# Chapter 5: Communications Policies and Procedures

## Table of Contents

# Chapter 5: Communications Policies and Procedures

| Section:   Communications Policy | Policy:   Overall Communication Policy |
|---|---|
| Approved Date: September 23, 2019<br><br>Revision Date: September 24, 2020 | Policy Number:     5.1.1 |

**Policy**

Communications activities and key messages shall be projected in a positive, coherent and consistent manner and be aligned with EHCLA's strategic plan and marketing strategy. The Executive Director/Communications Manager will develop specific procedures and protocols to address this alignment.

The Executive Director shall be the official spokesperson for the Association.  For specific requests, subject matter experts may be called upon to interact with the media.

The Executive Director shall appoint a substitute spokesperson in the event of his/her absence.

All official communication with the media, on behalf of the Association, shall be coordinated, supported and facilitated by the Executive Director/Communications Manager.

**Procedure**

1. An employee who is contacted by a representative of the media shall refer the opportunity to the Executive Director.

2. Although photography is usually permissible, the following protocols must be observed:
   - Anyone may decline an opportunity to be photographed for the media or EHCLA print and/or online materials.
   - The entry of a news photographer into the classroom requires the consent of the classroom instructor.
   - Participants must give verbal permission to publish their photograph. If participants request their images to be removed from digital platforms, it should be done within 24 hours.

3. Although employees, as private citizens, are free to send "letters to the editor," comment on blogs or provide opinions on the internet, they should not do so using EHCLA stationery or stating their EHCLA title or position without clearance from the Executive Director.

| Section:   Communications Policy | Policy:   Overall Communication Policy |
|---|---|
| **Approved Date: September 23, 2019**<br><br>**Revision Date: September 24, 2020** | **Policy Number:      5.1.1** |

4. Employees are responsible for immediately informing the Executive Director of any occurrence that could be interpreted by the news media to reflect negatively upon the association. 'Negative news' may develop from any occurrence or situation which reflects adversely upon an employee, a group or EHCLA as a whole.

# Chapter 5: Communications Policies and Procedures

| Section:   Communications Policy | Policy:   Internet and Email |
|---|---|
| Approved Date: September 23, 2019<br><br>Revision Date: September 24, 2020 | Policy Number:      5.1.2 |

**Policy**

This employee internet usage policy applies to all employees, contractors, volunteers and partners who access our network and computers.

EHCLA's employees are advised to use the Association's internet connection for the following reasons:
- To complete their job duties.
- To seek out information that they can use to improve their work.
- To access their social media accounts, while conforming to our social media policy.

EHCLA does not want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgement and remain productive at work while using the internet.

Any use of our network and connection must follow our confidentiality and data security policies.

**Procedure**

1. Employees should:
   - Keep their passwords secret at all times, except for the master copy of the Association's staff passwords
   - Log into their EHCLA accounts only from safe devices.
   - Use strong passwords to log into work-related websites and services.

2. EHCLA employees will not use the network to:
   - Download or upload obscene, offensive or illegal material.
   - Send confidential information to unauthorized recipients.
   - Invade another person's privacy and sensitive information.
   - Download or upload copyrighted material and software.
   - Visit potentially dangerous websites that can compromise the safety of the network and computers.
   - Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

| Section:   Communications Policy | Policy:   Internet and Email |
|---|---|
| Approved Date: September 23, 2019<br><br>Revision Date: September 24, 2020 | Policy Number:     5.1.2 |

3. EHCLA also advises employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask their supervisor.

4. EHCLA may install anti-virus and disk encryption software on the Association's computers. Employees may not deactivate or configure settings and firewalls without their supervisor's approval.

5. EHCLA does not assume any responsibility if an employee's devices are infected by malicious software, or if their personal data is compromised as a result of inappropriate employee use.

**EHCLA-issued Equipment**

EHCLA expects its employees to respect and protect the Association's equipment. "EHCLA-issued equipment" includes EHCLA-issued phones, laptops, tablets or any other electronic equipment that belongs to EHCLA.

EHCLA advises employees to lock their devices in a safe storage location when they're not using them. Employees are responsible for assigned equipment.

EHCLA-issued equipment is to be used for work-related purposes. Staff should have their own technology for personal use or for other employment.

EHCLA reserves the right to examine the content on issued equipment. This includes accessing messages through work phones, work e-mails, browser history and documents on computers and digital storage.

If an employee is found to be misusing EHCLA-issued equipment for personal use or other employment, EHCLA may confiscate said equipment. The Executive Director may determine if disciplinary measures are warranted.

# Chapter 5: Communications Policies and Procedures

**Email**

EHCLA employees can use their EHCLA email accounts for both work-related and personal purposes as long as they don't violate this policy's rules. Employees shouldn't use their EHCLA email to:

- Register to illegal, unsafe, disreputable or suspect websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorized advertisements or solicitation emails.
- Sign up for a competitor's services unless authorized.

EHCLA has the right to monitor emails. EHCLA also has the right to monitor the websites that employees visit on EHCLA computers.

| Section:   Communications Policy | Policy:   Internet and Email |
|---|---|
| **Approved Date: September 23, 2019**<br><br>**Revision Date: September 24, 2020** | **Policy Number:      5.1.2** |

**Disciplinary Action**

Employees who don't conform to this policy will face disciplinary action. Serious violations will be cause for termination of employment, or legal action when appropriate. Examples of serious violations are:

- Using EHCLA's internet connection to steal or engage in other illegal activities.
- Causing EHCLA computers to be infected by viruses, worms or other malicious software.
- Sending offensive or inappropriate emails to EHCLA's supporters, colleagues or partners.

# Chapter 5: Communications Policies and Procedures

| Section: Communications Policy | Policy:   Social Media Policy |
|---|---|
| Approved Date: September 23, 2019<br><br>Revision Date: September 24, 2020 | Policy Number:    5.1.3 |

**Policy**

This policy governs the publication of and commentary on social media by employees of EHCLA. For the purposes of this policy, social media means any facility for online publication and commentary, including without limitation blogs, wikis, social networking sites such as Facebook, LinkedIn, Twitter, Instagram, Flickr, and YouTube.

**Procedure**

1. Confidentiality

It's acceptable to talk about your work and have a dialog with the community. Employees may not publish confidential information, including unpublished details about our software, details of current projects, financial information, research, clients, or trade secrets. EHCLA must respect the wishes of funders and supporters regarding the confidentiality of current projects.

2. Employee's Privacy

Privacy settings on EHCLA social media platforms should be set to allow anyone to see profile information similar to what would be on the EHCLA website. Other privacy settings that might allow others to post information or see information that is personal should be set to limit access. Be mindful of posting information that you would not want the public to see.

3. Transparency

Employees will always use their real names, be clear who they are, and identify that they work for EHCLA when interacting online within areas and topics related to the organization and its interests. Nothing should be said that is dishonest, untrue, or misleading. Be cautious about disclosing personal details.

# Chapter 5: Communications Policies and Procedures

| Section: Communications Policy | Policy:   Social Media Policy |
|---|---|
| Approved Date: September 23, 2019<br><br>Revision Date: September 24, 2020 | Policy Number:     5.1.3 |

4.   Respect for Copyright Laws

Show respect for the laws governing copyright and fair use of copyrighted material owned by others, including EHCLA's own copyrights and brands. Never quote more than short excerpts of someone else's work, and always attribute such work to the original author/source or provide a link to others' work rather than reproduce it. When using pictures or video content, ensure you have the content creator's permission.

5.   Spelling and Grammar

As a representative of our organization, please be sure that the spelling and grammar in your post or message is correct. When in doubt, use a spell-checker or consult with a co-worker or your supervisor.

6.   Respect for your audience, EHCLA, and your coworkers

As a community-based organization, our stakeholders can be diverse. It is essential that our morals and values align. Don't say anything contradictory or in conflict with the EHCLA website. Employees should respect their audience -- no ethnic slurs, offensive comments, defamatory comments, personal insults, or obscenity. When in doubt, check with your supervisor before sharing your point of view. Immediate action by the Executive Director will be taken if an employee is found to be contravening communications policies.

7.   Protect EHCLA volunteers, learners, passengers and board members

Volunteers, learners, passengers and board members should not be cited without their approval. Never identify a learner or passenger by name without permission and never discuss confidential details of a learner, passenger or volunteer. It is acceptable to discuss general details about kinds of projects and to use non-identifying pseudonyms for a learner or passenger (e.g., a learner) so long as the information provided does not violate any non-disclosure agreements that may be in place with the individual or make it easy for someone to identify the person.

# Chapter 5: Communications Policies and Procedures

| Section: Communications Policy | Policy: Social Media Policy |
|---|---|
| Approved Date: September 23, 2019<br><br>Revision Date: September 24, 2020 | Policy Number: 5.1.3 |

8. Controversial Issues

If employees see misrepresentations made about EHCLA in the media, they may point that out. Always do so with respect and with the facts. If employees speak about others, make sure what they say is factual and that it does not disparage that party. Avoid arguments. Employees should make sure what they are saying is factually correct.

9. Correct Mistakes Quickly

If an employee makes an error, be up front about the mistake and correct it quickly. If an employee chooses to modify an earlier post, they should make it clear that they have done so. If someone accuses an employee of posting something improper (such as their copyrighted material or a defamatory comment about them), deal with it quickly - better to remove it immediately to lessen the possibility of a legal action. All instances must be reported to your supervisor.

10. Disclaimers

Many social media users include a prominent disclaimer saying who they work for, but that they're not speaking officially. This is good practice and is encouraged, but don't count on it to avoid trouble - it may not have much legal effect.

11. Enforcement

Policy violations will be subject to disciplinary action, up to and including termination for cause.

# Chapter 5: Communications Policies and Procedures

| Section: Communications Policy | Policy:   Data Security Policy |
|---|---|
| Approved Date: September 23, 2019<br><br>Revision Date: September 24, 2020 | Policy Number:     5.1.4 |

**Policy**

EHCLA is committed to protecting the privacy of the personal information of its employees, volunteers, members, learners, passengers, donors and other stakeholders. We value the trust of those we deal with, and of the public, and recognize that maintaining this trust requires that we be transparent and accountable in how we treat the information shared with EHCLA.

EHCLA frequently gathers and uses personal information. Anyone from whom such information is collected should expect that it will be carefully protected and that any use of this information is subject to consent.

**Defining Personal Information**

Personal information is any information that can be used to distinguish, identify or contact a specific individual. This information can include an individual's opinions or beliefs, as well as facts about, or related to, the individual. Exceptions include business contact information and certain publicly available information, such as names, addresses and telephone numbers as published in telephone directories, are not considered personal information.

Information in the public domain is not subject to privacy legislation and as such is not included in this policy.

Where EHCLA learners and passengers use their home contact information as business contact information, EHCLA considers that the contact information provided is business contact information and is not therefore subject to protection as personal information.

EHCLA always considers donor and volunteer information to be personal information and does not disclose information about donors or volunteers without consent.

EHCLA observes the following practices when collecting, maintaining and using personal information:

# Chapter 5: Communications Policies and Procedures

| Section: Communications Policy | Policy:   Data Security Policy |
|---|---|
| Approved Date: September 23, 2019<br><br>Revision Date: September 24, 2020 | Policy Number:     5.1.4 |

**Procedure**

1. Consent

An individual's consent is required regarding the collection and proposed use of personal information when information is collected. Consent can be either expressed or implied and can be provided directly by the individual or by an authorized representative.

2. Cookies

EHCLA's websites use persistent cookies within visiting browsers to enable the functions of the website and for tracking performance. Specifically, cookies are used the following ways:

- Preserving and expiring visitor sessions on the site (e.g. preserving data between steps of a process; and ending the session after a period of inactivity)
- Storing font size preferences on the site
- Enabling web analytic tools

Cookies are used anonymously and without storing Personally Identifiable Information (PII). Visitors that wish to opt-out of cookies should review the help documentation for their browser software to decline or selectively decline cookies. Note that declining cookies may adversely impact site performance.

3. Website, MailChimp and Facebook Analytics

EHCLA's website uses Google Analytics to track performance. Google Analytics uses persistent cookies to track visitor sessions, visitors across multiple sessions, and referral sources to our sites. In compliance with the Google Analytics Terms of Service, at no time is personally identifiable information (PII) passed to Google Analytics. Note that Google Analytics stores its data within the United States of America and is subject to US laws.  We use this data to understand site performance to serve you better.  Those wishing to opt out of Google Analytics data collection should use the Google Analytics Opt-out Browser Add-on.

EHCLA's Facebook page also uses analytics to track followers, likes and shares. The same is the case with our MailChimp email. EHCLA uses this data to understand Facebook and MailChimp performance to serve clients and subscribers better.

# Chapter 5: Communications Policies and Procedures

| Section: Communications Policy | Policy:   Data Security Policy |
|---|---|
| Approved Date: September 23, 2019<br><br>Revision Date: September 24, 2020 | Policy Number:     5.1.4 |

4. Limited Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

5. Accuracy

Personal information shall be as complete, accurate and up-to-date as possible

6. Security Safeguards

Personal information gathered by EHCLA shall be kept in confidence. EHCLA personnel shall be authorized to access personal information based only on their need to deal with the information for the reason(s) for which it was obtained.

Appropriate physical and electronic measures shall be used to ensure personal information is secure. Access to records shall be limited to those who require such information to fulfil their job responsibilities.

7. Confidentiality

Donors who request that their name and/or the amount of the gift not be publicly released shall remain anonymous.

8. Openness

Upon request, individuals shall be given access to the information in their donor record.

Further information on privacy and your rights in regard to your personal information may be found on the website of the Privacy Commissioner of Canada at www.priv.gc.ca.

# Chapter 5: Communications Policies and Procedures

| Section: Communications Policy | Policy: Crisis Communication Policy |
|---|---|
| Approved Date: September 23, 2019<br><br>Revision Date: September 24, 2020 | Policy Number: 5.1.5 |

**Policy**

EHCLA will effectively manage communications through a formal, clearly defined channel in order to mitigate crisis, or serious negative repercussions for EHCLA and maintain a reputation of leadership and transparency on vital issues.

**Procedure**

1. All crises should be reported to the Executive Director immediately.

2. The Executive Director is authorized to release information to the media and to the public. All other staff, board and committee members should be professional and helpful to the media by connecting them with the Executive Director, but will neither speak to the media, nor provide any information. If the Executive Director is unavailable, the Board Chair should be contacted.

3. All comments should be guided by professionalism and transparency, and serve to mitigate the crisis while reinforcing the leadership role of EHCLA.

4. Personnel matters are to remain confidential.

5. When possible, responses should be proactive, responsive, and action-oriented.

6. EHCLA recognizes the importance of media relation to public trust. In times of crisis, maintaining effective media relationships will be particularly critical in bolstering public confidence in the sector as a whole.

# Chapter 5: Communications Policies and Procedures

| Section: Communications Policy | Policy:   Crisis Communication Policy |
|---|---|
| **Approved Date: September 23, 2019**<br><br>**Revision Date: September 24, 2020** | **Policy Number:     5.1.5** |

**Preparation for a crisis in the future**

1. Disseminate an emergency list with phone numbers, cell phones, and email addresses for staff and board.  To be completed by assigned staff and updated quarterly or more frequently as needed by staff turnover and contact changes.

2. Perform annual communication audit and Strength Weakness Opportunity and Threat (SWOT) analysis.

3. Keep contact information for key audiences updated so that they can be easily contacted in a crisis.

4. Emergency Personnel* – Maintain contact information for police, fire, hospitals, the health department, utilities and paramedics. Make sure staff know how to access the information.

5. Off Site Alternatives – Determine a location to convene and/or from which to stage communications if the crisis situation prevents staff from getting to or using the office.

6. Equipment – Identify resources necessary prior to a crisis including extra cell phones, computers, etc. Determine how that equipment would be gathered and who would be responsible for operation.