most appropriate use of these services
- Also, with evolving legislation and public policy, these terms of use are regularly being modified and a notice to the user outlining the changes is sufficient for consent



- A typical example of how the terms of use govern intellectual property is Twitter’s Terms of Service (last updated May 25, 2018):

“By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed). This license authorizes us to make your Content available to the rest of the world and to let others do the same”

- Such terms of use typically define “Material” or “Content” to include photos, videos, text, graphics, logos, artwork and other audio or visual materials

- As an example of a limitation of liability, Kickstarter’s Terms of Use (last updated 25 May 2018) state that:

“To the fullest extent permitted by law, in no event will Kickstarter, its directors, employees, partners, suppliers, or content providers be liable for any indirect, incidental, punitive, consequential, special, or exemplary damages of any kind, including but not limited to damages (i) resulting from your access to, use of, or inability to access or use the Services; (ii) for any lost profits, data loss, or cost of procurement or substitute goods or services; or (iii) for any conduct of content of any third party on the Site. In no event shall Kickstarter’s liability for direct damages be in excess of (in the aggregate) one hundred U.S. dollars (\$100.00)”



2. Privacy and Data Challenges

a) Personal Information, Data and Social Media

- “Personal information” is defined under the *Personal Information Protection and Electronic Documents Act* (“PIPEDA”) as “information about an identifiable individual” (e.g. name, address, social insurance number, as well as photos or videos of individuals)
- It does not include anonymous or non-personal information
- Social media can give a false sense of security, a perception that “it is just me and my online friends”
- The reality is that whatever is posted on the Internet may become virtually impossible to erase



- The privacy issues that arise with the use of social media are a significant concern
- The rapid pace of online sharing of information has called into question how social media impacts an individuals' privacy
- The information posted on social media may breach applicable privacy law
- Also, large data sets are often collected without meaningful consent and later monetized



- Information that has been stripped of identifiable markers and anonymized data that cannot be linked back to individual records are treated as non-personal information that are not subject to privacy protection
- However, risk of re-identification always exists
- Also, aggregated or group-level information could become personal information depending on the sample size



- Facebook’s Terms of Service (last updated April 19, 2018) state:
 “You own the content you create and share on Facebook”
- However, it also includes a number of necessary “consents” and “permissions” to use their service:
 “To provide our services,... you give us permission to use your name and profile picture and information about actions you have taken on Facebook next to or in connection with ads, offers, and other sponsored content that we display across our Products, without any compensation to you. For example, we may show your friends that you are interested in an advertised event or have liked a Page created by a brand that has paid us to display its ads on Facebook.”



- Further, Facebook’s Data Policy (April 19, 2018) states:



“We use the information we have about you -including information about your interests, actions and connections- to select and personalize ads, offers and other sponsored content that we show you”

“We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners measure the effectiveness and distribution of their ads and services”

b) Donor Information

- Donor information constitutes personal information that must be respected and protected by the charity, especially in the context of fundraising on social media
- Who are donors? In addition to those making donations, they can include members, employees, patients, and even customers where a gift is tied to a purchase
- Donor information may include the donor’s name, mailing address, email address, phone numbers, birthdate, name of family members, photos, videos, financial information, place of employment, preferred donation restrictions, or health information
- Personal information on a third-party platform may also be the responsibility of the charity, depending on the terms of the applicable service agreements

- Donor information forms part of the books and records that charities must keep, subject to the *Income Tax Act* (e.g., 6 years from the end of the tax year or 2 years from dissolution) and also in accordance with corporate law
- Charities wishing to exchange donor lists with other organizations, whether connected or not, must first obtain express consent from each donor
 - If a donor list is obtained from a third party, ensure that appropriate consent was obtained and that no computer program was used for scraping websites or generating a list of electronic addresses (address harvesting) in contravention of PIPEDA
- Charities acting as fundraising intermediaries for other charities should clearly state how donors' personal information will be collected, used and disclosed

c) Posting Photos/Videos of Children on Social Media

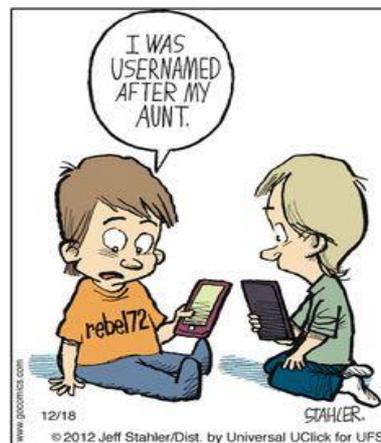
- Images of identifiable individuals, including children, are personal information
- Charities and NFPs typically use pictures of children to promote their programs and campaigns or to share with parents and other stakeholders in social media
- It is usual practice to request the consent from the child's parent or guardian
- However, there is no definitive case law yet on whether a waiver signed by a parent is binding on a minor as a matter of public policy, so best to assume that it does not
- As such, charities and NFPs may need to reconsider posting pictures or video of children on social media



d) Collecting Personal Information from Children on Social Media

- Charities using social media should limit or avoid the online collection of personal information from children,
- Problem of inadvertent collection of personal information - e.g. many children use their real names
- The Office of the Privacy Commissioner of Canada (“OPC”) has guidelines regarding the personal information of minors
- OPC guidelines include:
 - Limit/avoid collection from children
 - Obtain consent from parents of children under 13
 - From 13 to 18 must adapt consent processes to child’s level of maturity
 - Make sure default privacy settings are appropriate for the age of users

- Verify that real names are not used as usernames
- Have contractual protections in place with online advertisers to prevent the tracking of users and monitor those online advertisers
- However, any consent by parents on behalf of a minor for the collection of personal information may be unenforceable



e) General Data Protection Regulation (GDPR)

- New European Union (“EU”) General Data Protection Regulation (“GDPR”) came into effect May 25, 2018
- GDPR applies to Canadian charities and NFPs that collect or process personal data of EU residents to offer goods or services (even at no-charge)
- GDPR requires parental consent to collect, use, disclose (“process”) personal information of a child under the age of 16
- Charities and NFPs will be required to make “reasonable efforts” to verify that consent has been given
- GDPR will also require privacy notices and other information directed at children to be in plain language and easy to understand



f) Privacy Breach Reporting Obligations

- On November 1, 2018, new breach notification, reporting and recordkeeping obligations came into force under PIPEDA and accompanying regulations
- Organizations subject to PIPEDA (*i.e.*, those carrying out commercial activities) must report breaches to the OPC and notify affected individual (and possibly third parties) when:
 - The organization experiences a “breach of security safeguards” involving personal information under its control, and
 - It is reasonable in the circumstances to believe that the breach creates a “real risk of significant harm” to an individual (“RROSH”)



- “Breach of security safeguards” means loss of, unauthorized access to or unauthorized disclosure of personal information
- “Significant harm” includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property
- Relevant factors in determining whether a breach of security safeguards creates a RROSH include:
 - The sensitivity of the personal information
 - The probability of misuse of personal information
 - Any other prescribed factor (none yet from OPC)



g) Cross-border Data Transfers

- In its Report of Findings of its investigation of the data breach that affected Equifax, the OPC stated that Equifax Canada should have obtained express consent from the individuals whose personal information was sent to its US parent company for processing
- The OPC said express consent should have been obtained due to the sensitivity of the information and because the affected individuals would not reasonably have expected their personal information to be disclosed to a third party outside of Canada
- This finding may signal a sea change on the part of the OPC, which has up to now only required organizations to provide notice of cross border data transfers and not to obtain express consent

- Between April 9, 2019 and June 4, 2019, the OPC will be holding a consultation on cross border data transfers between controllers and processors and other cross border disclosures of personal information between organizations in order to solicit feedback on its evolving position including:
 - A company that is disclosing personal information across a border, including for processing, must obtain consent;
 - Individuals must be informed of any options available to them if they do not wish to have their personal information disclosed across borders

h) Privacy Torts

- Canadian courts are showing an increasing willingness to protect privacy interests
 - *Jones v. Tsige* 2013 - Ontario Court of Appeal recognized a new common law tort of “intrusion upon seclusion”
 - *Jane Doe 72511 v. Morgan* (2018), referencing *Doe 464533 v. N.D.* (2016), the Ontario Superior Court of Justice recognized “public disclosure of private facts” as a valid tort
 - Privacy-related class action litigation is also on the rise in Canada - e.g. 2017 Winnipeg Royal Ballet class action brought by former students for intimate photos taken by instructor and posted online

3. CASL Challenges



- Canada's Anti-Spam Legislation ("CASL") includes a prohibition on sending commercial electronic messages ("CEM") unless the sender has the express or implied consent of the receiver and the message contains prescribed information

A CEM is an electronic message that encourages participation in broadly defined "commercial activity"

- Generally, CASL does not apply to social media, *i.e.*, tweets or posts on a Facebook profile
 - However, it can apply if caught by the definition of "electronic address", *e.g.*, Direct Messaging on Twitter, Facebook messenger, LinkedIn, *etc.*

- Consent under CASL - express or implied
- Implied consent may be found when:
 - There is an "existing business relationship" or "existing non-business relationship" with the recipient
 - The recipient has (1) "conspicuously published" his or her electronic address or (2) disclosed it, such as through a business card; without prohibiting CEMs and the CEM relates to the recipient's business
 - As provided for in regulations or elsewhere in CASL
- Implied consent based on an existing business or non-business relationship may be relied upon only for 2 years
- Once given, express consent does not expire
 - However, consent, either express or implied, may be revoked at any time



- Directors, officers and agents of a corporation are liable for a violation of CASL unless they can demonstrate that they exercised due diligence to prevent the commission of the violation
- Employers are also vicariously liable for violations committed by their employees or agents
- CASL prescribes monetary penalties of up to \$1 million for individuals and \$10 million for corporations for a violation of CASL
- Private right of action was also to come into force on July 1, 2017 but has been delayed



4. Intellectual Property Challenges

- Charities and NFPs need to identify and protect intellectual property (“IP”)
 - There are different types of IP, including patents, trademarks, copyrights and industrial designs
 - A charity’s or NFP’s brand is one of its most important assets
 - With social media, branding reaches a large audience around the world in an instant
 - Failing to register trademarks prior to using them online can lead to third parties poaching and registering those marks prior to the owner
 - Charities and NFPs should be pro-active in protecting their marks



- Registration of a corporate name or business name does not by itself give trademark protection
- Once registered, ensure marks are properly used on social media
 - e.g. train staff on proper usage, proper markings, and consistent usage
- Ensure IP of others is not infringed
 - Social media can expose a charity or NFP to liability for infringing the IP rights of others, due to postings by employees and third parties, which may include trademarked or copyrighted material
 - Essential to identify and secure copyright of social media content through assignments and/or licences



- Hashtags (#YourCharityorNFP) may need to be protected as registered trademarks
 - Some social media sites, such as Twitter, Facebook and Instagram allow users to tag the content they share with a “hashtag”
 - Some advertising campaigns have encouraged supporters to upload photos or share stories on social media using the campaign’s hashtag
 - Concerns about hashtags include possible hashtag hijacking and/or damage to the brand or reputation of the charity or NFP
 - Popular hashtags for a charity or NFP name or major campaign can be protected as registered trademarks

5. Defamation Law Challenges

- A good reputation takes years to build, but it can be destroyed very quickly by defamatory statements spread or shared publicly (including on social media)
- In this regard, defamation law, as established in legislation (e.g., Ontario’s *Libel and Slander Act*) and common law, may restrict freedom of speech and attach liability to any person spreading defamatory materials on social media
- For example, in a recent decision dated March 4, 2019, the Court of Appeal for Ontario in *Lascares v B’nai Brith Canada*, 2019 ONCA 163 (“*Lascares*”), held that a defamation lawsuit against a charity could proceed

- In *Lascares*, the dispute arose out of an article and a social media “tweet” published by the charity stating that the appellant, a then-candidate in the 2015 federal election for the Green Party of Canada, had advocated on behalf of terrorists on social media
- The Court of Appeal held that accusing any person of supporting terrorists is a serious and damaging allegation which is likely to cause harm to that person’s reputation
- Charities and NFPs need to take appropriate steps to ensure that their social media presence does not give rise to liability under defamation law

6. Crowdfunding Challenges

- Crowdfunding involves raising funds by appealing to a “crowd” (broad group or network) of small donors or customers, using the Internet and social media
- Crowdfunding is more commonly used for specific projects with a time-limited campaign strategy
- Crowdfunding generally involves three elements: the campaigner, the crowd, and the platform
- There are a variety of types of crowdfunding, including reward-based, equity-based, debt-based or even software value token (initial coin offerings)



- Crowdfunding platforms establish their own terms of use and the charity’s or NFP’s only option is to either accept those terms or not, with no bargaining power
- Some popular crowdfunding platforms are: www.gofundme.com and www.canadahelps.com
 - Also, some social media networks offer their own crowdfunding platform (e.g. www.facebook.com)
 - However, social media networks are mostly used for sharing information about the campaign



- Crowdfunding may be subject to provincial securities legislation where it involves the issuance of securities (e.g. equity crowdfunding)
- Crowdfunding may also be subject to informal public appeals legislation (e.g. Saskatchewan's *Informal Public Appeals Act*)
 - This legislation has been applied to crowdfunding campaigns (e.g. Humbolt Broncos)
 - The Uniform Law Conference of Canada's model legislation from 2012 has only been adopted in Saskatchewan



7. CRA Regulatory Challenges

- CRA will review online content, including the materials to which a charity links and references on social media, to see if it accords with the information provided in its application
- Relevant considerations for charities:
 - Does social media content indicate programs outside of the stated charitable purposes of the charity?
 - Does the charity's social media provide a link to, and by implication agree or endorse, problematic materials or prohibited activities? e.g. "direct or indirect support of, or opposition to, any political party or candidate for public office"



8. Employment Challenges

- Employees might reveal confidential information intentionally or inadvertently
- Employees might use trademarks incorrectly, leading to dilution and weakening of a charity's or NFP's brand
- Employees might infringe the IP of others, breach CASL or other contractual obligations
- Both on-duty and off-duty conduct may justify discipline and dismissal of an employee
 - Connecting a personal mobile device on a workplace computer may allow the employer to access the employee's personal information



- Social media background checks
 - Generally, what an employee or job candidate has shared “publicly” online is also available to the employer and it may include Google search results, social media, personal websites and other content, even if not job-related
 - Social media checks are problematic from a privacy standpoint and could expose organizations to liability for privacy breach
 - An employer accessing information that is not reasonably appropriate in the circumstances may raise the question of whether the decision not to hire an individual was based on grounds of discrimination under provincial human rights legislation



D. MANAGING THE LEGAL CHALLENGES

1. Implementing a Social Media Policy

- There is no “one size fits all” policy; policy must be adapted to the needs of the charity or NFP, including posting rules, advertising, employee’s’ and other stakeholder’s’ use of social media
- Amongst other things, a social media policy may include:
 - A broad definition of social media which captures the use of email and Internet for sharing content
 - Designation of authorized individuals with access to the charity’s or NFP’s social media accounts and who is permitted to post “official” content
 - A requirement that authorized individuals posting on social media on behalf of the charity or NFP comply with all other policies on Privacy, IP, and CASL

- A requirement that no social media posting may include personal information without consent, including images of identifiable individuals
- Rules for “re-tweeting”, “hyperlinking” and “liking” without attracting liability
- As a general rule, prohibit the use of images of identifiable children or, at the very least, obtain written consent from the child’s parents or guardians
- A provision to reserve the right to edit or delete content that does not adhere to the social media policy or the terms of use of the website, as applicable



- A prohibition against postings that are obscene, racist, sexist, harassing, bullying, offensive, derogatory, defamatory, sexually explicit or otherwise inappropriate and which could discredit or cause embarrassment to the charity or NFP
- Rules for the use of proprietary information belonging to the charity or NFP on social media
- Clear indication that content creators grant the charity or NFP a world-wide, royalty-free, non-exclusive licence to publish, display, reproduce, modify, edit or otherwise use materials they share on the charity's or NFP's social media page

- A provision regarding the charity's or NFP's record retention policy for the collection, use and disclosure of donor information in its privacy policy
- A protocol for correcting and clarifying inaccurate comments made on behalf of the charity or NFP and for responding to comments made to the charity or NFP on its social media page;
- Rules for personal social media activities by employees (e.g. update profiles on professional networking sites if employment is terminated as well as personal disclaimers indicating that the views and opinions expressed are not those of the charity or NFP)

2. Implementing a Technology Use Policy

- Outline acceptable practices regarding using the charity or NFP's IT systems for accessing social media and cross reference with other policies as appropriate
- For example, the policy may provide that:
 - The charity or NFP reserves the right to monitor the use of its IT systems and as such, there is no expectation of privacy by the employee or volunteer
 - Employees and volunteers should not use the charity's or NFP's technology for personal purposes



- Use of personal IT devices (such as personal cell phones) for accessing social media during work hours, should be limited to pressing circumstances
- If the charity or NFP reimburses the employee for the cost of a cell phone or laptop, the device should be deemed to be owned by the charity or NFP and, as such, subject to being monitored or searched
- As well, when such device is no longer needed by the employee for the charity's or NFP's purposes, it should be returned to the charity or NFP and none of its content should be copied



3. Implementing a Privacy Policy

- Charities and NFPs should comply with PIPEDA and the 10 fair information principles whether or not they are technically subject to PIPEDA
- They should have a privacy policy that includes:
 - Identifies the purposes for which personal information is collected at or before collection (e.g. disclosure)
 - That the charity/NFP will obtain consent for the collection, use, or disclosure of personal information
 - That the charity/NFP will limit the collection of personal information to what is necessary for the purposes identified
 - That the charity/NFP will protect personal information
 - That the charity/NFP will give individuals access to the information about them



4. Implementing a CASL Compliance Policy

- Due diligence defence under CASL will help mitigate against liability, or reduce the imposition of a penalty by the CRTC
- What should an effective CASL compliance policy include?
 - Good record keeping practices to keep records of consent and to establish a due diligence defence
 - Effective training of staff at all levels – due to vicarious liability under CASL
 - Ongoing auditing and monitoring processes to prevent/detect misconduct and assess program effectiveness
 - Regular risk assessments and updates of the policy

5. Implementing an Intellectual Property Policy

- Protect IP before posting it online
 - Avoid a costly branding blunder by completing the necessary due diligence ahead of time
 - Conduct trademark clearance searches to ensure marks are not encroaching on others' marks before using them on social media
 - Register all trademarks, copyrights, and domain names to avoid poaching by third parties
 - Ensure that all posts on social media comply with the appropriate agreements regarding any assignment or licence over IP-protected content



E. CONCLUSION

- Although social media has many benefits, it is important to remember that discretion and common sense should be used when posting on social media
- A proactive approach to minimize potential risks should be taken before a charity or NFP embarks on any social media campaign, including a review of applicable terms of use, preferably by legal counsel
- The primary way to manage the risks associated with social media is to ensure that the various policies discussed above are implemented and reviewed on a regular basis



CARTERS

BARRISTERS
SOLICITORS
TRADEMARK AGENTS

Disclaimer

This handout is provided as an information service by Carters Professional Corporation. It is current only as of the date of the handout and does not reflect subsequent changes in the law. This handout is distributed with the understanding that it does not constitute legal advice or establish a solicitor/client relationship by way of any information contained herein. The contents are intended for general information purposes only and under no circumstances can be relied upon for legal decision-making. Readers are advised to consult with a qualified lawyer and obtain a written opinion concerning the specifics of their particular situation.

© 2019 Carters Professional Corporation

CARTERS PROFESSIONAL CORPORATION
TOLL FREE: 1-877-942-0001

Toronto Ottawa Orangeville
www.carters.ca www.charitylaw.ca www.churchlaw.ca