



**Centre canadien
de l'agrément**

*L'excellence en matière de
services communautaires*

**Canadian Centre
for Accreditation**

*Excellence in
community services*

General Organizational Policies and Procedures

ORG – 01 Commitment to Inclusiveness and Accessibility	1
ORG – 02 Management of Information including Confidentiality	6
Appendix # 1 to Policy ORG-02: Schedule of Retention of Information Collected and Resulting from CCA Reviews	11
Appendix #2 to Policy ORG-02: CCA Oath of Confidentiality.....	12
Appendix #3 to Policy ORG-02: Privacy Guidelines for Organizations Preparing for Accreditation.....	13
Appendix #4 to Policy ORG-02: Suggested Participating Organization Confidentiality Agreement for use with Accreditation Reviewers.....	16
ORG – 03 External Complaints about CCA.....	17
ORG – 04 Access to CCA Information and Educational Resources	21
ORG - 05 Use of CCA Information and Communication Technology (CCA ICT).....	24
ORG – 06 Review and Revision of CCA Policies.....	33
ORG - 07 Risk Management Framework	34



Section	General Organizational Policies & Procedures
No.	ORG-01
Title	Commitment to Inclusiveness and Accessibility
Approval date	April 18, 2012
Approved by	Executive Director
Dates of revision	August 10, 2016 February 28, 2017
Date Reviewed	May 18, 2016 January 30, 2020

ORG - 01 Commitment to Inclusiveness and Accessibility

Scope

This policy applies to all employees, volunteers and agents.

Purpose

CCA is committed to an inclusive framework where our behaviours and actions reflect our fundamental beliefs of trust, mutual respect and dignity for all individuals. Inclusion means an environment where each person has an opportunity to participate fully in creating success and is valued for her/his distinctive skills, experiences and perspectives. Such an inclusive, accessible environment that values differences motivates Board members, staff and volunteers to contribute their best.

We believe that diversity and inclusion are key drivers of creativity and innovation. Diversity includes individuals from different nations, cultures, ethnic groups, gender and sexual orientations, generations, backgrounds, skills, abilities and all the other unique differences that make each of us who we are.

Definitions

Disability – A disability, as defined by the *Accessibility for Ontarians with Disabilities Act*, includes physical, mental health, developmental and learning disabilities. Disabilities come in many different forms, sometimes obvious and sometimes not. Disabilities may be visible or invisible, they may differ in severity, and the effects of a disability may be continuous or intermittent. For example:

- A person with a brain injury has a disability that is invisible.
- A person with arthritis has a disability that over time may become more severe.
- A person with multiple sclerosis has a disability that may sometimes affect daily routine and other times not.

The impact of a disability depends on the person's ability to access services, assistive devices, transportation, education and employment.

Participating Organizations (POs) – Organizations that have agreed to participate in the CCA accreditation program or other CCA services.

Policy

1. Inclusiveness

- 1.1. CCA will provide an environment that supports inclusive principles and practices and will strongly encourage such an environment in its Members and POs.
 - a CCA, including staff and volunteers, will not tolerate actions that contravene the principles of inclusion.
 - b CCA, including staff and volunteers, will not violate those principles through inappropriate limitation of employment opportunity, access to services or participation in any CCA activity.
 - c CCA works to increase access and participation, especially for those who are marginalized, disadvantaged or oppressed.
- 1.2. CCA will work to ensure that the structure, systems and policies of the organization reflect the organizations and communities served and will encourage equal access to all.
 - a CCA must attract, develop, promote and retain a diverse workforce in order to better fulfill our mission and most effectively address our audiences.
 - b CCA staff and volunteers are expected to conduct themselves professionally, in a manner befitting the work environment and with respect for colleagues and co-workers.
 - c CCA staff and volunteers are expected to understand that behaviour which one individual considers innocent and harmless may be regarded as oppressive by another person.
 - d CCA does not tolerate discriminatory or oppressive behaviour.

2. Accessibility

- 2.1. CCA is committed to achieving a fully accessible organization. To achieve this commitment, all CCA staff, contractors, volunteers and students share in the responsibility for advancing accessibility by playing unique and important roles in removing and preventing barriers to participation. CCA strives at all times to provide its programs in a way that respects the dignity and independence of people with disabilities. CCA is committed to giving people with disabilities the same opportunity to access and benefit from the same programs and services, in the same place and in a similar way as other service users.
- 2.2. This policy outlines CCA responsibilities in providing programs and services to people with disabilities in compliance with the Accessibility for Ontarians with Disabilities Act, (2005), Accessible Customer Service Standard.

Procedures: Accessibility Policy

CCA is committed to excellence in serving all program participants, including people with disabilities. This commitment is demonstrated in a variety of ways that are detailed below.

1. Communication

- 1.1. CCA personnel shall communicate with people with disabilities in ways that take into account their disability by asking how they can help and taking guidance from the person with whom they are communicating.

2. Telephone Services

- 2.1. Accessible telephone service is provided to service users within the scope of CCA's resources.
- 2.2. When communicating with program participants, personnel shall speak clearly and at a pace the person can understand.
- 2.3. If telephone communication is not suitable to a person's communication needs or is not available, communication with service users can be done through secure e-mail, written means, or relay services and TTY services where a TTY machine is available.

3. Assistive Devices

- 3.1. Personnel are responsible for identifying the types of assistive devices program participants may use while accessing CCA programs and developing a familiarity with these devices.

4. Invoicing

- 4.1. CCA is committed to providing accessible invoices to all organizations which access fee-charging programs.
- 4.2. Invoices shall be made available in a range of accessible formats including hard copy or secure e-mail. Upon request invoices shall be created in large print.
- 4.3. Staff shall answer any questions program participants may have about the content of the invoice in person, by telephone or via secure e-mail.

5. Use of Service Animals

- 5.1. CCA welcomes people with disabilities who are accompanied by a service animal.
- 5.2. At no time shall a person with a disability who is accompanied by a service animal be prevented from having access to their service animal.

6. Use of Support Persons

- 6.1. CCA welcomes people with disabilities who are accompanied by a support person.
- 6.2. At no time shall a person with a disability, who is accompanied by a support person, be prevented from having access to his or her support person while on our premises.
- 6.3. In some circumstances, CCA may require a support person to accompany a person with a disability. Before making a decision about a support person for the person with a disability, staff must:
 - Consult with the person with a disability to understand their needs
 - Consider health or safety reasons based on available evidence
 - Determine if there is no other reasonable way to protect the health or safety of the person or others
- 6.4. Support persons who participate in a program for the purposes of supporting a person with a disability shall not be charged a fee.

7. Notice of Temporary Disruption

- 7.1. In the event of a planned or unexpected disruption, CCA shall provide program participants with as much advance notice as is reasonable.
- 7.2. This notice shall include information about the reason for the disruption, its anticipated duration and a description of alternative facilities or services, if available.
- 7.3. The notice shall be placed on CCA's website, at all public entrances and at reception counters on CCA premises. If participants will not reasonably have had access to notifications through these means, personnel shall make every effort to contact them by phone or e-mail to inform them of the disruption.

8. Training for Personnel

- 8.1. CCA shall ensure that all board members, staff, contractors, volunteers and students have received training on accessible customer service requirements and how to interact with people with different disabilities.
- 8.2. The following people/positions shall take lead responsibility with respect to this:
 - a The Executive Director shall ensure all new board members and newly hired staff members have undergone training as part of their orientation.
 - b The Accreditation Manager shall ensure all reviewers have undergone training as part of their orientation to their placement with CCA.
 - c The Office Manager shall ensure all administrative volunteers have undergone training as part of their orientation to their position.
- 8.3. Training shall include the following:
 - a the purposes of the Accessibility for Ontarians with Disabilities Act, 2005;
 - b overview of the requirements of the Customer Service Standard;
 - c CCA's policy on providing accessible customer service;
 - d Tips on how to interact with people with various types of disabilities;
 - e Tips on how to interact with people with disabilities who use an assistive device or require the assistance of a service animal or a support person;
 - f Information on how to use any equipment or devices available in your organization to help provide goods, services or facilities to people with disabilities;
 - g Tips on what to do if a person with a disability is having difficulty in accessing CCA's programs.

This training shall be accessed electronically at the following website:

Serve-Ability: Transforming Ontario's Customer Service

<http://www.mcass.gov.on.ca/mcass/serve-ability/splash.html>

- 8.4. Board members, staff, students and volunteers shall report completion of this training to the appropriate person, as indicated in section 8.2, within three months of their date of hire/placement.

9. Feedback, Complaints and Questions

- 9.1. Feedback, complaints and questions shall be addressed according to CCA's *Feedback and Complaints Policy and Procedures*.
- 9.2. CCA ensures that the feedback process is accessible by providing or arranging for accessible formats and communication supports, on request.

10. Modifications to CCA Policies

- 10.1. All policies about CCA shall respect and promote the dignity and independence of people with disabilities. Any that do not do so shall be reviewed and a decision shall be made about whether it shall be modified or removed.

Other websites of interest include:

Accessibility for Ontarians with Disabilities Act (AODA)

<http://www.aoda.ca/>

Accessibility Laws

<https://www.ontario.ca/page/accessibility-laws>

Accessibility Rules for Businesses and Non-Profits

<https://www.ontario.ca/page/accessibility-rules-businesses-and-non-profits>

Accessible Customer Service Policy Template

<https://www.ontario.ca/page/accessible-customer-service-policy-template>

Accessibility Compliance Reporting

http://www.opsba.org/index.php?q=system/files/2015BPS_AccessibilityReportQuestionnaire50.pdf

<https://www.ontario.ca/page/how-complete-your-accessibility-compliance-report>

Accessibility for Ontarians with Disabilities Act (AODA)

Contact Centre (Service Ontario)

Toll-free: 1-866-515-2025

1-416 849 8276

Fax: 416-325-9620

TTY: 416-325-3408 / Toll-free: 1-800-268-7095

Accessibility Directorate of Ontario

601A-777 Bay Street

Toronto, ON M7A 2J4



Section	General Organizational Policies & Procedures
No.	ORG – 02
Title	Management of Information including Confidentiality
Approval date	April 18, 2012
Approved by	Executive Director
Dates of revision	July 25, 2012 November 3, 2014 February 28, 2017
Date Reviewed	January 30, 2020

ORG - 02 Management of Information including Confidentiality

Scope

This policy applies to all employees, volunteers and agents.

Purpose

This policy describes CCA expectations concerning management of information in a safe and secure manner that protects privacy and confidentiality of CCA and our stakeholders.

In the process of conducting accreditation reviews, CCA identifies documents that demonstrate good practice in organizational and program policy, planning and management. By sharing this information, CCA is contributing to the learning and development of not-for-profit organizations, consistent with the CCA mission. CCA will seek to create a variety of opportunities for building the capacity of not-for-profit organizations, including promoting sharing of examples of good policies, procedures and tools.

Definitions

Participating Organizations (POs) – Organizations that have agreed to participate in the CCA accreditation program or other CCA services.

Policy

CCA produces information to support its corporate operations. Section 1 of this policy outlines handling, storage, security, retention and disposal procedures related to this information.

CCA also collects information from organizations for the purpose of conducting CCA reviews and making accreditation decisions. Section 2 of this policy addresses safeguarding and using this information, specifically:

- storage, security, retention and disposal of Participating Organizations' information;
- sharing of Participating Organizations' information.

The information collected from organizations is for the purpose of conducting CCA reviews and making accreditation decisions as stipulated in the CCA Accreditation Agreement. Therefore, explicit permission is required for CCA to use Participating Organization's policies, procedures or tools to share with other organizations. These documents will be used in a way that protects the anonymity of individuals and positions in organizations.

1. Policies and Procedures related to CCA's own Corporate Information

1.1. CCA generates information to support the functioning of its board of directors and staff. Information includes documents and data recorded on paper, computer hard drives and other means of electronic storage (e.g., memory keys/flash drives). CCA personnel and board members shall be guided by the following procedures for the handling (including disposal), retention and storage of this information.

a Handling of materials:

- Sign and respect the Oath of Confidentiality (Appendix #2) acknowledging that all information obtained in the course of their work for CCA is confidential, except for materials produced for distribution to the public.
- Keep documents in safe, dry and secure locations. Secure locations in workplaces include locked rooms, cupboards or filing cabinets. Homes and vehicles that are locked are considered to be secure locations.
- Exercise due diligence to ensure that documents are safeguarded, for example, by not leaving documents in locations where they can be viewed on desktops, computer screens, etc.
- Transport, courier or convey information using various secure means (e.g., courier services, airplanes, trains, taxicabs, private automobile, secure e-mail to which only the recipient has access).
- Return CCA documents to CCA for secure disposal or ensure they are disposed of in a secure manner.

b Retention and Secure Disposal:

- A copy of Board minutes and AGM minutes will be retained for CCA's life span plus two years.
- Annual audited financial statements, general ledger and annual adjusting journal entries will be retained for the CCA's life span plus two years.
- Financial records, including general ledgers and payroll information, will be retained for a minimum of six years from the end of the fiscal period to which they relate.
- Insurance policies will be retained indefinitely.
- Human resource records will be retained for three years after termination of employment.
- The disposal of confidential corporate documents must occur in a manner to preserve confidentiality, i.e., if hard copy, by having the documents shredded. If a third party is engaged to dispose of confidential corporate documents, CCA shall have an agreement with the third party to ensure disposal in a confidential manner.

c Storage:

- Electronic and paper records shall be stored in dry, safe and secure locations.
- In particular, the following shall be stored in a location where they could be accessed on fairly short notice (within two days): all deposit books with documentation supporting from whom funds were received and to what they relate, record of all cash disbursements, proof of payment (e.g., cancelled cheques), invoices, documents substantiating disbursements, payroll records, donation receipts and supporting documentation.

- One paper copy of approved Board and AGM minutes shall be retained in a fireproof safe or filing cabinet.
- At least one current (one day old) back-up copy of electronic documents shall be maintained. One electronic back-up copy shall be held in the fire proof cabinet.

1.2. Ensuring confidentiality of Board of Directors' Documents

- a The safety and protection of confidential Board documents is critical. Confidential Board documents include, but are not limited to, the following:
 - minutes of "in camera" Board meetings;
 - minutes of "in camera" Board committee meetings;
 - special confidential reports and correspondence;
 - confidential documents pertaining to the employment of the Executive Director, including: letters of employment, disciplinary letters, performance appraisals, salary-related correspondence.
- b Documents that are identified by the Board as confidential are to be put into a sealed envelope with the date noted on the outside and Board Officer's signature over the seal, and stored on the CCA premises in the CCA Board Minutes safe. These documents shall only be made available to current or future board members as requested.

2. Policies related to Information gathered from Participating Organizations (POs)

- 2.1. Other than information that is publicly available, the information obtained from POs is confidential and is to be used only for accreditation reviews, decision making and the evaluation of the accreditation process as stipulated in the CCA Accreditation Agreement. All precautions reasonable under the circumstances are taken to protect POs' confidential information and ensure that paper and electronic information is stored in dry, safe and secure locations and that confidential materials submitted online for review are on Canadian servers.
- 2.2. Information includes documents and data recorded on paper, computer hard drives and other means of electronic storage (e.g., CDs, memory keys/flash drives). This information may include names of board and staff members within documents (e.g., board and staff minutes) and contact information for board and staff members that is used to conduct CCA surveys and the evaluation of the CCA accreditation process.
- 2.3. In keeping with CCA's Oath of Confidentiality, CCA staff, board members, review team members and external agents are required to treat as confidential *"any information about an organization participating in the accreditation program or any other organization"*.
- 2.4. Documents that may be collected from POs are destroyed in a secure manner. For historical purposes, including evaluation and monitoring of the CCA accreditation process, results from reviews are retained according to CCA's retention schedule (see Appendix #1).
- 2.5. CCA staff and review team members will undertake measures to safeguard this information, as outlined in the procedures below.
- 2.6. It is the obligation of all POs to inform their clients that their personal health information may be disclosed to an on-site accreditation review team as part of the CCA Accreditation Program. Guidelines for POs about the privacy of personal information and personal health information are provided in Appendix. Although the Ontario Personal

Health Information Protection Act provides for disclosure of personal health information during an accreditation review, it is recommended that each PO require members of the CCA site review team to sign the PO's confidentiality agreement (Suggested procedures and format in Appendices #3 and #4).

Procedures: Information Gathered from POs

1. Safeguarding Participating Organizations' Information

1.1. In the process of preparing for and conducting reviews, writing reports and communicating about accreditation decisions, CCA staff, board members and review team members:

- Sign and respect the CCA Oath of Confidentiality acknowledging that all information obtained in the course of conducting a review shall be used only for the purpose of conducting the review and for making an accreditation decision.
- Keep documents in safe, dry and secure locations. Secure locations in workplaces include locked rooms, cupboards or filing cabinets. Homes and vehicles that are locked are considered to be secure locations.
- Exercise due diligence to ensure that documents are safeguarded, for example, by not leaving documents in locations where they can be viewed on desktops, computer screens, etc.
- Keep at least one back-up of electronic documents that are not saved in the CCA Accreditation Web tool.
- May transport, courier or convey information using various means (e.g., courier services, airplanes, trains, taxicabs, private automobile, secure e-mail to which only the recipient has access).
- Will refer questions about a PO's affairs to the organization itself, and will not convey such information to any other party without the PO's consent.
- Safely destroy their own copies of PO's documents and their own notes within two months of the final accreditation decision.
- If the review site visit includes a review of the PO's client or human resource files, the reviewer will not remove any personal health information or other personal information from the organization, including copies thereof, and will not make any notes that may identify a client or employee.

1.2. To safeguard POs' information, CCA will:

- Once the final accreditation decision has been made, securely dispose of original staff, client, volunteers, student, board, community and educational partner survey responses;
- Ensure electronic and paper documents are stored in dry, safe and secure locations;
- Ensure regular back-up copies of electronic information are stored in safe, dry and secure locations;
- Maintain a schedule for the retention and disposal of information related to the accreditation process and comply with the schedule (see Appendix).
- Any third party service that is used to store confidential PO information will ensure that information is stored on Canadian servers and CCA will have agreements in place to assure secure and confidential handling of all information and regular back-up.

- The disposal of confidential PO information must occur in a manner to preserve confidentiality, i.e., if hard copy, by having the documents shredded. If a third party is engaged to dispose of confidential PO documents, CCA shall have an agreement with the third party to ensure disposal in a confidential manner.

2. Using Participating Organization's Information as a Resource

2.1. Once a PO's policies, procedures or tools are selected to be shared, the following procedure is used to secure permission:

- Following the accreditation decision, correspondence is prepared to request permission to use an organization's documents. The correspondence (by email is satisfactory) is directed to the Executive Director and lists the specific policies, procedures and tools of interest.
- If the organization responds positively in writing (email message is satisfactory), CCA uses the source information as agreed.
- CCA credits the organization according to its preferences.

2.2. Organizations requesting and making use of documents from CCA are asked to credit the source of documents (i.e., CCA and, if applicable, the specific organization from which the document originated) and to indicate whether these are used in their entirety or in part, or modified or adapted (e.g., a human resources policy about overtime; a format or structure for planning; an adaptation of a pictorial representation of a process; a questionnaire modified for a particular type of health-promotion workshop).

Appendix # 1 to Policy ORG-02: Schedule of Retention of Information Collected and Resulting from CCA Reviews

Information includes documents and data recorded on paper, computer hard drives and other means of electronic storage (e.g., memory keys/flash drives). This information may include names of board and staff members within documents (e.g., board and staff minutes) and contact information for board and staff members that is used to conduct the evaluation of the CCA accreditation process.

Type of Document	Process	Timeframe for Retention
Electronic documents submitted by organizations for CCA reviews (entered on CCA Web tool, emailed to CCA or submitted on paper).	Following the final accreditation decision, CCA will keep these documents until after the next accreditation decision is concluded. Following this period CCA will securely destroy the organization's documents.	Retained until after the following CCA accreditation decision is concluded.
Information resulting from accreditation reviews including preliminary reports, final reports, databases, summaries of survey results, agreements with POs, conflict of interest.	CCA stores information in a safe, secure location for reviews resulting in full, conditional or no accreditation. Only the Final Report and agreements with the PO are retained after the following accreditation decision is completed by CCA.	Retained until after the following CCA accreditation decision is concluded.
Original survey responses.	Following the final accreditation decision, survey responses are destroyed.	Disposed securely on a regular quarterly basis (Jan 1, April 1, July 1, October 1) for those accreditation decisions made in the previous quarter.
Documents created and used by reviewers in the review process (including personal notes, draft reports, etc.).	Documents are disposed of by reviewers in a secure manner.	Disposed securely by reviewers within two months of the final accreditation decision.
Record of Organization's permission to retain organization's policies/procedures, etc.	CCA stores information in a safe, secure manner and/or location.	Retained for the life of CCA, plus 2 years.



Canadian Centre for Accreditation

Excellence in community services

Centre canadien de l'agrément

L'excellence en matière de services communautaires

OATH OF CONFIDENTIALITY

I, _____, shall treat as confidential any information of a character confidential to the affairs of the Canadian Centre for Accreditation (CCA) and any information about an organization participating in the accreditation program or any other organization, to which I become privy as a result of my role in the CCA accreditation program. Following an accreditation decision, I will continue to treat as confidential any information confidential to the affairs of these organizations.

I understand that disclosure of such information may result in termination of my responsibilities. I also understand that this obligation extends beyond the end of my tenure as a board member, reviewer, contractor or staff of CCA.

Signature

Date

Appendix #3 to Policy ORG-02: Privacy Guidelines for Organizations Preparing for Accreditation

These guidelines and sample agreement were developed by CCA to inform Participating Organizations on the privacy requirements related to the accreditation process. This is provided for reference only. Participating Organizations should always consult legislation in their jurisdiction prior to creating their own policies and procedures.

Organizations preparing for CCA accreditation are encouraged to proactively create systems that inform clients and obtain their consent for accreditation team members to see their confidential files.

All CCA review site visits involve some access by the review team to client files. The review process in certain sectors involves more extensive client file reviews than others. CCA reviewers sign an oath of confidentiality with CCA that commits them to respecting the privacy of organizations and their clients and specifically prohibits any client-identifying information from circulating outside the organization being reviewed.

1. Best Practice Guidelines: Organizations/Services that Must Comply with Ontario's Personal Health Information Protection Act, 2004 (PHIPA)

Introduction

Section 39(1)(b) of Ontario's Personal Health Information Protection Act, 2004 (PHIPA) states that health information custodians may generally disclose their clients' personal health information to a person conducting an accreditation review of their services. Specifically, any on-site disclosure of personal health information that is made as part of an accreditation review would be permissible. Under PHIPA, if any personal health information is to be taken off-site, a separate agreement must be entered into between the health information custodian and the reviewing party. However, CCA policy does not permit reviewers to take personal health information off-site.

Moreover, section 10 of PHIPA requires that health information custodians inform clients of their information practices. All Participating Organizations must inform clients that their personal health information may be disclosed to an on-site accreditation review team as part of the CCA Accreditation Program. This information may be communicated to clients in a variety of ways, including orally, through a consent form or in a privacy policy.

In the event that a client informs an organization that he/she does not want his/her personal health information to be disclosed as part of an accreditation review, this request must be adhered to and a notation made in the client's health record.

Guidelines re: Informing Clients about Accreditation in relation to their Personal Health Information

Organizations have two options to consider in determining how to inform clients that their personal health information may be disclosed to an on-site review team for the purposes of the CCA Accreditation Program. Both of these options are considered best practices.

Option 1:

Inform clients at the start of service that their personal health information may be shared with an on-site review team as part of the CCA Accreditation Program. A signed consent is optimal, but not required. If an organization chooses to obtain a signed consent, it is not recommended that a separate consent form be prepared. Rather, all information regarding the accreditation review should be included in the organization's general consent form that is provided to clients when they first begin service.

Option 2:

The organization outlines the CCA Accreditation Program and on-site review within the Privacy Policy. Organizations should confirm the need for the CCA Accreditation Program and on-site review process to take place in order to maintain the highest quality of service.

2. Best Practice Guidelines: Organizations Providing Social Services

For social service organizations that may not be health information custodians under PHIPA, but do deal with personal information (including health information) of clients, the same principles apply as in Part 1. In "A Legal Guide for Social Workers" (published in 2009 by Family Service Ontario and the Ontario Association of Social Workers), Robert Solomon, Professor at the University of Western Ontario's Faculty of Law, highlights the importance of explaining and expressly limiting the confidentiality obligations to a client at the initiation of service. The Legal Guide recommends that an organization providing service explains its confidentiality policies to clients at the outset of the relationship, including any situations in which client information will be disclosed to others and the rationale for those policies. Regarding accreditation, clients should be informed that their files may be reviewed by accreditation team members for purposes of conducting the accreditation as part of the agency's quality assurance processes.

In the event that a client informs an organization that he/she does not want his/her personal information to be disclosed as part of an accreditation review, this request must be adhered to and a notation made in the client's record.

3. Best Practice Guidelines: Personal Information of Employees, Foster Parents and Volunteers

Employees, volunteers and foster parents should be advised that their Human Resource file may be reviewed by an accreditation team member as part of an accreditation site visit, but that they have the opportunity to refuse to allow this. It is recommended that this be included as a routine item during the orientation process that takes place with all employees, volunteers and foster parents when they start their engagement with the organization and a human resource file is opened for them. The fact that this item is covered in the orientation should be documented in the individual's file.

4. Best Practice Guidelines: Confidentiality Agreements with Site Visit Accreditation Reviewers

An organization may wish to further emphasize its due diligence in the matter of confidentiality by having CCA reviewers sign an additional oath of confidentiality specific to any client or human resource information that reviewers may see or hear on the site visit.

The organizational confidentiality agreement should include the following information:

- A brief description of the Accreditation Program and on-site review
- The legislative authority for accessing personal health information, where applicable
- Confirmation that the personal health information and other personal information reviewed will not be disclosed to any other party and will only be used for the purposes of the Accreditation Program

- The on-site review team will not remove any personal health information or other personal information from the organization, including copies thereof, and will not make any notes that may identify a client, employee, foster parent or volunteer

Below is suggested wording for a Confidentiality Agreement that may be used by Participating Organizations for this purpose. Organizations may adapt this Agreement as they see fit.

Appendix #4 to Policy ORG-02: Suggested Participating Organization Confidentiality Agreement for use with Accreditation Reviewers

As part of an accreditation review of [INSERT NAME OF PARTICIPATING ORGANIZATION] (the Organization), which involves assessing the quality of its programs, management, governance and staffing against an established set of standards (the Accreditation Program), I will be part of a team of accreditation review experts conducting an on-site review of the Organization. To ensure that the Organization is maintaining all proper standards, I acknowledge and understand that during the course of the on-site review, it may be necessary to obtain access to and review the personal health information of the Organization's clients.

I acknowledge and understand that section 39(1)(b) of the Personal Health Information Protection Act (PHIPA) provides the authority for the Organization to disclose personal health information to a person reviewing an application for accreditation relating to services that it provides, such as the CCA Accreditation Program contemplated herein.

I acknowledge and understand that pursuant to section 10 of PHIPA, it is the legal obligation of the Organization to inform its clients of its information practices, which would include that their personal health information may be accessed for the purposes of an accreditation review such as the CCA Accreditation Program. I acknowledge and agree that in the event that it has been brought to my attention that any client of the Organization has specifically requested that their personal health information not be disclosed for the purposes of the CCA Accreditation Program, the personal health information of such a person will not be accessed.

I confirm that no personal health information, in any form, including copies thereof or any notes that may identify a client, will be removed from the Organization without the express written consent of the Organization and a confirmation that the information will be held in a secure and confidential manner and will be returned when the CCA Accreditation Program is complete.

I confirm that none of the personal health information that may be accessed as part of the on-site review will be disclosed to any other party or used for any purpose outside the scope of the CCA Accreditation Program, under any circumstances.

I confirm that to the extent that other personal information may be accessed as part of the on-site review, such as information about the families of the Organization's clients or information about the Organization's employees, directors or other related parties, this information will not be disclosed to any other party or used for any purpose outside the scope of the CCA Accreditation Program, under any circumstances.

Name:

Signature:

Date:

Witness:



Section	General Organizational Policies & Procedures
No.	ORG-03
Title	External Complaints about CCA
Approval date	April 18, 2012
Approved by	Executive Director
Dates of revision	January 20, 2016 February 28, 2017 January 30, 2020
Date Reviewed	January 30, 2020

ORG - 03 External Complaints about CCA

Scope

This policy applies to all employees, volunteers (including CCA reviewers) and agents.

Purpose

The purpose of this policy is to outline the process by which CCA will address complaints made by external sources about its services and operations.

Definitions

Member Associations – Associations that are members of CCA as described in the CCA Bylaws.

Participating Organizations (POs) – Organizations that have signed an agreement to participate in the CCA accreditation program or other CCA services.

Policy

As an organization interested in continuous quality improvement, CCA will view complaints and concerns as a learning opportunity. Complaints will be investigated and responded to in an expedient manner.

1. Principles

- 1.1. An individual or organization with a complaint has the right to have his/her/its complaint reviewed in a timely manner without fear of embarrassment or reprisal.
- 1.2. Individuals who are the subject of a complaint have the right to be informed of allegations and afforded the opportunity to respond to them.
- 1.3. The values that govern CCA will guide the complaints resolution process.
- 1.4. In reviewing the complaint, the CCA Executive Director and/or Board Executives will ensure that the parties involved in the complaint are given fair opportunity to explain their perspectives.
- 1.5. If the complaint is about a CCA accreditation review process, every effort will be made by CCA to ensure a fair accreditation review process. The Complaints process is not to be used for disagreements about the findings of an accreditation process, as these matters should be dealt with through the organization's response to their Preliminary Report or by accessing CCA's Appeal Process after the Final Report.

1.6. All materials and information relating to the complaint and any resulting investigation will be treated as confidential and will not be shared except on a need-to-know basis.

2. Documentation and Reporting

2.1. Complaints received will be recorded using the *Complaint Investigation Documentation Form* (see Appendix). All documentation is stored in the Complaints Folder with copies in the organization's folder (if applicable). If the complaint is verified as valid, the *Documentation Form* shall also be saved on the file of the individual who is the subject of the complaint (i.e., a CCA staff person or reviewer). Complaints are stored for four years. The Executive Director monitors all complaints and CCA Staff review them semi-annually for any trends. The Executive Director shall report to the board on an annual basis the number and type of complaints received and their resolution. In addition, the Executive Director will report to the board in a timely manner any complaints that pose a risk to the organization.

Procedures: External Complaints

1. Complaints related to individual CCA staff, contractors, volunteers (including CCA reviewers) or board members

1.1. Contacts made to CCA with a concern/complaint about CCA shall be acknowledged within 5 working days. This means that at minimum, a CCA staff person will contact the person to set up a time when they may speak to the CCA Executive Director to discuss their concern/complaint.

1.2. The individual with the complaint will first be encouraged to express the complaint to the individual most directly involved in the situation. This is important in terms of ensuring that every attempt has been made to resolve the complaint in a direct, open and constructive manner.

1.3. If expressing the complaint to the individual involved is not feasible, or if doing so does not resolve the complaint, the individual is encouraged to express the complaint to the CCA Executive Director (or designate) or, in the case of a CCA board member, to the Chairperson of the CCA Board of Directors.¹ The Executive Director/Board Chairperson will respond to the complaint in writing within one month of receiving it.

1.4. If the complaint is about an accreditation review process that is underway, a more immediate response shall be taken and the complaint will be investigated immediately. When a complaint is found to be valid, the Accreditation Specialist, in consultation with the Executive Director, will develop and implement a corrective action plan as soon as practically possible and will communicate this to the complainant as appropriate. Corrective action may include a change of review team member if deemed necessary.

1.5. If the complaint is in regard to the Executive Director and/or the Executive Director is unable to resolve the situation to the individual's or organization's satisfaction, the individual/organization involved may proceed to the next step and submit their complaint to the Chairperson of the CCA Board of Directors.

1.6. The Board Chairperson will refer the complaint to the other Board Executives, who jointly will conduct an investigation of the complaint and provide a written response to the individual/organization involved within two months of receiving the complaint.

¹ Note: It is understood that it would be difficult for an individual at an organization undergoing an accreditation review to complain directly to one of the CCA review team members, therefore, in this situation the complaint would be directly accepted by the Executive Director or designate.

- 1.7. If the complaint is in regard to the Board Chairperson, it will be referred to the Vice Chairperson of the board. The Vice Chairperson shall constitute an ad hoc committee of board members to investigate the complaint and provide a written response to the individual/organization involved within two months of receiving the complaint.
 - 1.8. Complainants and those who are a subject of a complaint shall be advised of progress in the investigation process and the outcome of the process.
 - 1.9. Depending on the nature of the complaint and the outcome of the complaint investigation, a decision may be taken to take follow-up action. (If the complaint pertains to staff, please refer to Human Resource Policies - Disciplinary Action, or if a Reviewer, see Human Resource Policies - Reviewers.)
2. Complaints related to CCA Policies, Procedures or CCA Review Processes
 - 2.1. Contacts made to CCA with a concern/complaint about CCA Policies or Procedures shall be acknowledged within 5 working days. This means that at minimum, a CCA staff person will contact the person to set up a time when they may speak to the CCA Executive Director to discuss their concern/complaint.
 - 2.2. Individuals or organizations with such a complaint are encouraged to initially express it to the CCA Executive Director in order to receive clarification of CCA policies, procedures and processes.
 - 2.3. If the complainant continues to have a concern, or does not wish to verbally express it to the Executive Director, they shall be encouraged by the Executive Director to submit the concern/complaint in writing.
 - 2.4. The Executive Director will review the written complaint and, if it involves board policies, will bring it forward for consideration to the Board Chairperson and/or a committee of the board as appropriate. The Board Chairperson or board committee (whoever is reviewing the complaint) shall investigate the complaint and respond in writing to the complainant within two month(s) of receiving the complaint in writing.
 - 2.5. The complainant shall be advised of progress in the investigation process and of the outcome of the process.

CCA Complaint Investigation Documentation Form

Date Complaint Received: Verbal Written *(attach document if written complaint)*

Complainant Name (Organization and/or Individual)

Phone Number: Email:

Address

Nature of complaint: *((Who, what, where, when and why) Provide details regarding the complaint and identify any staff or Board person or reviewer being addressed in the complaint)*

Follow up with Complainant: *(include name, time and any written documents, emails)*

Follow up with Subject of Complaint: *(include name, time and any written documents emails)*

Decision: *(Was complaint found to valid/verified or not)*

If Complaint is Valid/Verified - Action Plan:

(includes but is not limited to a review of practice, training, mentorship, and/or ongoing supervision and performance monitoring while still employed/engaged or may be suspended, include timelines in plan)

Feedback provided to Complainant – Date _____

Feedback provided to Subject of Complaint – Date _____

File CCA Complaint Folder – and if applicable copy to Organization’s Folder, and/or Staff/Reviewers Folder

Signature _____ Date _____



Section	General Organizational Policies & Procedures
No.	ORG – 04
Title	Access to CCA Information and Educational Resources
Approval date	January 11, 2013
Approved by	Executive Director
Dates of revision	February 28, 2017
Date Reviewed	January 30, 2020

ORG - 04 Access to CCA Information and Educational Resources

Scope

This policy applies to all directors, employees, volunteers and agents.

Purpose

This policy outlines conditions and guidelines for access to CCA Information and Educational Resources (hard copy and electronic versions), either through CCA Website or office.

The CCA Resources addressed in this policy are all the materials describing the CCA and its programs, resources for organizations participating in CCA reviews and CCA reviewers, resources for the public, including organizations interested or considering the CCA program. This policy does not address materials internal to CCA operations, that is, primarily for board and staff use. This policy does not deal with non-CCA-owned materials.

Definitions

Participating Organizations (POs) – Organizations that have agreed to participate in the CCA accreditation program or other CCA services.

Policy

1. CCA wishes to balance the protection of its intellectual property, with its goal of promoting quality improvement in community service organizations, by allowing access to CCA information and resources that would enable interested organizations and individuals to learn about the value of accreditation and the CCA program.
2. Information to be provided about the Accreditation Status of Participating Organizations: On CCA's website, CCA will publish only the names of all POs with current accreditations as of the date that the web listing is updated. The names of accredited POs may also be published in regular CCA newsletters or news bulletins.

The following will apply depending on the kinds of accreditation status that a PO may have other than full accreditation:

- if conditional accreditation, and PO is being accredited for the first time, publish only after full accreditation is granted;

- if conditional accreditation, and the PO has been previously accredited by CCA, keep the PO on the accredited list, unless a non-accreditation decision is made;
- if the PO has been granted an extension of their accredited status, their name will not be removed from the accredited list.

POs will be removed from the published list of accredited organizations if:

- the PO receives a decision to deny accreditation;
- the PO's accreditation status is rescinded (as per Policy ACC-11);
- the PO allows its accreditation to lapse.

If there is an enquiry about the accredited status of an organization:

The only information that CCA may disclose about the accredited status of a PO, is whether a PO is currently accredited by the CCA and the term dates of the accreditation. Unless an organization is currently accredited at the time of the enquiry, CCA will not affirm or deny that any organization is a Participating Organization with CCA or reveal that it may have undergone an accreditation review and is not accredited.

3. Access to CCA Resources will be according to the Table below. Each level proceeding down in this Table shall have access to the materials in the rows above. Any access to CCA Standards will be conditional on the understanding that it is protected intellectual property and users are not at liberty to circulate or copy it without permission.

Who May Access	What Materials/Resources	How accessed	Fee (where applicable)
Available to all – Public, including funders	<ul style="list-style-type: none"> - General Info about CCA and CCA Program (at least at Component level with short descriptors) - CCA Brochure, Annual Report, quarterly Newsletters - Information Sheets for eg. Why accreditation, benefits of CCA accreditation, descriptions of CCA program, general FAQs, etc - general CCA Fee scale (for orgs that are not part of CMHO or OACCS/ CACCS) 	<ul style="list-style-type: none"> - off website (pdf only) - by email - electronic format (pdf) - may be produced as hard copy handouts, could be mailed or distributed at mtgs, displays 	<p>Free of charge –</p> <p>Most often electronic pdf version that would be available from CCA website;</p> <p>Some hard copy Info Kits used for outreach to particular Orgs</p>
Continued: Available to all public for sale.	- CCA Organizational Standards Module with all Standards/ Indicators and CCA Accreditation Manual	- provide info about this option on website but require that purchaser submit purchase order through CCA office (not as a web sale)	Sell pdf copy only - charge \$350.
Continued: Available to all public for sale (Does not address non-CCA-owned materials)	Program Modules owned by CCA: <ul style="list-style-type: none"> - Community-Based Primary Health Care - Community Support Services - Community Mental Health and Addiction 	same as above	Sell pdf copy only – Charge \$150 for each Module.

Who can Access	What Materials/Resources	How accessed	Fee (where applicable)
Funders	- CCA Manual and CCA-owned Standards to be made available on request to funders free of charge.		Free of Charge
Interested Organizations (considering CCA accreditation)	- more detailed descriptions of the CCA Accreditation Program (but not at the indicator level), such as a description of what is included in the Components /Standards (some sample Standards) - info about CCA Fee schedule for accreditation program and other CCA services	- not available automatically off the website – but they would need to contact CCA for further info to get these – may be provided in pdf format.	Free of charge- electronic pdf version only
Organizations interested in CCA Accreditation but not yet ready to sign on and commit to a date (e.g., newer orgs)	- through CCA Preliminary Service - have access to CCA Resources for limited time period - access to full range of Modules applicable as per Prelim Service policy (hard copy and pdf) - access to CCA Resource Library - secure access code to CCA website		Preliminary Service Fee: \$1,000/yr (plus licensing fee for the program modules not owned by CCA)
Organizations signed on with CCA for accreditation	- all resources related to their review - CCA Policies & Procedures	- have Web portal access to resources and to provide information about their organization	Accreditation Fee (including license fee where this applies); no additional charge
All Reviewers	- additional info for Reviewers re: conducting a review; tools, rating scales, etc	- have Web Portal access to the Organizational info; access code for Reviewers section of website	Free of charge



Section	General Organizational Policies and Procedures
No.	ORG-05
Title	Use of CCA Information and Communication Technology
Approval date	January 28, 2016
Approved by	Executive Director
Dates of revision	January 30, 2020

ORG - 05 Use of CCA Information and Communication Technology (CCA ICT)

Purpose

The purpose of this policy and procedure is to provide direction and guidelines to employees, contractors or other authorized users concerning the use of CCA’s information and communication technology. This policy does not include access to the GoCCA Web Tool by authorized CCA reviewers and participating organizations.

Definitions and Acronyms

Electronic communications - Communications performed on workstations, networks, internet, social media and networking platforms, e-mail, peripherals, communication devices, switches, hardware, as well as related devices.

GoCCA Web Tool - A custom-developed web-based application enabling streamlined management of the accreditation process from start to finish, that is the main point of contact for participating organizations with CCA. The application stores and organizes participating organizations’ documents and information in a logical and secure way, then provides a straightforward way for authorized CCA staff and reviewers to review and assess the submitted information, enter decisions and notes and prepare reports. CCA contracts with a Canadian remote storage (cloud-based) provider to store this data securely.

Portable electronic and computing devices - A general term used to refer to a variety of portable technology devices, including but not limited to the following:

- Cellular/mobile phone, smartphone
- Computers including laptops, tablets/ipads
- Portable data storage device, including USB or flash drive, video, CD, DVD and digital memory card
- Portable hard drive and other mass storage device.

Participating Organizations (POs) – Organizations that have a current signed agreement with CCA to participate in the Accreditation Program or other CCA Services.

Shared Drive - Networked file storage areas accessible by more than one employee.

Virtual Private Network (VPN) - The network that uses the Internet to provide remote, secure access to CCA’s computer network from non-networked locations and equipment.

Procedure Introduction

This Procedure is based on and aligned with CCA Policy ORG-06 Management of Information (including Confidentiality).

CCA Information and Communication Technology (CCA CIT) Procedures apply to all CCA employees and other authorized users.

These Procedures cover the usage of all CCA ICT resources, whether the ICT resources and systems are resident at CCA or at any off-site locations, including but not limited to:

- all software including purchased or licensed business software applications, CCA-written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on CCA-owned equipment.
- all intellectual property and other data stored on CCA equipment plus any applicable process/procedure
- all hardware systems, including computers, workstations, portable electronic devices, networks, communication devices, switches, hardware and software programs, as well as related devices

The goal of these policies is to ensure that employees and other authorized users of CCA information and communication systems:

- experience uninterrupted access to administrative and operational data and systems
- trust the integrity of administrative and operational data and systems, and
- trust that sensitive information is treated with care.

CCA owns all information found in any of CCA's ICT resources. This includes, but is not limited to:

- All files and documents, including those found in the user's directories
- Messages found in users' CCA email accounts including those stored in personal folders

CCA ICT resources have been provided to assist CCA employees in their job duties and review processes. They are not for personal or commercial use. CCA reserves the right to access and monitor the use of these systems by employees (including accessing information on user directories and email folders) at any time upon approval of the Executive Director, or her/his designate, to determine compliance with this policy and to evaluate performance standards. Any personal messages, files, devices may be subject to inspection and removal. Use of CCA systems constitutes consent to security monitoring, and employees should remember that most sessions are not private.

Procedures

1. Acceptable and Prohibited use of CCA Information and Communication Technology

Users must report any weaknesses in CCA ICT security, and any incidents of possible misuse or violation of this procedure to the Executive Director or designate.

CCA ICT systems and data are for use only by the individual granted access and all user accounts will be protected with passwords. CCA employees may access CCA data and programs stored on CCA systems, except for two confidential drives (concerning human resources and finances) that are only available to the Executive Director. Users are to ensure that the CCA Office Manager is aware of their CCA account(s), passwords, security fobs or similar information or devices used for identification and authorization purposes. These are not to be shared with anyone beyond other CCA employees.

Users shall not make unauthorized copies of copyrighted software. Only CCA approved software can be installed on CCA hardware. Users are not to use non-standard shareware or

freeware software without the CCA-Administration approval unless it is on the CCA standard software list.

Users shall not purposely engage in activity that may:

- harass, threaten, shame or abuse others
- degrade the performance of the CCA ICT resources
- deprive an authorized CCA user access to any of the CCA ICT resources
- obtain extra resources beyond those allocated
- circumvent the CCA ICT security measures

Users are discouraged from accessing non-business related information and shall not access offensive, profane, pornographic, obscene, or harassing material. Employees who encounter such material downloaded from external sites should immediately report this to Office Manager.

Users shall not access social networking sites for personal use through their CCA work email address.

Users shall not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system, e.g., password cracking programs, packet sniffers, or port scanners.

Users shall not intentionally access, create, store or transmit material which the CCA management may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of CCA Executive Director).

Users shall not otherwise engage in acts against the values and purposes of CCA as specified in its governing documents or in policies and procedures adopted from time to time.

Users shall not send or knowingly receive files or documents that may cause legal action against, or embarrassment to CCA.

Any use of CCA ICT for the above purposes is prohibited, and will be considered grounds for disciplinary action, up to and including termination of employment.

2. Safeguarding CCA ICT Assets

These procedures address misuse from both inside and outside the organization. Threats may arise via a person (e.g. an employee) or via an automated source (e.g. a computer virus infecting e-mail). In order to safeguard CCA ICT assets, the following general practices should be observed:

- Critical hardware systems (i.e. servers) are located in a secure, locked location that is restricted to authorized employees only
- Computer equipment is best stored away from radiators, heating vents, air conditioners
- Cabling, plugs, and other wires are protected from foot traffic
- All workstations whether connected to the CCA network, or standalone, must use the approved virus protection software and configuration.
- The virus protection software must not be disabled or bypassed.
- The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software. The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

- Every virus that is not automatically cleaned, quarantined or deleted by the virus protection software constitutes a security incident and must be reported to the Office Manager.
- Quarantined viruses are cleaned/deleted from CCA systems by contracted IT supplier
- Computers are logged off when the operator is not in the vicinity of the computer. Automatic logout is recommended after 15 minutes of inactivity.

When an employee with access to CCA's shared drives leaves the employ of CCA, his/her access to individual accounts will be blocked and general access passwords to shared CCA drives or programs (e.g., Fluid, GoCCA, Google apps, GoTo Mtgs, etc) shall be changed. Email accounts may stay active for some period of time with messages forwarded to another current employee who is taking over these particular duties.

3. New User Setup Policy

Authorized users of CCA ICT shall be provided with a copy of this ICT Procedure and, before access to ICT resources is permitted, are expected to read it and sign a statement that they have read, understood, and agreed to abide by the policy and procedures. This applies to all existing employees as well as all new employees. Each new user will be provided with their own user ID and an initial password, which the user may revise. Employees shall inform the Office Manager of their current passwords.

Guidelines for CCA passwords: Since short passwords or dictionary words are easy to guess using automated password crackers, all passwords must be at least seven characters long; must not be simple, dictionary words; must contain a mix of alphabetic, numeric and special characters (e.g. "*&^2\$%\$#"); and must change on a regular basis (ideally every three months.)

4. ICT resources - Security and Confidentiality

4.1 Use of Internet

The following uses of the Internet using CCA equipment, facilities or email address, either during working hours or personal time, are NOT allowed:

- engaging in any unlawful activities or any other activities, which would in any way bring discredit to CCA
- engaging in personal or commercial activities on the Internet, including offering services or merchandise for sale
- engaging in any activity, which would compromise the security of any CCA servers
- downloading video and voice files from the Internet except when they will be used to serve an approved CCA function

Employees will follow existing security policies and procedures in their use of Internet services and will refrain from any practices, which might jeopardize CCA's computer systems, and data files, including but not limited to virus attacks when downloading files from the Internet.

4.2 Voice mail

CCA Voice mailbox accounts have passwords. The CCA Office Manager should be informed of the passwords by all users.

4.3 Videos/Photographs/Media

Except for stock photos or videos that are purchased by CCA, the consent of individuals who are pictured in photos, videos or other media is required before the item may be posted to CCA's information systems including the Web site. This consent may be obtained through an email message and should be saved in a central file.

4.4 Facsimile

Confidential information may be sent via facsimile provided the cover page indicates the information is 'Confidential', and is intended only for the use of the individual to whom it is addressed, and is not to be disclosed, copied, or distributed. Recipients are directed to contact CCA immediately by telephone should the facsimile arrive at an inappropriate destination.

4.5 Electronic Mail

Email accounts must have passwords in accordance with this policy. Access to email accounts is restricted to the owner of the mailbox. The owner of the mailbox may authorize other users specific access to their mailbox by activating the share function of the email program. Any other access to the mailbox requires the permission of the Executive Director or designate. Except if an employee is away from work for a period of time, his/her email may be accessed by designated CCA employees.

Confidential information may be sent via electronic mail provided the signature line indicates the information is 'Confidential', and is for the addressee only. Recipients are directed to contact CCA immediately by telephone should the electronic mail message arrive at an inappropriate electronic mail destination.

Users shall not open attachments containing .exe, .dll, .com, .bat or .scr file extensions unless authorized by System Administrator. Users shall not click on hyperlinks embedded in emails from unknown source.

4.6 Telephones/Smart Phones

CCA employees may use cellular phones or smart phones for business but are responsible for protecting confidential information from unauthorized disclosure and must use caution when discussing confidential information.

4.7 CCA Computer Network and Shared Drives and Applications

Documents and reports created by CCA employees that contain confidential information pertaining to participating organizations are to be stored on CCA computer networks or cloud services which are regularly backed up to protect against loss, and not on local hard drives. Confidential information which is stored on CCA computer networks is protected from unauthorized access or disclosure through the use of individually-assigned passwords.

Access to information on GoCCA and CCA hard drive is also controlled through individually assigned 'permissions' that allow different levels of access to various CCA programs, documents or sites from simply viewing the content to full editorial authorization. The Executive Director shall approve the level of permission/authority that CCA employees may be granted.

4.8 Laptop Computers and Other Portable Computing Devices

Only CCA approved portable computing/communication devices may be used to access CCA ICT resources. Portable computing devices must be password protected.

Employees using personally owned computers, laptops or smart phones must conform to CCA's software standards. CCA will not provide or reimburse employees for software that is commercially available for their personal computers.

All portable storage devices should be checked using the approved Anti-Virus application.

Users should avoid storing CCA data on portable computing devices if at all possible, or to strictly limit the time period for when it may be stored there. In the event that there is no alternative to local storage, all sensitive CCA data must be password protected and deleted as soon as possible after it is needed.

Employee information should never be stored on portable or electronic devices. If on occasion this information is required to be shared in electronic format, permission from the Executive Director must be obtained and a secure password-protected device must be used.

Portable computing devices must not be used while operating a vehicle without the use of an appropriate hands-free USB device.

4.9 Remote Access

Employees who telecommute from home are subject to the same policies regarding the use of CCA-provided equipment (hardware and software), services and internet as that of employees at the CCA Office.

Employees who telecommute shall not allow anyone, except other CCA employees to use CCA-provided equipment (including hardware and software) and services.

Telecommuting employees may use their own personal computer equipment. Employees may consult with their IT support person for work-related assistance for their computer at their own risk. CCA will not be able to provide technical support for computer or telecommunications equipment that is not compatible with equipment that is currently supported by CCA. Employees will be responsible for the maintenance and repair of their own equipment.

CCA will not purchase or reimburse employees for the cost of an Internet service provider in order to access CCA's remote access through VPN or Google Apps.

All remote users may connect to the CCA network only through VPN or through Google Apps using protocols approved by CCA.

VPN access is provided to employees as required and approved by the Executive Director.

When employees use VPN access to access confidential information:

- work should not be done in an area where others may view the information (e.g. cafes, libraries, or other non-private settings);
- the computer should not be left unattended with an active remote access connection; and,
- when exiting applications it is required that the employee log off and ensure the web browser is closed and VPN access is terminated.

Non-CCA computer systems are not permitted to connect to the CCA network unless approved by the Executive Director or designate.

5. Incidental Personal Use of CCA ICT

CCA reserves the right to restrict or revoke access to any CCA ICT resource or service.

As a convenience to CCA users, incidental use of CCA ICT resources is permitted. The following restrictions apply:

- Incidental personal use of electronic mail (including personal mail accounts), internet access, fax machines, printers, copiers, telephone system, smart phones and so on, is restricted to CCA approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to CCA.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- Storage of personal email messages, voice messages, files and documents within the CCA ICT resources must be nominal.
- Users shall not use CCA's email account to join listservs, newsgroups or social networking sites unless they have verified to the best of their knowledge that the listserv/newsgroup/social network is reliable and work related.
- Users understand that all messages, files and documents – including personal messages, files and documents – located on any of the CCA ICT resources are owned by CCA and may be accessed in accordance with this policy and CCA's Management of Information Policy.

6. CCA-Provided Portable Devices

In order to achieve appropriate operational oversight and accommodate program expectations, portable devices may be provided to CCA management and employees. The assessment of whether an employee requires a portable or electronic device will remain with the Executive Director and will be based on:

- Program needs (i.e. safety considerations, working from multiple locations, on-call while out of the building)
- Available program budget
- Organizational needs (i.e. accessibility)

Employees will be accountable for ensuring responsible use and assume liability for any unreasonable costs associated with portable device use. This includes any subscription services (games, ringtones, contests, etc.) that may be ordered by text, as well as costs associated with device replacements if lost, stolen or damaged. The use of CCA portable devices for personal purposes is expected to comply with Section 5 above.

In the event a portable device is lost or stolen, the Office Manager must be informed as soon as possible in order to avoid charges being incurred by unauthorized users.

7. Use by Employees of Personal Portable Devices for Work

When employees use their own devices to conduct CCA business their activity is expected to adhere to CCA policies. Unless approved by the Executive Director, employees will not be reimbursed for the use of their own portable or smart phone devices for CCA-related work.

Employees may be reimbursed for use of their own portable or smart phone device if they can demonstrate that they need to use it regularly to support the delivery of CCA's programs. In such situations employees may apply for a monthly allowance to cover the additional billing charges. The charges will be in keeping with reasonable plan costs available to CCA and will be revised from time to time to keep up with market changes. Where a personal smart phone has been approved for use for CCA purposes and for reimbursement, employees may be required to submit billing information related to the reimbursement requested.

8. Disciplinary Action

CCA will carry out an investigation when:

- There is a complaint of misuse of the CCA ICT resources
- CCA suspects misuse of the CCA ICT resources

CCA reserves the right to:

- Access the user's files and messages as stipulated above
- Make these materials available to an external IT adviser to carry out the necessary investigations
- Suspend user from employment with CCA to allow the necessary investigations to be carried out
- Immediately deactivate the user's accounts

CCA reserves the right to implement the corrective action process if there is a violation of these policies and procedures.

Appendix - GoCCA Program Set Up and Security - General

The Go-CCA application relies mostly on [ASP.NET](#) for its server-side programming and JavaScript is used for client-scripting requirements. The site makes extensive use of [ASP.NET](#) Web forms, Web user controls and Master Pages. A "code-behind" methodology was used to provide a distinct separation between presentation and logic. The site is built on the Microsoft dot NET Framework, a platform that allows the building of applications that have good user experience, seamless and secure communication, and the ability to model a range of business processes.

The application is hosted on a Windows server. Managed hosting services give CCA access to 24/7 real-time monitoring, regular back up, proactive security management and ongoing maintenance.

The functionality and responsibilities of the system are partitioned into a standard three-tiered architecture with a presentation layer, business object layer and data access layer.

All data within the system is stored within a SQL database. The system secures and isolates files on a per-organization / per-accreditation basis. An organization's uploaded documents, for example, are stored as binary data within a database table.

Access to download these documents is only available through a process that requires the checking of user credentials (the organization's users and, at a given point in time, CCA reviewers and CCA employees authorized for that accreditation) and the status of the accreditation process (open for the organization's use, or under review by the CCA review team, or closed/done and no longer accessible to the CCA review team).

Mitigating the Practical Risks of Loss, Theft, Unauthorized Access

In addition to the technical ways in which the information stored in GoCCA is safeguarded and unauthorized access prevented, there are human and practical considerations when it comes to mitigating the risk of an electronic document being shared outside the circle of those authorized to see them for an accreditation review.

An organization's accreditation pre-site submission is accessible on a per-review basis for a limited time to the members of the CCA review team (and to CCA employees). This includes documents that, when opened as part of the indicator assessment step, are indeed saved and/or savable electronically on these CCA users' computers.

CCA takes steps to help mitigate the risk of electronic documents being shared outside the circle of those authorized to see them for a review:

- CCA employees and reviewers go through a screening process.
- CCA employees and reviewers are bound by a contract/engagement with CCA that includes an oath of confidentiality.
- As part of training and before each review, CCA reviewers are re-familiarized with their responsibilities to safeguard information and instructed on how to manage any electronic files (deleting, email not used to circulate accreditation pre-site evidence).
- After the site visit, reviewers are prompted (two scheduled emails) by CCA's office to shred paper files and delete (fully delete) any electronic files (and instructed how to do so).
- A user interface that gives clear and explicit cues to the user that s/he is in a secure section of the site (for example, "Welcome, First Name"/"You are logged in as username" and a distinct visual identity for the password-protected Go CCA Accreditation Tool). Like seeing "https" before an URL gives a visual reassurance and situates the user, so do these aspects of CCA's user interface.
- A tagging system for any files that are downloaded electronically to a reviewer's computer. Any downloaded file is tagged with a prefix in its filename that identifies it as part of a specific accreditation review (word-number identifier). This makes it easier for reviewers to follow CCA's step by step instructions post-site-visit to find files, select, delete and fully delete.
- Results of CCA surveys are shared via shared read-only online reports and are not circulated to the review team over email or other means.



Section	General Organizational Policies and Procedures
No.	ORG – 06
Title	Review and Revision of CCA Policies
Approval date	July 30, 2013
Approved by	Executive Director
Dates of revision	February 28, 2017
Date Reviewed	July 14, 2022

ORG - 06 Review and Revision of CCA Policies

Scope

This policy applies to CCA Executive Director.

Purpose

The purpose of this policy is to outline responsibilities and timelines for regular review and revision of CCA Operational Policies.

Definitions

Policy

CCA is committed to maintaining relevant and up-to-date policies in response to internal or external changes. One way to ensure that this occurs is by conducting a regular review of our policies and bylaws.

CCA policies will be reviewed every three years on a staggered cycle and revised as needed. Additional revisions to particular aspects of CCA policies may be considered and implemented at any time as needed.

Regular Review of CCA Policies – Responsibility and Timelines			
Policy Area	Last Review	Next Review	Who approves the Policies
General Organizational Policies and Procedures	January 2020		Executive Director
Human Resource Policies	January 2020	July 2022	Executive Director
Occupational Health & Safety Policies	September 2016		Executive Director
Financial and Fee Policies and Procedures	October 2020		Executive Director
Accreditation Policies and Procedures	February 2020	Ongoing	Executive Director



Section	General Organizational Policies and Procedures
No.	ORG – 07
Title	Risk Management Framework
Approval date	July 17, 2017
Approved by	Executive Director
Dates of revision	
Date Reviewed	January 30, 2020

ORG - 07 Risk Management Framework

Scope

This policy applies to staff and reviewers.

Purpose

The Risk Management Framework outlines CCA's approach to identifying and managing the risks CCA faces through a range of prevention and mitigation strategies.

Definitions

Participating Organizations (POs) – Organizations that have signed an agreement with CCA to participate in the Accreditation.

Member Associations – These are the corporate members of CCA, which are associations of service providers, as outlined in the CCA Bylaws.

Policy

1. CCA is committed to the proactive identification and management of potential risks to our people, our program and participating organizations, our property including the information we hold, our financial health and reputation. Risk management takes place within a culture of continuous quality improvement, where issues are identified and resolved in an effective and systematic manner.
2. Roles and Responsibilities
 - a. The Board of Directors is ultimately responsible for ensuring that risks faced by CCA are addressed both pro-actively and reactively.
 - b. The Executive Director is responsible for developing and overseeing implementation of a Risk Management Plan (aligned with the Strategic Plan) that identifies key areas of risk and outlines strategies for preventing and mitigating the risks. The Executive Director is responsible for informing the Board about risks identified and for making regular reports on the Plan.
 - c. Risk management is integrated with all other activities at the organization. All CCA staff are responsible for identifying potential and actual risks to CCA and reporting them to the Executive Director. The Executive Director shall ensure that education and communication take place on a regular basis to keep staff informed of the various risk areas that CCA faces and strategies to manage them.

3. Reporting and review of the Risk Management Plan

- a On a quarterly basis (or more frequently if needed) the Executive Director shall review the Risk Management Plan and update it based on a scan of trends and evolving best practices, and feedback from staff and other stakeholders.
- b Twice a year, the Executive Director shall report to the Board of Directors on the Risk Management Plan including effectiveness of the plan and systems for minimizing risk, assessment of new risks and revision of the Plan.

Procedures

In order to effectively identify and manage situations that may present actual or potential risk, CCA has instituted the following measures in order to systematically monitor, assess and address risk issues. They are as follows:

1. **Accountability**

The Executive Director is the organization lead for Risk Management and has the following responsibilities:

- Ensure that the Organization is adhering to established risk management practices
- Act as an organizational resource in risk related matters
- Ensure that staff are educated on relevant risk management topics
- Review and update the RM Plan on a quarterly basis and report to the Board on the Plan twice each year

2. **Risk Prevention Program**

2.1 Personnel (paid and unpaid including Board members)

- Up-to-date Policies and bylaws that comply with legislative and regulatory requirements re: Governance, Human Resources, Information Management, Inclusion and Accessibility
- Up-to-date Occupational Health and Safety Policies and monthly workplace inspections
- Code of Conduct for Employees and Reviewers, Board Code of Conduct
- Communication with Board and staff about possible risks
- Ongoing relationship with legal advisor to consult as needed
- Emergency response plans

2.2 Financial, Property, and Assets

- Up-to-date Financial and Fee Policies and communication with personnel and POs about these
- Annual financial audits
- Quarterly financial reports to the Board comparing to budget
- Reliable system for invoicing POs for services and collecting fees
- Inventory of property
- Monthly workplace inspections
- Funds held with a registered/insured financial institution and invested in secure mechanisms
- Lease and co-tenancy agreements
- Copyrights statements on CCA standards and related documents

2.3 CCA Program

- Up-to-date Accreditation Program Policies and communication with personnel and Participating Organizations about these;
- Monitoring of CCA Program performance
- Code of Conduct for Employees and Reviewers, Board Code of Conduct
- Performance Appraisals with Staff
- Regular reporting on program to Quality Committee and Board
- Regular review and updating of CCA Standards
- Regular maintenance and development of CCA Information policies, procedures, technology and systems (including the GoCCA Program)
- Complaints Reporting Policies (about CCA and about accredited organizations)
- Evaluation surveys conducted with Participating Organizations and results regularly monitored
- Relationships maintained with stakeholder sector associations
- Effective clear agreements with Participating Organizations
- Ongoing communications about CCA and benefits of CCA accreditation
- Accreditation of Standards by ISQua and plan to have CCA organization accredited in 2019

3. **Risk Mitigation Program – See Risk Management Plan for more details**

- 3.1 Incident Reporting and Follow-up re Occupational Health and Safety (including harassment)
- 3.2 Insurance re General Liability, Fraud/Theft, Directors and Officers, Errors and Omissions, Property Loss and Business Continuation
- 3.3 Reliable and effective Information Technology support
- 3.4 Policies concerning complaints about CCA or about accredited organizations
- 3.5 Appeal Policy re accreditation decisions