

CARTERS

BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CPA Not-for-Profit Executive Forum 2018

February 27, 2018

LEGAL ISSUES IN SOCIAL MEDIA FOR CHARITIES AND NOT-FOR- PROFITS


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

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

© 2018 Carters Professional Corporation

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


Toronto (416) 675-3766 Ottawa (613) 235-4774
Mississauga (416) 675-3766 Orangeville (519) 942-0001
www.carters.ca www.charitylaw.ca

 <p>BARRISTERS SOLICITORS TRADEMARK AGENTS</p>	<p>CPA Not-for-Profit Executive Forum 2018</p> <p>Toronto – February 27, 2018</p>
<p>Legal Issues in Social Media for Charities and Not-for-Profits</p> <p>By Terrance S. Carter, B.A., LL.B., TEP, Trade-mark Agent tcarter@carters.ca 1-877-942-0001</p> <p>© 2018 Carters Professional Corporation</p>	
<p>CARTERS PROFESSIONAL CORPORATION TOLL FREE: 1-877-942-0001</p>	<p>Toronto Ottawa Orangeville Mississauga www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca</p>

2

A. INTRODUCTION

- With the increasing use of social media by charities and not-for-profits collectively (“Organizations”), this presentation identifies legal issues and pitfalls that can arise for Organizations using social media, as well as the corresponding policies to manage those issues



www.charitylaw.ca www.carters.ca

- The topics that will be covered are:
 - What is meant by Social Media?
 - Benefits of Using Social Media
 - General Pitfalls of Using Social Media
 - Privacy Pitfalls
 - CASL Pitfalls
 - Intellectual Property Pitfalls
 - CRA Regulatory Pitfalls
 - Online Fundraising Pitfalls
 - Employment Related Pitfalls
 - Other Legal Pitfalls
 - Social Media and Related Risk Management Policies



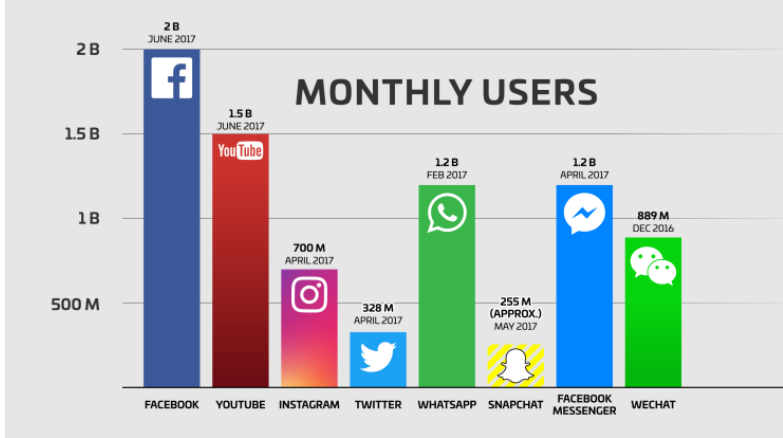
B. WHAT IS MEANT BY SOCIAL MEDIA?

- Websites and applications that enable users to create online communities where they can share content or network with others
- Social media sites are based on user participation and user-generated content
- Social networking sites provide users with the ability to upload profiles, post comments, blogs, links, photos, videos, and join “networks”
- Social media is akin to private broadcasting but without the oversight of a regulator



5

- Examples of popular social media in 2017:



Platform	Users	Date
Facebook	2 B	JUNE 2017
YouTube	1.5 B	JUNE 2017
Instagram	700 M	APRIL 2017
Twitter	328 M	APRIL 2017
WhatsApp	1.2 B	FEB 2017
SNAPCHAT	255 M (APPROX.)	MAY 2017
FACEBOOK MESSENGER	1.2 B	APRIL 2017
WECHAT	889 M	DEC 2016


<https://techcrunch.com/2017/06/27/facebook-2-billion-users/>

- Others are: Reddit, Google+, Tumblr, Flickr, Digg, Vimeo, Delicious, Blogs, etc.

www.charitylaw.ca www.carters.ca

6

C. BENEFITS OF USING SOCIAL MEDIA



- It's very inexpensive
- It helps supporters and donors to spread the word about their Organization and increase awareness with little to no advertising budget
- It can assist with employee and volunteer recruitment
- It can increase an Organization's donor base
- It can expand fundraising opportunities, including crowdfunding
- It allows for instant feedback
- It allows sharing of content in a timely manner
- It strengthens relationships with donors, volunteers, beneficiaries, employees and partners

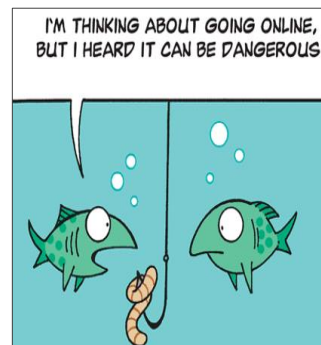
www.charitylaw.ca www.carters.ca

D. GENERAL PITFALLS OF USING SOCIAL MEDIA

- Given all the benefits of using social media, it may seem hard to envision any downside
- However, there can be negative consequences of social media for Organizations, their employees and volunteers in terms of civil and regulatory liability, as well as reputational harm
- Social media gives a false sense of security about personal information (e.g. a perception that “it is just me and my online friends”)
- The reality is that whatever is posted on the Internet may become permanent and virtually impossible to erase

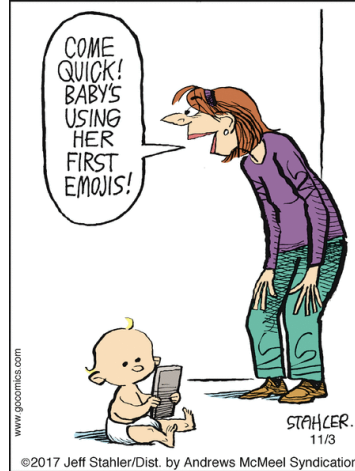


- As such, whatever an Organization posts on social media can have immediate as well as long-term legal implications
- Prior to launching or revamping a social media presence or campaign, it is important for an Organization to consider the following pitfalls:
 - Privacy Pitfalls
 - CASL Pitfalls
 - Intellectual Property Pitfalls
 - CRA Regulatory Pitfalls
 - Online Fundraising Pitfalls
 - Employment Pitfalls
 - Other Legal Pitfalls



E. PRIVACY PITFALLS OF USING SOCIAL MEDIA

- Privacy is a key legal issue that arises with the use of social media
- The rapid pace of the online sharing of information has called into question how social media impacts an individuals' privacy
- The information posted on social media can unintentionally breach applicable privacy law



www.charitylaw.ca

www.carters.ca

- Social media has spurred a change in how individuals and Organizations share and protect personal information
- As a result, Canadian legislatures and courts are continually creating new privacy laws to keep up with the changing landscape
- It is important to note that there is no express exemption from privacy laws for Organizations
- There are privacy laws in Canada (discussed below) that prevent individuals from using other individuals' "personal information" without their knowledge and consent



www.charitylaw.ca

www.carters.ca

1. What is Personal Information?

- “Personal information” is an important concept defined in privacy legislation as “any information about an identifiable individual”
- It does not include anonymous or non-personal information
- Examples include: name, address, social insurance or health card numbers, financial information, as well as photos or videos of identifiable individuals



2. Key Canadian Privacy Laws that May Apply to Social Media Use

- Federal private-sector legislation, i.e. *Personal Information Protection and Electronic Documents Act* (PIPEDA), and “substantially similar” provincial legislation
- Ontario public-sector privacy legislation
- Privacy torts



3. PIPEDA and “Substantially Similar” Provincial Legislation

- PIPEDA is the main private-sector legislation for protecting privacy in all provinces that have *not* enacted “substantially similar” legislation
- PIPEDA applies to the collection, use or disclosure of personal information in the course of a “commercial activity” - broadly defined as any transaction, act or conduct of a commercial character, and includes the sale, lease or exchange of donor, membership or other fundraising lists

- Given that it is hard to predict when a “commercial activity” by an Organization may occur, it is generally prudent to assume that PIPEDA or similar provincial legislation will apply at some point and, therefore, steps to comply should be taken
- Even if an Organization is not subject to PIPEDA, if a province has enacted privacy legislation that is declared “substantially similar” to PIPEDA, that substantially similar provincial legislation might apply to the Organization, e.g., BC’s *Personal Information Protection Act* applies to charities and NFPs



- Alberta, British Columbia, and Quebec have passed substantially similar legislation to PIPEDA
- Ontario, New Brunswick, and Newfoundland have passed substantially similar legislation with respect to personal *health* information (e.g. in Ontario, the legislation is the *Personal Health Information Protection Act* (PHIPA))
- Organizations dealing with personal health information in Ontario need to consider PHIPA
- As well in Ontario, the public-sector *Freedom of Information and Protection of Privacy Act* (FIPPA) governs “institutions” (e.g. universities and hospitals) use of non-health personal information
 - Applies to sharing of information between hospitals and foundations
 - Freedom of information for access to records

4. Key Principles from Privacy Legislation and Fair Information Principles

- An Organization is responsible for personal information in its custody and under its control
- Policies and practices regarding the management of personal information must be implemented
- An individual must be designated to oversee compliance with applicable legislation (“Privacy Officer”)
- Contracts which provide for the protection of personal information should be in place with any third party, e.g., data processors, partners, affiliates
 - Storage outside of Canada involves additional issues
 - Books and records requirement for charities



- Purposes for using personal information must be identified and documented at or before the time the information is collected
- Purposes must be those that “a reasonable person would consider appropriate in the circumstances” considering the sensitivity of the information
- The collection of personal information should be limited to that which is necessary for the purposes identified
- Personal information must be protected by appropriate safeguards



- Subject to limited exemptions, the knowledge and consent (implied or express) of the individual are required for the collection, use, or disclosure of personal information
- *e.g.*, personal information of an individual cannot be transferred without express consent
- When personal information that has been collected is used for a new purpose, the consent of the individual is required before the information can be used for that new purpose



5. Donor Information

- Donor information constitutes personal information that must be respected and protected by the Organization, especially in the context of using 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 donation
- Donor information may include the donor name, mailing address, email address, phone numbers, birthdate, name of family members, photos, videos, financial information, name of business, place of employment, preferred donation restrictions and even health information

- Need to coordinate donor information with a record retention policy
 - Donor information forms part of the books and records that Organizations must keep, and therefore must be held subject to applicable statutory retention periods
 - Retention periods for books and records by a charity for tax purposes under the ITA depends on the type of book or records (e.g., 6 years from the end of the tax year or two years from dissolution)
 - There are also corporate law record requirements
 - As a result, a charity should consider the protection of donor information in conjunction with the development of a record retention policy that considers the charity's use of social media in collecting, using and disclosing donor information

- Don't sell, barter, or trade donor information without consent
 - PIPEDA specifically prohibits “the selling, bartering or leasing of donor, membership or other fundraising lists”
 - Therefore, Organizations wishing to exchange donor or membership lists with other Organizations, whether connected or not (*e.g.*, federated, associated or affiliated Organizations), must obtain express consent from each listed donor or member prior to doing so
 - If a donor list is obtained from a third party, ensure no computer program was used for scraping websites or generating a list of electronic addresses (address harvesting) in contravention of PIPEDA



6. Posting Photos/Videos of Children on Social Media

- Images of identifiable individuals are personal information, and includes images of children
- Charities often use pictures or videos of children online to promote their programs/fundraisings or to share with parents and other stakeholders
- It is standard practice among schools and other entities to request the consent from the child's parent or guardian
- However, it is not clear that a court would give effect to a consent or waiver signed by a parent on behalf of a child
- 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 may not
- However, parental consent is still helpful in providing evidence of due diligence by the Organization

- Risk of misuse - common for innocuous photos to be taken from websites and photo-shopped or posted with inappropriate content or comments
- National Post article April 18, 2017 - “Do you know where your child’s image is?” - morphing innocent Facebook photos into sexualized imagery
- In February 2016, the French national police warned parents to stop posting photos of their children on Facebook as that could violate their privacy and expose them to sexual predators
- Sexualized images of a child becomes a permanent, indestructible record - ongoing violation
- If an Organization does decide to assume the risk of photographing/posting images or videos of minors, it must obtain robust consents, including consent to data being stored, accessed or disclosed outside of Canada

7. Collecting Personal Information from Children Online

- Organizations using social media should limit or avoid the online collection of personal information from children, taking into consideration their age and maturity
- Problem of inadvertent collection of personal information - e.g. many children use their real names as username
- Office of the Privacy Commissioner of Canada (“OPC”) and Working Group of Privacy Commissioners and Child and Youth Advocates – have raised concerns about online advertisements aimed at children and aligned with their specific interests - interest-based advertising (cookies) and disguised marketing

- United States - the *Children's Online Privacy Protection Act* ("COPPA") requires websites to obtain "verifiable" parental consent before collecting information from a child under 13
- No such law in Canada, and complaints that COPPA has been ineffective
- Organizations with websites are expected to have effective procedures to protect personal information - especially to protect the personal information of children



- Examples from the OPC include:
 - Limit/avoid collection from children
 - Obtain consent from parents of children under 13
 - Make sure default privacy settings are appropriate for the age of users
 - Verify that users are not using their real names as user names
 - 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 or may not be enforced, so there is a risk in doing so

- New European Union (“EU”) General Data Protection Regulation (“GDPR”) coming into effect May 25, 2018 has a number of provisions relating to children, including requirement for parental consent to collect, use, disclose (“process”) personal information of a child under the age of 16
- Organizations 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
- GDPR will apply to Canadian Organizations that collect or process personal data of EU residents to offer goods or services (even at no-charge)

8. Privacy Torts

- Canadian courts 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”
- *Doe 464533 v. N.D.* - January 2016 Ontario courts recognized another new tort - “public disclosure of private facts” - still good law
- 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

F. CASL PITFALLS OF USING SOCIAL MEDIA



- Canada's Anti-Spam Legislation ("CASL") came into force on July 1, 2014
- CASL includes prohibition on the sending of commercial electronic messages ("CEM") unless the sender has express or implied consent and the message contains prescribed information
- A CEM is generally an electronic message that encourages participation in broadly defined "commercial activity"
- Normally, CASL does not apply to social media, *i.e.*, tweets or posts on a Facebook profile - but can apply if caught by definition of "electronic address", *e.g.*, Direct Messaging on Twitter, Facebook messenger, LinkedIn messenger, etc.

- Regulations exclude CEMs that are sent by or on behalf of a registered charity as defined in subsection 248(1) of the *Income Tax Act* and the message has as its primary purpose raising funds for the charity
- Since some electronic messages sent by a charity may be CEMs, it is best to assume CASL will apply, subject to statutory exemptions
- Penalties possible under CASL include monetary penalties of up to \$10,000,000 for corporations and \$1,000,000 for individuals for a violation of the prohibition on sending CEMs or other prohibitions contained within CASL



- Directors and officers of a corporation can also be personally liable if the corporation sends CEM without consent or prescribed requirements
- Private right of action was also to come into force on July 1, 2017 but this has been suspended
- Consent under CASL - express or implied
- Implied consent may include:
 - There is an “existing business relationship” or “existing non-business relationship”,
 - The receiver has “conspicuously published” his or her address and hasn’t indicated he or she doesn’t want to receive spam
 - As provided for in regulation or elsewhere in CASL



- What is an “existing non-business relationship”?
 - The receiver has made a donation in the immediate two-year period the day before the CEM was sent and the sender is a registered charity
 - The receiver has volunteered in the immediate two-year period the day before the CEM was sent and the sender is a registered charity
 - The receiver was a member in the immediate two-year period the day before the CEM was sent and the sender is a “club, association, or voluntary Organization” as defined in regulation
- Best to obtain express CASL consent in order to comply

G. INTELLECTUAL PROPERTY PITFALLS OF USING SOCIAL MEDIA

- Register and enforce intellectual property (“IP”)
 - An Organization’s brand is one of its most important assets - it distinguishes the Organization from other Organizations
 - With social media, branding reaches a large audience around the world in an instant
 - Failing to register trademarks in all applicable jurisdictions prior to using them online can lead to third parties poaching and registering those marks prior to the owner



- Trademarks can be lost if they are not properly protected
- An Organization needs to be pro-active in protecting its trademark rights or it may risk losing them by default
- 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
- Consider registering a trademark for “#Organization Name” to protect brand on social media



- Ensure IP of others is not infringed
 - Social media can expose your Organization to liability for infringing the IP rights of others
 - Need to monitor social media sites for postings by employees and third parties that may infringe trademarks or copyrights of others
 - Review posted content and consider who is the owner of the work
 - If the Organization does not own the work, any reproduction of that work on social media can constitute copyright infringement



- Generally, the *author* of the work is the *owner*, unless an exception exists:
 - Work made in the “course of employment” “under a contract of service” vests in the employer unless there is an agreement to the contrary
 - Independent contractors and volunteers are not usually considered employees and therefore no automatic vesting in the Organization
- Author must be human - corporations cannot be an author
- Employment contracts should be reviewed by legal counsel to address IP issue



AUTHOR

H. CRA REGULATORY PITFALLS INVOLVING SOCIAL MEDIA

- Does the online presence of a charity accord with its stated charitable purposes?
- This is important for charities seeking charitable status, as well as those that already have charitable status
- CRA will review online content, including the materials to which a charity links, to see if it accords with the information provided in the application for charitable status



Canada Revenue
Agency

Agence du revenu
du Canada

- Relevant considerations for charities:
 - Does website content indicate programs outside of the stated charitable purposes of the charity?
 - Does the website provide a link - and therefore by implication agree and endorse - problematic materials?
 - Does the website content indicate prohibited activities?
 - CRA auditors will review website content for information and data that may support a case for revocation
 - This can include links to other Organizations, as well as reviewing Internet search history on the charity's computers

I. ONLINE FUNDRAISING PITFALLS

- Combines several of the issues mentioned previously regarding Privacy, CASL, Intellectual Property, as well as other issues described below
- There are a variety of fundraising strategies that use the Internet, such as online auctions, donation websites and crowdfunding platforms (e.g., www.gofundme.com; www.globalgiving.org; www.kickstarter.com)
- Crowdfunding involves donation-based fundraising by appealing to a “crowd” (broad group or network of small donors) over a limited period of time (typically less than 50 days) and it may or may not involve service fees

- Crowdfunding campaigns may be supporter-driven or Organization-driven
- Organization-driven crowdfunding gives the charity greater control over the messages posted on its behalf
- Crowdfunding platforms establish their own terms of service governing the use and storage of personal information, the use of intellectual property, liability for representations made, jurisdiction, the withdrawal of funds from an account, and the payment of a flat percentage of each donation and other service fees



- Different crowdfunding models may include donations via cryptocurrencies, or possibly even a “charitable cryptocurrency” offering (e.g., Donationcoin, Cleanwatercoin)
- Cryptocurrencies raise other complicated legal issues, including the use of “smart contracts”
- Online fundraising may also give rise to issues concerning identifying and compliance with donor expectations and/or restrictions



J. EMPLOYMENT RELATED PITFALLS

- Employees’ use of social media
 - Employees may reveal confidential information intentionally or inadvertently
 - Employees may use trademarks incorrectly, leading to dilution and weakening of an Organization’s brand online
 - Employees may infringe the IP of others
 - Former employees may disparage the Organization
- Social media background checks
 - Using social media in this way to vet prospective employees or volunteers or to monitor current ones can place an Organization at risk of a privacy breach



K. OTHER LEGAL PITFALLS

- Electronic discovery and evidence
 - Information can be used as evidence in litigation
- Libel, cyber-stalking, cyber-bullying
 - The content could be defamatory or lead to cyber-stalking or cyber-bullying (criminal offences)
- Data breaches
 - Third parties “hacking” into the social media page and inappropriately using it to tarnish reputation
- Ubiquitous Audience
 - Once something is posted online, it reaches a world-wide audience immediately, and is open to individual criticism and interpretation - once posted, it is virtually impossible to control or get back

L. SOCIAL MEDIA AND RELATED RISK MANAGEMENT POLICIES

- In order to help understand and minimize the legal risks associated with using social media, some of the policies and practices that an Organization may want to implement include:
 - A Social Media Policy
 - A Technology Use Policy
 - A Public Privacy Policy
 - A Privacy in the Workplace Policy
 - A CASL Compliance Policy
 - An Intellectual Property Policy



1. Implementing a Social Media Policy

- There is no “one size fits all” policy; it will need to be adapted to fit the needs of the Organization, its employees and volunteers
- An Organization should carefully consider what it wishes to include in the policy and ensure that it is consistently implemented
- For example, does the social media policy only reflect the use of the employer’s official social media pages, or also the use of employees’ personal social media pages as it impacts the Organization?



- Amongst other things, a social media policy may include the following:
 - A broad definition of social media which captures the use of email and internet surfing
 - No one may violate the privacy of another person (e.g., disclosure of salary)
 - Proprietary information belonging to the Organization may not be disclosed
 - Restricted behaviours, such as posting material deemed inappropriate or which could discredit or cause embarrassment to the Organization
 - Who is allowed to post “official” social media communications on behalf of the Organization



- Use of the Organization’s name or other trademarks or copyright on social media pages require consent
- Make reference to other relevant policies such as employment policy, privacy policy, etc.
- Encourage the use of a disclaimer such as, “*The views expressed on this website are mine alone and do not necessarily reflect the views of [name of particular Organization]*”
- Include prohibitions on speaking on behalf of the Organization or disparaging the reputation of the Organization
- Social media content of an Organization should be reviewed by management on a regular basis
- Be prepared to immediately take down inappropriate content from social media

2. Implementing a Technology Use Policy

- Outline acceptable practices regarding using the Organization’s IT systems for accessing social media and cross reference with the technology use policy if one is implemented
- For example, the policy may provide that:
 - The Organization may monitor use of its IT systems and as such, should not be used for personal purposes
 - If the IT systems are used for personal use, then the individual acknowledges that they have no expectation of privacy in connection with that use
 - Use of personal IT systems is not subject to monitoring, so it is clearly the preferred means of personal communication for employees

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



3. Implementing a Privacy in the Workplace Policy

- This policy should form part of the employee policy manual and be incorporated into employment contracts (along with other relevant policies)
- Relates specifically to the use, collection, and disclosure of employees’ personal information
- Depending on the applicable legislation, privacy laws may require an Organization to obtain consent for the collection, use or disclosure of employees’ personal information



- Employment contracts should also be reviewed to:
 - Ensure they clearly state that the Organization is the owner of all work and that moral rights are waived
 - Ensure that similar contracts are in place for volunteers and independent contractors otherwise the copyright vests in these entities by default
 - Ensure the contract incorporates by reference the various employment policies, (e.g. social media policy, etc.
 - Any termination of employment should prohibit disparaging the reputation of the Organization in any form, including on social media



4. Implementing a Public Privacy Policy

- Privacy laws in Canada require Organizations to be open about their personal information handling practices
- Organizations should implement a “public facing” privacy policy which is posted on the website
- In the event of an investigation, the privacy policy will help to demonstrate to the relevant Privacy Commissioner appropriate due diligence by the Organization
- Organizations that are subject to PIPEDA should reflect the 10 principles in the Model Code
 - See: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/



- Amongst other things, the public privacy policy should outline the following:
 - How personal information will be used, collected, and disclosed, including a document retention policy
 - How personal information is safeguarded
 - The process for making and handling complaints and requests for personal information
 - The process for dealing with, reporting and communicating data breaches
 - Identify the Privacy Officer and include contact information



5. Implementing a CASL Compliance Policy

- Due diligence defence under CASL may help mitigate against liability, or reduce the imposition of a penalty by the Canadian Radio-television and Telecommunications Commission (“CRTC”)
- What should a CASL compliant policy include?
 - establish internal procedures for compliance with CASL, including training and record keeping, specially as it pertains to consent;
 - establish auditing and monitoring mechanisms for the compliance program(s), including a process for employees to provide feedback to compliance officer;
 - establish procedures for dealing with third parties

6. 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
- Third party use of IP belonging to an Organization must be done in accordance with an appropriate trademark and/or copyright license agreement

M. CONCLUSION

- Although social media has many benefits for Organizations, it is important to remember that discretion and common sense should be used when posting on social media pages
- A proactive approach to minimizing potential risks should be taken before an Organization embarks on social media campaigns, including a review of existing insurance policies
- Primary way to manage the risk 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.

© 2018 Carters Professional Corporation

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

Toronto Ottawa Orangeville Mississauga
www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca

TERRANCE S. CARTER, B.A., LL.B, TEP, TRADE-MARK AGENT



Terrance Carter, as the Managing Partner of Carters, practices in the area of charity and not-for-profit law, and has been recognized as a leading expert by *Lexpert* and *The Best Lawyers in Canada*. Mr. Carter is also a registered Trade-mark Agent and acts as legal counsel to the Toronto office of the national law firm Fasken Martineau DuMoulin LLP on charitable matters.

Mr. Carter is a co-author of *Corporate and Practic Manual for Charitable and Not-for-Profit Corporations* (Thomson Reuters), a co-editor of *Charities Legislation & Commentary*, 2018 Edition (LexisNexis Butterworths), a contributing author to *The Management of Nonprofit and Charitable Organizations in Canada* (2014 LexisNexis Butterworths), co-author of *Branding and Copyright for Charities and Non-Profit Organizations* (2014 LexisNexis Butterworths) and the *Primer for Directors of Not-for-Profit Corporations* (Industry Canada).

Mr. Carter is a member of the Government Relations Committee of the Canadian Association of Gift Planners (CAGP), the Association of Fundraising Professionals, a past member of the Technical Issues Working Group of Canada Revenue Agency's (CRA) Charities Directorate, a past member of the Imagine Canada Technical Advisory Committee, a past member of CRA's Charity Advisory Committee and the Uniform Law Conference of Canada Task Force on Uniform Fundraising Legislation, a Past Chair of the Charities and Not-for-Profit Law Section of the Canadian Bar Association (CBA) and a past Chair of the Charity and Not-for-Profit Law Section of the Ontario Bar Association (OBA), and was the 2002 recipient of the AMS - John Hodgson Award of the OBA for charity and not-for-profit law. He is also a member of the Intellectual Property Institute of Canada, the Association of Fundraising Professionals, and the American Bar Association Tax Exempt Section, and has participated in consultations with the Public Guardian and Trustee of Ontario, the Charities Directorate of CRA, Finance Canada, and was a member of the Anti-terrorism Committee and the Air India Inquiry Committee for the CBA.

Mr. Carter has written numerous articles and been a frequent speaker on legal issues involving charity and not-for-profit law for the Law Society of Upper Canada, the CBA, the OBA, the Association of Fundraising Professionals, the American Bar Association, the CAGP, the Canadian Tax Foundation, The Institute of Chartered Accountants, the CSAE, the New York University School of Law, the University of Ottawa Faculty of Common Law, Ryerson University, McMaster University, the University of Waterloo Master of Tax program, Queensland University of Technology (Brisbane, Australia), University of Manitoba Law School as well as the C.D. Howe Institute.

Mr. Carter is also the editor of, and a contributor to www.charitylaw.ca, www.churchlaw.ca, www.carters.ca, and www.antiterrorismlaw.ca, as well as Chair of the annual *Church & Charity Law*TM Seminar, and a founder and a past co-chair of the CBA National Charity Law Symposium.

PRACTICE AREAS: Charity and Not-for-Profit Law, Fundraising, Gift Planning, National and International Strategic Planning, Charity Tax and Trusts, Intellectual Property and Corporate and Commercial Law.

EDUCATION: B.A. (Joint Honours), and a McGill University Scholar, McGill, 1975
LL.B., Osgoode Hall Law School, 1978

CALL TO THE BAR: Ontario Bar, 1980

CONTACT INFO: Orangeville: (519) 942-0001 x 222, Fax: (519) 942-0300
Toll Free: (877) 942-0001, Email: tcarter@carters.ca