

SEDA Anti-Spam Legislation Policy

Adopted by the Board of Directors March 28, 2017

The objective of this policy is to outline the roles and responsibilities of SEDA and its employees/contractors to ensure compliance with the provisions of *Canada's Anti-Spam Legislation* and its associated regulations (collectively referred to as "CASL").

Scope:

This Policy applies to all full-time, part-time, contract and casual employees of SEDA, and/or any other persons who represent SEDA or have been given access to a SEDA email account, all of whom are collectively referred to herein as "employees". Specifically, this Policy applies to all employees of SEDA, including third parties acting on SEDA's behalf when:

1. Sending electronic messages from any SEDA account or SEDA owned domain name for the purpose of promoting, advertising, marketing, or selling a SEDA product or service or promoting SEDA's brand(s) (referred to under CASL as "commercial electronic messages" or "CEMs");
2. Receiving opt-out/unsubscribe directives to unsubscribe an electronic address from receiving future CEMs;
3. Altering the transmission data of electronic messages; or
4. Installing computer programs onto another person's personal computer system (i.e. home computer) during the course of commercial activity. This includes installing malware or computer programs that the user did not consent to.

Definitions:

Altering transmission data: Manipulating or changing the transmission data (e.g. the electronic address in the "To:" line of an email message) so that the electronic message is delivered to a destination/recipient that is different than or in addition to that which was indicated to the sender, unbeknownst to and without the sender's express consent.

Commercial activity: Anything of a commercial nature (e.g. an activity that promotes a product(s), good(s), or service(s) to a person(s) or encourages a person(s) to engage in the purchase of a product(s), good(s), or service(s)), whether or not there is an expectation of profit.

Commercial electronic messages (CEMs): Electronic messages (e.g. text (SMS/MMS), sound, voice or image) sent to an electronic address (e.g. email, instant messaging, telephone account, or any similar account) that, based on the message content, links, or contact information in the message, encourages participation in a "commercial activity".

Computer program: Data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function.

Express consent: Permission that is specifically given by an individual to receive messages, which has been documented in writing (or by a computer generated process).

Implied consent: Consent that can be inferred based on the nature of the service being provided, that the individual is knowingly giving permission(eg: membership status).

Social media: Digital technologies and practices that enable people to use, create, and share content in many forms, including text, images, audio, video, and other multimedia communications. Examples include blogs, social networking websites such as Facebook, Twitter and LinkedIn, and videosharing websites such as YouTube.

Transmission data: The information about where, how, and when electronic communication is sent (e.g. the sender's and recipient's domain/email address/phone number, the date/time the message was sent, etc.).

Third party: A Third Party is an entity or individual that supplies a particular service or commodity to SEDA. The terms third party, third party provider, service provider, affinity partner, vendor and supplier and consultant can be used interchangeably.

Policy:

General Principles:

a. Sending CEMs

Every person governed by this Policy will be responsible for ensuring they meet prescribed

CASL requirements for the sending of CEMs and unsubscribing an electronic address from receiving future CEMs.

All outbound CEMs will:

1. Have the requisite (implied or express) consent from the recipient;
2. Identify the SEDA employee sending the information along with requisite SEDA contact information; and
4. Provide an easy method for recipients to opt out of receiving CEMs.

b. Sending messages via Social Media platforms

Direct messages via social media may only be sent if the direct message is in response to an inquiry or a question. Additionally, only SEDA employees or any third parties acting on behalf of SEDA who have been specifically authorized to do so may use external Social Media channels to communicate for SEDA's business purposes. Employees should consult the SEDA Executive Director before sending messages via social media.

c. Consent

All employees will ensure they have prior implied or express consent to send a CEM to an electronic address, unless the CEM is exempt. Please see the CASL CEM and Consent Procedure for more information on consent requirements and exempt CEMs.

d. Messaging Formalities

All CEMs sent by employees (including when using third parties to send CEMs on behalf of SEDA) will be sent in accordance with the requirements outlined in the CASL CEM and Consent Procedure.

e. Obtaining Express Consent to Send CEMs

Express consent must detail:

1. The purpose for which the consent is being sought;
2. The SEDA employee requesting consent and their contact information;
3. A statement that consent can be withdrawn at any time.

Please see the CASL CEM and Consent Procedure for more information and sample templates on how to obtain express consent.

f. Documenting and Storing Consent

Real-time verbal consent (i.e., express consent obtained orally) and other proofs of consent must be stored for a minimum of three (3) years. Electronic optin and opt out records are automatically stored by the SEDA newsletter server. Membership status will be recorded in a database.

g. Checking for Unsubscribe

Employees will verify and respect the unsubscribe status of electronic addresses before sending any CEMs.

h. Honouring Unsubscribe Requests

Unsubscribe requests must be honoured within ten (10) business days of receipt and electronic mail lists must be updated accordingly.

i. Emails to Foreign Countries

When sending CEMs to recipients outside of Canada, SEDA will comply with the requirements of CASL.

j. Employee Training and Awareness:

The Executive Director is responsible for ensuring that employees receive CASL awareness training. Employees will be provided training regarding CASL as appropriate upon hiring and on an ongoing basis as needed.

k. Monitoring and Control:

The Executive Director is responsible for monitoring overall compliance with this Policy.

l. Exception Management:

Departures from this Policy require prior written approval from the Executive Director and will be reviewed with specific regard to assessing the impact to SEDA and consistency with applicable legal requirements. All exceptions will be documented and retained for audit purposes