

# Generative AI Lab: Facilitator's Guide



*Inspiring Possibilities*



## **Generative Artificial Intelligence Lab**

### **Facilitator's Guide**

#### **Generative AI Lab Prerequisites**

Before the delivery of a Generative AI Lab, it is essential to build a strong foundation with employees. This ensures they understand the agency's reasons for approving the use of Generative AI, as well as the ethical considerations and procedures for its use. Given that Generative AI Labs focus on hands-on experiential learning, participants must meet the following prerequisites:

1. Read your agency's Artificial Intelligence Policy, and
2. Complete the agency-wide Generative AI training titled, "Generative AI: An Online Learning Module for Developmental Services Employees", available on REAL Xchange.

Additionally, before attending a Generative AI Lab, it is strongly recommended that employees create a ChatGPT account. This requirement helps ensure a smooth start for participants and mitigates the risk of ChatGPT's processing delays, due to multiple simultaneous sign-ins, particularly in locations with limited Wi-Fi.

The notes section of the Generative AI Lab PowerPoint presentation provides the information needed to deliver each slide effectively. This Facilitator's Guide outlines the practical and physical requirements for successful training.

#### **Registration**

Depending on an agency's specific requirements, Generative AI Labs may or may not be mandatory for all employees.

To track registrations, use the spreadsheet program application of your choice, as this will help to control class size limits, create sign in sheets, and name tags. To facilitate group exercises, use name tags for participants that have either "ChatGPT" or "Co-Pilot" displayed.

#### **Logistics**

Choose a facility that is/has:

- dependable Wi-Fi
- sufficient electrical outlets to accommodate charging the number of laptops and other IT equipment required
- enough space so that seating can be arranged to create an interactive learning environment
- comfortable heating/cooling
- a light airy space, if possible and affordable
- adequate parking, if participants will be driving to the training
- locked storage capabilities (if you are holding a series of sessions over more than 1 day, to leave laptops onsite and seating arrangement in place)
- accessible

#### **Room Setup**

Set up the training room with enough lead time to:

- Arrange tables and seating (a "U" shape seating arrangement is recommended). This way, all participants can see the presentation, the facilitators and each other, preventing anyone from having their backs to one another.

### **Room Setup (continued)**

- Place laptops/IT equipment at the tables (one per pair of participants is recommended) for participants' use, and ensure the equipment is charged and ready to be used.
- Affix (2) jumbo sticky Post-It flipchart sheets of paper at two different sites around the room for the group activity, with markers available.
- Test the PowerPoint presentation to ensure links, audio, etc. are working.
- Provide signage with the Wi-Fi login credentials.

### **Contingency Plans**

- Be sure to have backup activities or alternative approaches in case the original plans or activities cannot be executed. For example, schedule 2 trainers for each session, plus 1 trainer on stand-by.

### **Materials Needed**

- Participant class list
- Sign-in sheet
- Name tags for participants (half of the nametags include the ChatGPT logo, and the other half include the CoPilot logo)
- Facilitator laptop with the Generative AI Lab presentation pre-loaded
- Printed paper copy of the Generative AI Lab presentation, including slide notes
- Laptops (recommend one laptop per pair of participants)
- Jumbo, sticky Post-It flipchart paper
- Buzzers or bells for competitive games
- Printed scenario worksheets for the group exercise
- Wi-Fi access
- Snacks for group activities and games (accommodate dietary restrictions, i.e. no peanuts, gluten-free, sugar-free, etc.)
- Printed feedback forms or evaluation surveys for participants to complete **or** create a QR Code that directs participants to an online anonymous survey

### **List of Attachments to the Facilitator's Guide**

- Use of Artificial Intelligence Policy (Policy # ADM-100-22)
- Confidentiality/Release of Confidential Information Policy (Policy # ADM-100-04)
- Information Technology Policy (Policy # ADM-100-15)
- Privacy and Protection of Personal Information Policy (Policy # ADM-100-17)
- AI Lab Participant Name Tags
- Scenario Worksheets for Group Exercise
- Supporting Document - E-Mail to All Employees - Announcing Generative AI Training Module and Lab
- Supporting Document - E-Mail to All Employees - Registration for Generative AI Lab
- Supporting Document - E-Mail to All Employees - Reminder for Registered Employees for their Generative AI Lab Session

**Policy & Procedure**

Section: General

Board Approval: September 6, 2023

## **USE OF ARTIFICIAL INTELLIGENCE**

---

### **POLICY STATEMENT**

The Agency supports innovation through the use of modern technology. Artificial intelligence, accessed through generative AI chatbot applications, is a powerful tool that can provide information to employees to assist them in providing high-quality supports and services to people. AI may be used to facilitate information gathering, to aid in problem-solving, and to enhance productivity. AI must be used in an ethical and responsible manner at work and only after receiving training on its appropriate use.

### **DEFINITIONS**

**Artificial Intelligence:** the theory and development of computer systems able to perform tasks that normally require human intelligence, such as learning, problem-solving, decision-making, visual perception, speech recognition, and translation between languages.

**ChatGPT:** is an artificial intelligence (AI) chatbot developed by OpenAI that provides responses to questions using language that sounds like a normal conversation with a person. ChatGPT is a member of the generative pre-trained transformer (GPT) family of language models.

**Generative AI:** is a type of artificial intelligence that can create new content or data, such as images, text, or music, that was not previously in its training data. Generative AI tools can produce entirely new and unique outputs based on patterns they've learned from their training data.

**Large Language Model:** is an AI model that is trained on massive collections of existing information/text to use as a basis for responding to questions.

**AI Ethics:** An area of study in the field of AI that ensures systems respond in ways that are beneficial and avoid things such as bias, racism, sexism, etc that may have been found in the language used to train it.

**Generative AI Bias:** the tendency of a generative model to produce outputs that reflect and potentially amplify pre-existing biases present in the data it was trained on. This can lead to unfair or unrepresentative results when the model generates new content or predictions.

**Natural Language Processing:** is a subfield of artificial intelligence (AI) that focuses on the interaction between computers and human (natural) languages. It involves enabling machines to understand, interpret, and generate human language in a way that is valuable.

**Bing:** Originally developed as Microsoft’s alternative to Google’s search engine, Bing is currently being revised to include elements from ChatGPT and is part owner.

## **GUIDING PRINCIPLES**

That employees understand and maintain good practices, including appropriate and guarded use of artificial intelligence that aligns with the Agency’s goals, values, and ethical standards.

Employees are encouraged to use Agency approved AI tools to aid their work and to enhance productivity.

A person-directed approach to planning and supports must remain of utmost importance, so employees should examine and revise any AI generated resources which may be incorporated into support-related plans and documents.

Employees have a duty to, upon becoming aware of people receiving supports using AI applications, offer and encourage participation in internet safety training and education to help people we support understand the potential risks and opportunities of AI.

Employees must maintain high ethical standards when using AI at work. AI generated works should be checked for factuality, copyright violations, privacy and confidentiality infringements, and sufficiently edited to reflect a standard equal to or better than non-AI supported work.

Employees, volunteers, students, and agents of the Agency must understand their responsibility to safeguard and not disclose any confidential information when using AI. Employees should not input or upload any private or confidential data to AI applications.

See the following policies:

1. Social Media (ADM-100-19) policy and the Social Media User Guide
2. Oath of Confidentiality (PER-100-09) policy
3. Confidentiality/Release of Confidential Information (ADM-100-04) policy
4. Privacy and Protection of Personal Information (ADM-100-17) policy

Violations of this policy are subject to disciplinary action, up to and including dismissal.

## **PROCEDURE**

1. Artificial intelligence tools will be reviewed by the Director, Marketing and Innovation and approved by the Executive Director prior to any use by Agency employees. Currently ChatGPT and Bing Chat are the only Agency approved AI tools.

2. All employees must have successfully completed the AI Training module provided by the Agency. This training shall cover guidelines outlined in this policy, as well as any other relevant policies and procedures. Employees shall receive regular updates as needed.
3. The use of AI at work is intended to assist employees in providing high-quality supports and services to people. AI may be used for information gathering, to aid in problem solving non confidential matters and to enhance productivity.
4. Employees using AI for work purposes must not disclose any confidential information, sensitive, or personally identifying information, even if they believe it is harmless or insignificant. If an employee is unsure about whether the information is confidential or not, they must consult their Manager.
5. AI should be used in an ethical and responsible manner. Employees should not use AI to engage in inappropriate or unethical behaviour, such as harassment or discrimination. Employees shall use professional language when communicating with AI chatbots and shall not use abusive, offensive, or discriminatory language. If an employee feels that an AI chatbot is responding inappropriately, they shall report it using the application complaint mechanism.
6. Employees shall not use AI chatbots for personal reasons, such as personal research or leisure activities while on work time.
7. AI is a powerful tool but it is not perfect. Employees must not accept all information obtained through AI chatbots as factual and must not rely solely on AI generated content to develop support plans, protocols, policies, procedures, or any other documents where inaccuracies could lead to harm or negative outcomes for people we support, employees, or the Agency.
8. All AI chatbot drafts must be carefully reviewed, examined for AI bias and potential copyright violations, and sufficiently edited. Employees are responsible for their own work; therefore, care must be taken in fact checking, editing, and proof reading prior to submitting work for Manager review.
9. All paid AI application subscriptions must be approved by the Executive Director.
10. Employees must take appropriate measures to protect Agency privacy and security when using AI applications, such as using strong passwords and avoid using public open wifi networks. If an employee suspects their AI account has been compromised, they must change their password immediately.
11. Employees must use a work email address when registering for an Agency approved AI application but must use a different password to their work Microsoft 365 account.
12. The Director, Marketing and Innovation is responsible for monitoring generative AI updates, the AI threat landscape, news, capabilities and changes to identify areas where additional training, support and/or policy changes may be needed.

**Policy & Procedure**

**CONFIDENTIALITY / RELEASE OF CONFIDENTIAL INFORMATION**

**POLICY STATEMENT**

The Agency will uphold each person's right and their family's right to privacy. All records and all information on people supported and their family's access to services will be considered private and confidential and will be subject to restricted use and controlled access. Employees and agents of the Agency are required to sign an Oath of Confidentiality declaring they will hold confidential all information related to people supported and their families.

**PROCEDURES**

**1. CONFIDENTIAL INFORMATION**

- a) All requests to obtain information from outside Agencies or individuals, must be made in writing and be accompanied by an original consent form authorizing the Agency to obtain specific information and signed by the person/family or legal representative.
- b) Information or records forming part of a person's support file cannot be released, without the informed, written consent from the person, or a parent/guardian if the person is a child under the age of sixteen (16). In circumstances where a person is incapable of understanding consent, the person's nearest relative may give consent. Where it is not reasonable to secure consent from a relative, an appropriate third party will be secured.
- c) Verbal or written information will not be released without completed Consent (ADMIN11) and Approval for Release of Information (PROG44) forms, signed, and approved by the Director. These forms are filed and retained in the file of the person supported. If the information request involves the person's medical or health care status, the Medical/Health Consent (ADMIN39) form must be completed for information to be released. A person or their substitute decision maker may revoke their consent at any time. The ability to revoke consent must be explained to the person supported and/or their substitute decision maker at the time of signing.
- d) Consents must have an expiry date. The expiry date is a maximum of one (1) year from the date of signing. Consents must be reviewed and re-signed on a minimum annual basis, or more frequently where appropriate.
- e) Third party information, received from an outside Agency or professional, forming part of a person's file, cannot be released by the Agency. Requests for the release of any third-party information must be made directly to the Agency or professional from which the information originated.

## 2. **INFORMED CONSENT**

- a) Informed consent is a process by which a person gives permission, after the purpose, benefits, risks, possible side effects/consequences, and alternative courses of action have been explained and understood.
- b) If a person cannot provide informed consent, their designated family member or alternative decision maker should be noted in the person's file.
- c) The Best Practices for Obtaining Informed Consent (Appendix A) and the Checklist for Informed Consent (ADMIN41) are attached to this policy. Complete this checklist each time informed consent is obtained. Employees must do their best to ensure any consent given is informed. The checklist must be completed whenever the level of ability for the person providing consent could bring into question if the consent given was informed.

## 3. **RELEASE OF INFORMATION WITHOUT CONSENT**

Release of information without consent will be limited to the following:

- a) Employees of the Agency, who are directly, involved in providing service to a person or who are involved in the handling of records, and who require information to carry out their respective duties.
- b) Agents of the Agency, such as Board members, volunteers, or contracted service providers, who in the discretionary judgement of the Executive Director or designate require selected information to carry out a specific duty or responsibility.
- c) A peace officer in circumstances of **urgency** or **emergency** where there are reasonable grounds to believe that failure to release information is likely to cause the person or other persons physical harm. In such circumstances, prompt and written notice of the information disclosed will be provided to the person or the parent/guardian, and a Serious Occurrence Report (PROG70) completed.
- d) A person providing medical treatment in cases of urgent or emergency situations shall be provided with whatever information is required for the person's physical or emotional well-being, and a Serious Occurrence Report (PROG70) completed.
- e) A Provincial government Program Supervisor or Director as provided in specific legislation can access records upon request for the purpose of carrying out their duties.
- f) Any court, upon receipt of a court order, in consultation with the Agency's legal counsel.

## 4. **RELEASE OF INFORMATION FOR RESEARCH PURPOSES**

- a) Release of information for approved research purposes may be permitted only in accordance with the Research (ADM-100-20) policy.
- b) Information will not be provided to a researcher that in any manner identifies the person supported without their informed consent.



## BEST PRACTICES FOR OBTAINING INFORMED CONSENT

### Reasoning behind informed consent

Community Living Essex County provides person directed support, which encourages the person to be active in all decisions. Involving the person in the process of obtaining informed consent will increase their autonomy. Employees need to do their best to determine that the consent given is informed in accordance with the Confidentiality/Release of Confidential Information (ADM-100-04) and the Privacy and Protection of Personal Information (ADM-100-17) policies.

Informed consent is a process by which a person gives permission, after the purpose, benefits, risks, possible side effects/consequences, and alternative courses of action have been discussed and understood.

### When to obtain informed consent

In a variety of ways, the Agency regularly asks a person supported to give consent.

Examples include:

- Implementing behaviour support protocols;
- Rights restrictions,
  - Locking up their money and medications
  - Video monitoring
  - The use of safe areas that confine the person when having a difficult time
- Talking to the person's doctor on their behalf;

There are specific situations where consent must be given in writing, for example:

- To allow a person's picture to be used in promotional material,
- Submitting personal information to the Rights Review Committee and the Joint Third-Party Review Committee

### Process for obtaining informed consent

The first priority is to determine that the person understands the information given to them. It is important that discussions of a sensitive or confidential nature take place in private and not in front of other people supported, Employees, or members of the community.

1. **Explain the Consent Process** - Obtain accurate information and have a good understanding before attempting to explain the process of informed consent to the person supported.
2. **Person Must Understand the Information Being Provided** - make sure the person is provided with information in a manner they can understand. The following are tips to assist in the process:
  - **Accessible language** - do not overcomplicate the information, limit the number of words used and keep the words simple and easy to understand.
  - **Reading/comprehension level** - consider the person's reading and comprehension level during the explanation process. ShareVision may have external reports/assessments completed that may help you learn the best method.
  - **Communication** - communicate appropriately using a variety of forms of communication suited to the person (PECS, sign language, body language, and other visual aids if needed).
  - **Teach-back technique** - to determine if the person understands the information. This is where the Employee asks the person to retell the information that was discussed. Can they state it in their own words?
  - **Questions and answers** method for presenting information and determining the persons understanding.
  - **Communication translator** - People supported who do not use traditional words to

communicate have a communication translator. If the person has a communication translator, it will be located in ShareVision and their personal file.

- **Observe** - try to observe if the person supported is consenting nonverbally through their body language, and or facial expressions. A person can convey, through verbal or other means, that informed consent is given.
  - **Involve others** who know the person best to explain and communicate the information, and to facilitate their understanding and to determine if informed consent has been given.
3. **Involving the person throughout the process** - ensure the person is actively involved in the decision process. Supportive decision making can assist a person to ensure they fully understand what is being asked. Use some of the tips above.
  4. **Question & Answers for the person/family** - creating an opportunity for the person/family to gather a further understanding of the information being presented.
  5. **Consent must be voluntary** - must not be obtained through fraud, coercion, duress, undue influences, or stress.
  6. **Consents must have an expiry date** - The expiry date is a maximum of one (1) year from the date of signing. Consents must be reviewed and re-signed on a minimum annual basis, or more frequently where appropriate.
  7. **Any consent given can be revoked at any time** - The ability to revoke consent must be explained to the person supported and/or their substitute decision maker at the time of signing.

**The Checklist for Informed Consent (ADMIN41) must be completed each time informed consent is obtained.**

**Things to keep in mind:**

In situations where the person is unable to grant consent then a substitute decision maker or public guardian is given the same information and is requested to make an informed decision on the person's behalf. Employees cannot give consent for the person supported, but they can co-sign to verify the person's signature.

A person may be able to give informed consent in one situation but not another; the understanding of each situation may vary.

More complex/abstract situations may mean that in order for a person to understand and give informed consent, a family member/substitute decision maker/public guardian may need to be involved in the process.

The following persons, ranked in order according to the Health Care Consent Act and the Child, Youth and Family Services Act, can be substitute decision-makers. The person's:

1. Guardian
2. Power of Attorney for personal care
3. Representative appointed by the Consent and Capacity Board
4. Spouse or partner
5. Parent, (unless they only have right of access) Children's Aid Society or other person lawfully entitled to give or refuse consent
6. Parent with only a right of access.
7. Sibling
8. Other relative
9. Office of the Public Trustee

**Policy & Procedure**

Section: General  
Board Approval: February 6, 2002  
September 11, 2013

## INFORMATION TECHNOLOGY

---

### **POLICY STATEMENT**

The Agency may provide employees with access to and use of computers, mobile devices, software, apps and other forms of information technology. Such access is to facilitate effective communication, enhance productivity, meet operational requirements, support the provision of high-quality services and to interact with the community we serve while respecting privacy and confidentiality.

### **GUIDING PRINCIPLES**

That employees understand and maintain good practices, including appropriate use of information technology to safeguard and protect Agency equipment, systems and data. All communications must be consistent with the Canadian Charter of Rights and Freedoms, the Ontario Human Rights Code, and the Agency's values, policies and professional standards.

Employees are encouraged to use IT resources to communicate, acquire or share information and participate in educational or professional development activities.

Employees, volunteers, students, and agents of the Agency must understand their responsibility to safeguard and not disclose any confidential information. See the following policies:

1. Social Media [ADM-100-19] policy and the Social Media User Guide
2. Oath of Confidentiality [PER-100-09] policy
3. Confidentiality/Release of Confidential Information [ADM-100-04] policy
4. Privacy and Protection of Personal Information [ADM-100-17] policy

Agency information and equipment are corporate resources with substantial value that must be protected from unauthorized use, modification, destruction or disclosure, whether intentional or inadvertent. The Agency, at its discretion, reserves the right to implement monitoring systems and/or software (see Electronic Monitoring [ADM-100-21] policy) to ensure compliance with Agency policies, employment agreements, or any other applicable policies and agreements.

Violations of this policy are subject to disciplinary action, up to and including dismissal.

## **DEFINITIONS**

### **Information Technology:**

The use of any computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data.

### **Hardware:**

- a) The physical parts of a computer and related devices. Computer equipment includes, but is not limited to servers, workstations, laptops and peripheral devices including printers, scanners and external data storage devices.
- b) Electronic devices including cell phones, smartphones, mobile devices, tablets and other wireless devices, whether owned by the Agency, the employee, volunteer, student or agent of the Agency.

### **Software:**

A general term for the various programs, applications, scripts and instruction sets used to operate computers and related devices. Some general types of application software include:

- a) Productivity programs such as word processors, spreadsheets, and databases
- b) Presentation, graphics, and video editing software
- c) Communication applications such as email programs and video conferencing platforms

### **Password:**

A string of characters that can contain letters, numbers and special characters, used to verify the identity of a user during the authentication process in order to gain access to a file, application, or computer system.

### **Multifactor Authentication:**

Multifactor authentication (MFA) is a security process that requires the use of two (2) or more methods of authentication to verify the identity of a user.

### **User:**

An employee, volunteer, student, or agent of the Agency, including all personnel affiliated with a third party who has been granted access to the Agency's secure network.

### **Personal Use:**

Any use of computers, electronic devices or other technology that is not part of the employee's professional duties.

### **Remote Access:**

The ability to access the Agency's computer network through a secure connection. Remote access enables users to access the Agency computer system when they are not physically at an Agency location to connect directly; in other words, users access systems remotely by using an internet connection.

## **PROCEDURE**

### **1. Access to Systems**

- a) Access to the computer network is restricted through the use of usernames and passwords. The Director, Marketing and Innovation or designate, is responsible for defining appropriate access levels for all Agency employees.
- b) Human Resources will initiate user access requests for new employees and terminations through the Agency's database program, for action by the IT service provider.
- c) Upon creation of new user accounts, the manager will receive an auto-generated email alert containing a temporary password for the employee. Managers must deliver the temporary password directly to the employee.
- d) Employee permissions and access to work programs and applications are restricted by security group membership maintained by the IT service provider. Security groups and access are reviewed and approved by the Director, Marketing and Innovation bi-annually.

The IT service provider assigns users to security groups based on job title and instructions provided by Human Resources using the User Access Request form in the electronic database.

- e) Permissions within Agency programs and applications for non-support positions are restricted based on job classification and responsibilities. Administrators for Agency programs and applications, as listed below, must complete the User Access Checklist promptly for all employees entering and exiting the department.

|                        |                                    |
|------------------------|------------------------------------|
| <b>Department:</b>     | <b>Administrator:</b>              |
| Human Resources        | Director, Human Resources          |
| Finance                | Director, Finance                  |
| Marketing & Innovation | Director, Marketing and Innovation |

- f) Prior to receiving access to the Agency computer system, employees must read this policy and sign the Information Technology Policy Acknowledgement (ADMIN22).
- g) Managers must inform the Director, Marketing and Innovation or designate immediately when access to information systems is to be restricted for suspended or terminated employees.
- h) All employees must log out of Agency systems prior to leaving any device or computer unattended. A proper log out means that the user has selected 'Log Out' rather than simply exiting the program or application.

## 2. Passwords

- a) Passwords are confidential. Users are responsible to safeguard, not share or disclose their password. The Agency will hold users responsible for all activity that occurs under their username and password.

- b) Users shall immediately report any known or suspected compromise of their passwords to the Director, Marketing and Innovation or designate.
- c) The use of another user's account password is strictly prohibited. Employees who need to share files should contact system administrators to arrange an appropriate method.

### **3. Multifactor Authentication**

- a) All users accessing Agency IT systems and data are required to use multifactor authentication (MFA) for authentication purposes.
- b) The use of MFA is mandatory for all remote access connections to the Agency's IT systems and data, including access from home or other remote locations.
- c) MFA must be enabled for all cloud-based applications and services used by the Agency.
- d) MFA must be enabled for all privileged accounts, including administrative and system accounts.
- e) Users are prohibited from sharing or disclosing MFA credentials to anyone, including co-workers, family members, or friends.
- f) All computer users must select at least one Agency-permitted MFA method. The two permitted MFA methods are:
  - an Agency-issued FIDO2 security key
  - the Microsoft Authenticator Application
- g) All employees must complete the Multifactor Authentication Method Selection Form upon hire.
- h) The Agency will purchase one FIDO2 key for every employee selecting this MFA method. Employees will be responsible for the replacement cost of lost or stolen MFA devices.
- i) All employees who choose the FIDO2 key as their MFA method must have their key with them at every shift.
- j) All lost or stolen MFA devices must be immediately reported to the Director, Marketing and Innovation for deactivation and replacement.
- k) The agency offers employees the option of using a personal mobile device for authentication should they wish to do so for convenience. Personal mobile devices are not required for work purposes as the Agency provides an alternate MFA method along with devices at locations for employee work to be completed.

- l) All employees who choose to use the Microsoft Authenticator App as their MFA method must install the app on their own personal mobile device. Installing the app on an agency-owned location device or a device owned by someone else is not permitted.
- m) All employees who choose to use the Microsoft Authenticator App as their MFA method must complete and submit the Personal Electronic/Mobile Devices section of the Information Technology Policy Acknowledgement (ADMIN22) form.
- n) All employees who choose to use the Microsoft Authenticator App as their MFA method must have their personal mobile device with them at every shift.
- o) Employees are permitted to change their MFA method by re-submitting the Multifactor Authentication Method Selection Form.
- p) Failure to bring your MFA device (FIDO2 key or phone) to work may result in disciplinary action.
- q) The Director, Marketing and Innovation will regularly review and monitor the use of MFA to ensure compliance with this policy.

#### **4. Computer Use and Security**

- a) Users do not have privacy rights or ownership to anything that is accessed, sent or received on equipment owned or operated by the Agency. All documents and files created using Agency information technology are the property of Community Living Essex County.
- b) Users will refrain from using Agency equipment to download, store, transfer, or share content that is illegal, inappropriate, derogatory, offensive, or damaging to the reputation of the Agency and/or anyone that is supported or employed by Community Living Essex County.
- c) Users are not permitted to purchase goods or services using Agency equipment for personal use without the express written consent of their Manager.
- d) Only the Director, Marketing and Innovation or designate will authorize the download and installation of software on Agency equipment.
- e) Users must not deliberately perform acts that waste computer resources (including network bandwidth, Wi-Fi, disk space, and internet) or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, uploading or downloading large files, unnecessary printing, non-work-related streaming audio or video files, or otherwise creating unnecessary network traffic.
- f) IT support requests must be submitted through the IT Service Request form found in the Agency database program. All requests for service will be screened by the Manager, Technology and New Media and forwarded to the Agency contracted IT service provider

as appropriate. Employees must not call the IT service provider directly. Emergency IT requests outside regular business hours should be reported by email to the Director, Marketing and Innovation or designate.

## 5. Email

- a) Employees are provided email access to support and facilitate Agency business. The Agency is the sole owner of all email messages sent or received through any Agency email server. Email transmitted through the Agency email server should not be considered private. The Agency reserves the rights to audit, intercept, and access and disclose all messages created, received or sent over the email systems for any purpose.
- b) Email communication is to be treated with the same authority and professionalism as any other Agency correspondence.
- c) Notwithstanding the Agency's right to retrieve and read any email messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient.
- d) All employees must check their Agency email at the start of each shift and Managers should allow employees time to do so.
- e) Employees are permitted to synchronize their Agency email account on their personal device in accordance with sections **3. Multifactor Authentication** **8. Mobile Devices** and **9. Personal Electronic Devices** of this policy.
- f) Managers, Directors, Administrative Officers and Human Resources Officers who will be away from work should engage the Out of Office assistant. The message should include the duration of absence and the name of an alternate contact.
- g) A standard email signature is applied by the mail server to all outgoing Agency emails. Employees must not create and attach their own signature.
- h) A specific distribution list has been established to distribute emails to all employees. However, to avoid over-use, inappropriate use, and the potential for viruses, the distribution list must only be used by Directors and authorized Management personnel.
- i) All emails are saved on the server which is backed up each night. To ensure the system continues to operate efficiently, employees must perform periodic cleanup of their email folders by deleting or archiving emails from the Inbox, Sent, Draft and Deleted folders.
- j) Unacceptable and prohibited use of the email system includes, but is not limited to the creation or sending of:
  - Information which could be considered by any reader to be obscene, racist, sexist, culturally disrespectful or otherwise offensive;
  - creating or sending disruptive messages that:



- adversely affect the operation of the computer network,
  - reduce a person's ability to perform Agency work;
  - solicitation for non-Agency related business;
  - messages that intentionally misrepresent the identity of the sender;
  - harassing or threatening messages;
  - material that is illegal in any way
- k) Employees who receive a large number of unsolicited emails (often called SPAM) of an offensive or disruptive nature are expected to notify the system administrator who can take steps to block the sender(s).
- l) Personal email accounts, i.e., Hotmail, Gmail etc., are not to be used for any work-related correspondence.
- m) The email account will be closed immediately if an employee is no longer employed by the Agency.

## **6. Direct Messaging**

- a) Communication between employees via text messaging, chats or instant messaging on an Agency or personally owned device should be limited to non-identifying matters that maintain the privacy of people supported and employees.
- b) Messaging through Agency provided communication applications (such as Microsoft Teams) should be carried out in a professional, respectful manner and in accordance with the User Guide for each.
- c) The Agency reserves the rights to audit, intercept, and access and disclose all messages created, received or sent through Agency provided communication applications for any purpose.

## **7. Internet**

- a) Internet access is intended to support Agency operations. Employees are permitted to access Agency Wi-Fi on their personal smartphone for work-related purposes during their shift.
- b) Only the Agency IT service provider, as approved by the Director, Marketing and Innovation or designate, is authorized to install and manage an internet/network connection (wired or wireless) for Agency business in any location owned, rented or leased by the Agency.
- c) Downloading of software or executable files from the Internet is not permitted without prior approval from the Director, Marketing and Innovation or designate.
- d) Transmissions to and from the internet may be audited by the Agency without the consent of the user and with no advance notice. Auditing includes, but is not limited to, tracking

internet sites visited, the content of information or messages sent and received, and the amount of time spent using the internet.

- e) The Agency hosts a website which provides employees access to a variety of information including job postings, newsletters, policies and forms through a password protected intranet. This information is intended for employees only. Employees must not grant others access to this site.

## **8. Mobile Devices**

- a) Agency mobile devices are assigned to designated employees, locations and vehicles for reasons of safety, program delivery and Agency business.
- b) The Director, Marketing and Innovation or designate will be responsible for acquisition, disposal and maintaining a record of all Agency owned mobile devices using Agency mobile device management software.
- c) All mobile devices accessing Agency information must be password-protected and used in ways consistent with Agency policies and procedures.
- d) Use of mobile devices must never interfere with work responsibilities, the provision of services, interaction with those being supported or the maintaining of a safe environment.
- e) Employees are prohibited from using any hand-held mobile/electronic device while operating a motor vehicle. Calls to 911 are exempt from this policy.
- f) Agency owned mobile devices must be kept secured and not left unattended.
- g) All management employees must read and sign the Personal Smartphone Memo, obtained from Human Resources, if they wish to use the Agency issued mobile device for purposes beyond fulfilling work duties.
- h) All lost or stolen Agency-owned communication devices, which store Agency information or are connected to its networks, must be reported immediately to the Director, Marketing and Innovation or designate as it may be a Ministry reportable serious occurrence. If a breach of confidentiality is likely, the Director, Marketing and Innovation may remotely delete all data on the device, including personal data (texts, images and video).
- i) Employees must secure their mobile device and set it to lock after a minimum of three (3) minutes of inactivity.

## **9. Personal Electronic Devices**

- a) The Agency recognizes that personal electronic/mobile devices can assist employees during their workday. It is critical that employees remain attentive to the requirements of their position and avoid unnecessary distractions. All usage of personal electronic/mobile devices at work must be approved by a Manager (see Personal Property [PER-100-10])

policy).

- b) Employees who wish to use their personal device for Agency business must read and sign the Information Technology Policy Acknowledgement (ADMIN22).
- c) If an employee loses a personal device that has usernames or passwords on it for Agency systems, the employee must immediately report it to the Director, Marketing and Innovation or the Manager, Technology and New Media.
- d) Any person leaving the employ of the Agency must delete all Agency-related data from any personal devices in their possession.

## 10. Enterprise Software

Enterprise software, where multiple users access a central data pool and the data pool contains confidential information, shall be assessed by the Director, Marketing and Innovation and the Executive Director before implementation and reviewed on an ongoing basis.

## 11. Security

- a) Agency-owned computers and mobile devices will be configured for hardware logon access and hard drives will be locked to prevent data capture.
- b) Users will connect via a secure session to the Agency's infrastructure using their assigned username and password.
- c) The Agency will utilize a secure data centre for all self-hosted data and programs. For all cloud-based services and applications, security measures including user authentication, advanced threat protection, data encryption, data residency and backups will be reviewed and approved by the Director, Marketing and Innovation prior to implementation.
- d) Data backups are run daily. All information and services will be backed up to an off-site location or secure cloud service.
- e) Servers will be monitored remotely by a contracted IT service provider for event management. Hardware and software maintenance as well as upgrades as recommended by the IT service provider will be reviewed and approved by the Director, Marketing and Innovation or designate.
- f) All Agency computers and mobile devices shall have an approved anti-virus program installed and scheduled to run at regular intervals.
- g) Director, Marketing and Innovation or designate is responsible to ensure there is a system for data/disaster recovery and to periodically review the plan.

- h) Users will adhere to warnings and practices set by the Director, Marketing and Innovation or designate in order to minimize computer virus attacks. Do not open emails and attachments from unknown senders.
- i) Any user who suspects the security of the network has been compromised must immediately report the suspected breach to their Manager who will inform the Director, Marketing and Innovation or designate.
- j) Users must ensure that they have logged out or locked their computer/mobile device before leaving it unattended.

## **12. Remote Access**

Employees must ensure security measures are taken when working remotely to guard against:

- the physical loss or theft of Agency information or IT equipment/mobile devices
- inappropriate access by non-employees (e.g., family members)
- loading and/or transferring data onto home or personal devices
- communicating information through unprotected channels. Wireless security measures must be used.
- printing information with inappropriate disposal options

## **13. Training**

The Agency will provide training in the effective use of its information technology and the operation, security and safe keeping of electronic devices to meet work requirements.

## **14. Monitoring and Reporting**

- a) The Director, Marketing and Innovation or designate will audit the IT system for unauthorized and/or unprofessional activities, proper use of equipment and monitor and/or capture statistics including but not limited to usage habits, keystrokes and content.
- b) In the event of a breach of confidentiality (the loss or misplacement of unprotected personal information) including paper documents, information stored on a laptop, portable information storage device, mobile communication device, or any other electronic device that is not encrypted and/or protected as required by policy related to the personal information of a person supported, a Serious Occurrence Report (PROG70) form must be completed.
- c) If the Agency is presented with an order from a law enforcement Agency or other legislative authority for access to an employee's personal information and usage contained on any Agency equipment, the request will be referred to the Agency's Privacy Officer in accordance with the Privacy and Protection of Personal Information [ADM-100-17] policy.
- d) The Director, Marketing and Innovation or designate will monitor monthly usage for billing and budgeting purposes.

**Policy & Procedure**

**Policy # ADM-100-17**

Section: General

Approved On: November 5, 2008

---

**PRIVACY AND PROTECTION OF PERSONAL INFORMATION**

---

**POLICY STATEMENT**

Community Living Essex County is committed to maintaining confidentiality and protecting the privacy of the personal information it collects, uses or discloses on behalf of the people we support, Employees we hire or other people who interact with us throughout the course of our activities. Compliance will be maintained with all relevant legislation including the Personal Information Protection and Electronic Documents Act of Canada (PIPEDA) and Personal Health Information Protection Act (Ontario) (PHIPA).

**SCOPE**

To preserve the confidentiality of personal information we collect and the privacy of the people we support/families and Employees, this policy outlines Employee obligations and the procedures to be followed when dealing with such personal, privileged and/or confidential information. This policy applies to all Employees and to anyone who is granted access to personal, privileged and/or confidential information about a person supported and/or about Employees.

This policy addresses two (2) broad issues:

1. The way in which Community Living Essex County collects, uses, discloses and protects personal information as well as privileged and confidential information.
2. The right of the people supported/families and Employees or a third party to have access to personal information, and if necessary, to correct the information.

**DEFINITIONS**

**Person**

A person we support, a member of their family, guardian, trustee, an Employee, a volunteer, a person being recruited to support one of our fundraising initiatives or others we do business with, and any person from whom or about whom we collect personal information.

**Personal Information**

Personal information is factual or subjective information, recorded or not, about an identifiable person. It includes, but is not limited to, name, home address, telephone numbers, age, sex, marital or family status, identifying numbers such as social insurance number, drivers licence or passport, race, national or ethnic origin, colour, religious or political beliefs or associations, educational history, medical history, disabilities, blood type, employment history, financial

history, criminal history, anyone else's opinions about a person, a person's personal views or opinions, and name, address and phone number of parent, guardian, spouse or next of kin.

### **Consent**

The knowledge and consent of the person are required for the collection, use or disclosure of personal information. Consent is obtained from the person about to receive supports or the new Employee, to collect, store, use and exchange or disclose personal information for the purposes stated herein at the time of acceptance of service or in the hiring agreement. This consent may be express or implied.

### **Personal Health Information**

Personal health information means information about an identifiable person that relates to the physical or mental health of the person, the provision of healthcare to the person, the person's entitlement to payment for healthcare, the person's healthcare number, the identity of providers of healthcare to the person or the identity of substitute decision-makers on behalf of a person.

### **Third Party**

Third party means individuals or organizations other than the subject of the records or representatives of Community Living Essex County who may request or provide personal information.

## **LEGAL REQUIREMENTS**

Community Living Essex County will do its utmost to abide by the ten fair information principles of PIPEDA.

### **1. Accountability/Privacy Officer**

The Privacy Officer is responsible for ensuring that Community Living Essex County is in compliance with the PIPEDA and PHIPA and the policy and procedures contained therein. The Director, Human Resources is designated as the Privacy Officer.

### **2. Purpose of the Collection of Personal Information**

Personal information is collected by Community Living Essex County from a person. The purpose for which personal information is collected shall be identified at or before the time the information is collected. All personal information is used for one or more of the following purposes:

- a) confirm the person's identity, communicate with the person, respond to inquiries from the person, to provide the person with support and services, to fulfil the legal and business requirements of the Community Living Essex County and/or to ask for their financial support and to provide donor recognition for charitable gifts;
- b) to determine eligibility of a person to receive support and services or to be offered employment;

- c) to fulfil legislated and reporting requirements (such as but not limited to, Ontario Disability Support Program, Canada Pension Plan, Employment Insurance, Income Tax);
- d) to provide a high quality of support;
- e) to protect people receiving support, Employees and Community Living Essex County from illegal activity;
- f) to provide information about educational seminars or workshops, notice of professional development, career or volunteer opportunities or participation in special interest groups;
- g) to support research, analysis and overall management of supports and services;
- h) from time to time personal information may be shared with third party vendors, suppliers, data processors, and other providers responsible for administering supports or services on behalf of the person and ensure the health and safety of the person. Any such third party will be required to have policies in place regarding the collection and use of personal information which are consistent with this policy.

### 3. Consent

The knowledge and express or implied consent of the person are required for the collection, use or disclosure of personal information. Consent is obtained from the person about to receive supports or the new Employee, to collect, store, use and exchange or disclose personal information for the purposes stated herein at the time of acceptance of service or in the hiring agreement. See Confidentiality / Release of Confidential Information (ADM-100-04) policy.

### 4. Limiting Collection of Information

The personal information collected is limited to what is necessary to achieve the purposes stated above, in **2. Purpose of the Collection of Personal Information**. The collection of information will be by open, fair and lawful means. The method of collection may include, but is not limited to, from the person, in person, over the telephone, by fax or by correspondence via mail or e-mail or on the internet through our website or by any other means.

### 5. Limiting Use, Disclosure and Retention of Information

Personal information will only be used for the purpose stated above, in **2. Purpose of Collection of Personal Information**. A separate explicit consent is obtained from the person or unless required or allowed by law. If a person's personal information is disclosed or exchanged with a third party, such as another service provider, Community Living Essex County will take reasonable steps to ensure that such party agrees to comply with the provisions of PIPEDA and PHIPA. A person's personal information will be retained as long as necessary to achieve the stated purposes and to comply with legislation and regulations regarding records retention. When information is no longer required to be kept, this Agency

will follow policies and procedures as stated in Management of Individual Records (PRO-300-03) and Personnel Records (PER-100-07). Privacy statements to protect personal information may be used on various forms.

## **6. Accuracy**

All best efforts will be taken to maintain the accuracy and currency of all personal information contained in our files and to update such information when advised by the person of a change.

## **7. Safeguards**

Community Living Essex County commits to doing its utmost to protect the personal information in its possession from unauthorized access, disclosure, copying, use, error, loss or modification. Personal information about a person, both paper and electronic, will be stored in files to which only authorized personnel have access. The storage area will be locked and computer files protected by passwords. All Employees and members of the Board of Directors must sign an Oath of Confidentiality (PER06) in which they acknowledge their duties subject to this and the Rules of Conduct (PER-100-04) policy.

## **8. Openness**

A copy of this policy will be posted on the website. Copies are available at each location operated by the Agency and further, copies are available upon request from the Privacy Officer.

## **9. Individual Access**

All persons shall have access to the files containing their personal information, as per the Personnel Records (PER-100-07) and Management of Individual Records (PRO-300-03) policies.

## **10. Challenging Compliance**

A person who has a complaint concerning compliance with these principles shall address the complaint to the Privacy Officer. The procedures are set out under Complaint Procedures.

## **RESPONSIBILITY**

Privacy Officer is responsible for:

- receiving and responding to questions/complaints regarding privacy;
- internal compliance with applicable policies and legislation;
- act as a resource in developing internal policies for the collection, use and disclosure of personal information, personal health information and other confidential data; and
- through established policies and training; ensure appropriate consents are obtained for the collection, use and disclosure of personal information and third party requests.

Management is responsible for:

- through established policies and training, ensure appropriate consents are obtained for the collection, use and disclosure of personal information and third party requests;
- policies and procedures regarding collection, use and disclosure of personal information are consistently adhered to;



- that systems and procedures are in place to ensure records are kept private;
- requests from persons for access to their files are responded to;
- proper disposal of unnecessary files/information as per policy;
- cooperation with the Privacy Officer to investigate complaints or breaches of policy;
- that disclosure of personal information or personal health information to a third party is done with the approval of a Director in order to minimize the risk of non-compliance with applicable legislative or regulatory regimes;
- ensuring this policy is explained to the people we support, their families and others and referring them to the Privacy Officer if necessary; and
- ensuring that Employees return any personal, privileged and/or confidential information in their possession upon request, or before or immediately upon, termination of employment.

Employees are responsible for:

- understanding and following policies and procedures regarding personal, privileged and/or confidential information;
- keeping their own Employee files current regarding their personal information; including consent to disclose;
- immediately reporting any breaches of confidentiality to the Privacy Officer;
- keeping private passwords and access to personal information privileged and confidential;
- explaining this policy to the people we support, their families and others and referring them to the Privacy Officer if necessary; and
- returning to management, any personal, privileged and/or confidential information in their possession upon request, or before or immediately upon, termination of employment.

## **COMPLAINT PROCESS**

Questions or complaints regarding a breach in privacy may be resolved by following the Appeals Process for Individuals / Families (PRO-200-05) or the Employee Concern Process (PER-100-03) policies or by contacting the Privacy Officer who will assist you through the process.

|                                                                                   |                                                |                    |                  |
|-----------------------------------------------------------------------------------|------------------------------------------------|--------------------|------------------|
|  |                                                |                    |                  |
| <b>STATEMENT of POLICY and PROCEDURE</b>                                          |                                                |                    |                  |
| Manual:                                                                           | Program, Board                                 | SPP No.            | <b>PRG 22.16</b> |
| Section:                                                                          | Information Technology                         | Issued:            | June 2022        |
| Subject:                                                                          | <b>Generative Artificial Intelligence (AI)</b> | Replaces:          |                  |
| Issue to:                                                                         | All Manual Holders                             | Page:              | I of 5           |
|                                                                                   |                                                | Procedure Revised: |                  |
| Issued by:                                                                        | Board of Directors                             | Dated:             | Feb 23, 2023     |

## 1 POLICY

- 1.01 Community Living Chatham-Kent shall empower employees to explore and promote the use of new technologies that help to achieve our goal, mission, and vision, so long as they continue to provide value and maintain compliance with other organizational policies as determined by management.

## 2 PURPOSE

The purpose of this Statement of Policy and Procedure is to offer guidelines on how Community Living Chatham-Kent employees shall use Generative AI, and similar large language models designed to assist with tasks and answer questions in the workplace. The purpose of this policy is to ensure that the use of Generative AI aligns with the organization's goals, values, and ethical standards, while ensuring that privacy, confidentiality, and security are protected.

## 3 SCOPE

- 3.01 This policy applies to all employees.

## 4 RESPONSIBILITY

- 4.01 Employees are responsible for following the procedures outlined in this policy and for asking questions of their manager or the IT department when unsure.
- 4.02 Information Systems is responsible for training and educating employees in the responsible use of Generative AI and similar technologies.

|                                                                                   |                                                |                    |                  |
|-----------------------------------------------------------------------------------|------------------------------------------------|--------------------|------------------|
|  |                                                |                    |                  |
| <b>STATEMENT of POLICY and PROCEDURE</b>                                          |                                                |                    |                  |
| Manual:                                                                           | Program, Board                                 | SPP No.            | <b>PRG 22.16</b> |
| Section:                                                                          | Information Technology                         | Issued:            | June 2022        |
| Subject:                                                                          | <b>Generative Artificial Intelligence (AI)</b> | Replaces:          |                  |
| Issue to:                                                                         | All Manual Holders                             | Page:              | 2 of 5           |
|                                                                                   |                                                | Procedure Revised: |                  |
| Issued by:                                                                        | Board of Directors                             | Dated:             | Feb 23, 2023     |

## 5 DEFINITIONS

- 5.01 **Artificial Intelligence (AI)** – Artificial intelligence refers to computer systems that can perform tasks that would typically require human intelligence such as learning, problem-solving, decision-making, and pattern recognition.
- 5.02 **AI Ethics** – An area of study in the field of AI that ensures systems respond in ways that are beneficial and avoid things such as bias, racism, sexism, etc. that may have been found in the language used to train it.
- 5.03 **Chatbot** - a computer program designed to simulate conversation with human users, especially over the internet.
- 5.04 **ChatGPT** – A natural language chat model developed by OpenAI that provides responses to questions using language that sounds like a normal conversation with a person.
- 5.05 **Copilot** – A Microsoft product similar to ChatGPT and using the same architecture.
- 5.06 **Gemini** – A Google product recently introduced to the Canadian market.
- 5.07 **Generative AI** – refers to artificial intelligence systems that can generate new content, such as text, images, and music, based on their training data and specific inputs given to them.
- 5.08 **Generative Pretrained Transformer (GPT)** – A language model relying on deep learning that can generate human-like texts based on a given text-based input. A user “feeds” the model with a sentence, and the transformer creates coherent paragraph-based information extracted from publicly available datasets.
- 5.09 **Large Language Model (LLM)** – An AI model that is trained on massive collections of existing information/text to use as a basis for responding to questions.
- 5.10 **Natural Language Processing (NLP)** – A natural language model is a type of artificial intelligence that uses neural networks to process and generate human-like language at a massive scale. Rather than using ‘key words’ to trigger specific responses, these models communicate using normal speech patterns and context.

## 6 REFERENCES and RELATED STATEMENTS of POLICY and PROCEDURE

22.07 Systems, Internet, and Email Acceptable Use

|                                                                                   |                                                |                    |                  |
|-----------------------------------------------------------------------------------|------------------------------------------------|--------------------|------------------|
|  |                                                |                    |                  |
| <b>STATEMENT of POLICY and PROCEDURE</b>                                          |                                                |                    |                  |
| Manual:                                                                           | Program, Board                                 | SPP No.            | <b>PRG 22.16</b> |
| Section:                                                                          | Information Technology                         | Issued:            | June 2022        |
| Subject:                                                                          | <b>Generative Artificial Intelligence (AI)</b> | Replaces:          |                  |
| Issue to:                                                                         | All Manual Holders                             | Page:              | 3 of 5           |
|                                                                                   |                                                | Procedure Revised: |                  |
| Issued by:                                                                        | Board of Directors                             | Dated:             | Feb 23, 2023     |

### 9.32 Privacy Breach

## 7 PROCEDURES

### 7.01 **Approved Platforms:**

Generative AI systems not included in the list below should be directed to Information Systems for review prior to using them for work purposes.

Currently approved platforms include:

OpenAI ChatGPT

<https://chat.openai.com/>

Microsoft Copilot

<https://copilot.microsoft.com/>

Google Gemini

<https://gemini.google.com/>

**7.02 Confidentiality:** This policy applies to all information about Community Living Chatham-Kent that is not publicly available. Examples of confidential information include financial data, proprietary information, information about people who access services, and employee data. Employees shall not disclose any confidential information, even if they believe it is harmless or insignificant. If an employee is unsure about whether the information is confidential or not, they shall consult their manager or the Information Systems Manager.

**7.03 Respect:** This policy applies to all interactions with Generative AI, whether verbal or written. Employees shall use professional language when communicating with Generative AI and shall not use abusive, offensive, or discriminatory language.

**7.04 Accuracy:** Generative AI is a powerful tool, but it is not perfect. Employees shall use

|                                                                                   |                                                |                    |                  |
|-----------------------------------------------------------------------------------|------------------------------------------------|--------------------|------------------|
|  |                                                |                    |                  |
| <b>STATEMENT of POLICY and PROCEDURE</b>                                          |                                                |                    |                  |
| Manual:                                                                           | Program, Board                                 | SPP No.            | <b>PRG 22.16</b> |
| Section:                                                                          | Information Technology                         | Issued:            | June 2022        |
| Subject:                                                                          | <b>Generative Artificial Intelligence (AI)</b> | Replaces:          |                  |
| Issue to:                                                                         | All Manual Holders                             | Page:              | 4 of 5           |
|                                                                                   |                                                | Procedure Revised: |                  |
| Issued by:                                                                        | Board of Directors                             | Dated:             | Feb 23, 2023     |

their own judgment when using information provided by Generative AI and shall not rely on it blindly. If an employee has doubts about the accuracy of the information, they shall verify it with a manager or other reliable sources.

- 7.05 **Bias:** Generative AI may include biases or misrepresented information based on past training data. It's important to understand that responses could include content that may be offensive to some, which is not the overall intent of use.
- 7.06 **Business Purpose:** This policy applies to all uses of Generative AI, including internal and external communications. Employees shall not use Generative AI for personal reasons, such as personal research or leisure activities while on paid time. If an employee is unsure about whether a particular use of Generative AI is appropriate, they shall consult their manager.
- 7.07 **Security:** This policy applies to all aspects of Generative AI security, including access credentials, data storage, and network connections. Employees shall take appropriate measures to protect the security of Generative AI, such as using strong passwords and avoiding public Wi-Fi networks and enabling 2FA if available. If an employee suspects that their account has been compromised, they shall notify their manager immediately.
- 7.08 **Data Protection:** This policy applies to all data collected or processed by Generative AI, including personal data. Employees shall use a work email address when registering for Generative AI when using it for work-related activities to better separate any work-related use from personal. Any information generated by Generative AI shall be stored in other documents for archive. While it is a current feature, we shall not expect Generative AI platforms to retain data on behalf of the user or agency.
- 7.09 **Training:** Community Living Chatham-Kent shall provide appropriate training to all employees who will be using Generative AI. This training shall cover the guidelines outlined in this policy, as well as any other relevant policies and procedures. Employees shall receive regular updates and refresher training as needed.

|                                                                                                                    |                                                |                    |                  |
|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------------|------------------|
| COMMUNITY LIVING<br>Chatham-Kent  |                                                |                    |                  |
| <b>STATEMENT of POLICY and PROCEDURE</b>                                                                           |                                                |                    |                  |
| Manual:                                                                                                            | Program, Board                                 | SPP No.            | <b>PRG 22.16</b> |
| Section:                                                                                                           | Information Technology                         | Issued:            | June 2022        |
| Subject:                                                                                                           | <b>Generative Artificial Intelligence (AI)</b> | Replaces:          |                  |
| Issue to:                                                                                                          | All Manual Holders                             | Page:              | 5 of 5           |
|                                                                                                                    |                                                | Procedure Revised: |                  |
| Issued by:                                                                                                         | Board of Directors                             | Dated:             | Feb 23, 2023     |

- 7.10 **Compliance:** Employees who violate this policy or any other relevant policies and procedures may be subject to disciplinary action, up to and including termination. Community Living Chatham-Kent may also monitor the use of Generative AI to ensure compliance with this policy and to identify any areas where additional training or support may be needed.

## 8 ATTACHMENTS

None



**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot

**First Name**  
**Last Name**



Team Microsoft CoPilot





## Scenario Worksheet for Group Exercise: Writing and Revising Prompts & Verifying and Editing AI Outputs

### Topic #1: Create a Travel Itinerary

#### Scenario Description:

A person you support wants to plan a vacation to someplace warm and tropical so they can enjoy some swimming, visiting beaches, and sight-seeing. They would like to go for 3 nights and require accessible accommodation. They have a budget of \$3000 to work with to cover their and staff's expenses while on vacation including transportation, accommodation, food, and entertainment. Use ChatGPT to help the person determine what destination they would like to visit according to their interests.

**GROUP ACTION STEP #1: Draft a request/prompt for AI to complete the task and run it.**

*Once you're done move on to Step #2.*

**GROUP ACTION STEP #2: Ask it to modify your request/prompt and run it again.**

**Things to Consider** (*can your prompt be modified to address any of the following, as applicable?*)

- ✓ **Unique needs of the person**
- ✓ **Barriers that need to be overcome or addressed**
- ✓ **Budget constraints**
- ✓ **Alignment with agency values and mission**
- ✓ **Other**

*Done? Move on to Step #3.*

**GROUP ACTION STEP #3: Read the revision below and further modify your prompt accordingly and run it again.**

#### **Revision:**

The person wants to be able to see some wildlife on their trip. Modify your search for entertainment to include some type of animal interaction activity.

*Done? Move on to Step #4.*

**GROUP ACTION STEP #4: Discuss as a group whether the final AI output is ready for implementation/use. Does it require editing, verification, or additional information? No computer work is needed here.**

**Verification and Editing Tips:**

- ✓ Does the output require a human touch? (i.e. add language to convey thoughtfulness, care, etc.)
- ✓ Is the output free of bias?
- ✓ Does the output meet workplace/professional standards?
- ✓ Does the output contain language typically used at work?
- ✓ Does it need to be simplified or summarized?
- ✓ Is there anything contained in the output that needs to be fact-checked with a reliable source?

*Done? Move on to Step #5.*

**GROUP ACTION STEP 5: Present to the class!**

1. Give a short summary of your group's scenario.
2. What was the AI request or prompt that you entered?
3. How did you revise your prompt based on the new information?
4. How did you protect the privacy and confidentiality of the person you are supporting or the employee?
5. What (if anything) needs to be done with the AI output before you use this in supports and/or documentation?



## Scenario Worksheet for Group Exercise: Writing and Revising Prompts & Verifying and Editing AI Outputs

### Topic #2: Personal Outcomes Plan – SMART Goals

#### Scenario Description:

You are supporting Sam, a 30-year-old who is interested in getting into better shape with the goal of walking their first 5km race in 12 months at race event. Use ChatGPT to help create a SMART (Specific, Measurable, Achievable, Relevant, Time-Bound) goal with Sam and help them move towards their goal of completing their first race.

**GROUP ACTION STEP #1: Draft a request/prompt for AI to complete the task and run it.**

*Once you're done move on to Step #2.*

**GROUP ACTION STEP #2: Ask it to modify your request/prompt and run it again.**

**Things to Consider** (*can your prompt be modified to address any of the following, as applicable?*)

- ✓ **Unique needs of the person**
- ✓ **Barriers that need to be overcome or addressed**
- ✓ **Budget constraints**
- ✓ **Alignment with agency values and mission**
- ✓ **Other**

*Done? Move on to Step #3.*

**GROUP ACTION STEP #3: Read the revision below and further modify your prompt accordingly and run it again.**

#### **Revision:**

Sam has limited mobility and uses a walker.

*Done? Move on to Step #4.*

**GROUP ACTION STEP #4: Discuss as a group whether the final AI output is ready for implementation/use. Does it require editing, verification, or additional information? No computer work is needed here.**

**Verification and Editing Tips:**

- ✓ Does the output require a human touch? (i.e. add language to convey thoughtfulness, care, etc.)
- ✓ Is the output free of bias?
- ✓ Does the output meet workplace/professional standards?
- ✓ Does the output contain language typically used at work?
- ✓ Does it need to be simplified or summarized?
- ✓ Is there anything contained in the output that needs to be fact-checked with a reliable source?

*Done? Move on to Step #5.*

**GROUP ACTION STEP 5: Present to the class!**

1. Give a short summary of your group's scenario.
2. What was the AI request or prompt that you entered?
3. How did you revise your prompt based on the new information?
4. How did you protect the privacy and confidentiality of the person you are supporting or the employee?
5. What (if anything) needs to be done with the AI output before you use this in supports and/or documentation?



## Scenario Worksheet for Group Exercise: Writing and Revising Prompts & Verifying and Editing AI Outputs

### **Topic #3: Menu Planning**

#### **Scenario Description:**

As part of your role, you are responsible for working with the people you support to create a menu for each month, keeping in mind Canada's Food Guide recommendations. You support the three young men that live together who rely on this menu for their daily nutritional needs. Use Chat GPT to help create a 2-week menu for the men.

**GROUP ACTION STEP #1: Draft a request/prompt for AI to complete the task and run it.**

*Once you're done move on to Step #2.*

**GROUP ACTION STEP #2: Ask it to modify your request/prompt and run it again.**

**Things to Consider** (*can your prompt be modified to address any of the following, as applicable?*)

- ✓ **Unique needs of the person**
- ✓ **Barriers that need to be overcome or addressed**
- ✓ **Budget constraints**
- ✓ **Alignment with agency values and mission**
- ✓ **Other**

*Done? Move on to Step #3.*

**GROUP ACTION STEP #3: Read the revision below and further modify your prompt accordingly and run it again.**

#### **Revision:**

Ask ChatGPT to create a grocery list and provide recipes for the menu.

*Done? Move on to Step #4.*

**GROUP ACTION STEP #4: Discuss as a group whether the final AI output is ready for implementation/use. Does it require editing, verification, or additional information? No computer work is needed here.**

**Verification and Editing Tips:**

- ✓ Does the output require a human touch? (i.e. add language to convey thoughtfulness, care, etc.)
- ✓ Is the output free of bias?
- ✓ Does the output meet workplace/professional standards?
- ✓ Does the output contain language typically used at work?
- ✓ Does it need to be simplified or summarized?
- ✓ Is there anything contained in the output that needs to be fact-checked with a reliable source?

*Done? Move on to Step #5.*

**GROUP ACTION STEP 5: Present to the class!**

1. Give a short summary of your group's scenario.
2. What was the AI request or prompt that you entered?
3. How did you revise your prompt based on the new information?
4. How did you protect the privacy and confidentiality of the person you are supporting or the employee?
5. What (if anything) needs to be done with the AI output before you use this in supports and/or documentation?



## Scenario Worksheet for Group Exercise: Writing and Revising Prompts & Verifying and Editing AI Outputs

### Topic #4: Committee - Employee Engagement

#### Scenario Description:

You have been tasked with planning a 2-day employee appreciation event for agency employees. You need venue, food, entertainment and activities. Your budget is \$5000.

**GROUP ACTION STEP #1: Draft a request/prompt for AI to complete the task and run it.**

*Once you're done move on to Step #2.*

**GROUP ACTION STEP #2: Ask it to modify your request/prompt and run it again.**

**Things to Consider** (*can your prompt be modified to address any of the following, as applicable?*)

- ✓ Unique needs of the person
- ✓ Barriers that need to be overcome or addressed
- ✓ Budget constraints
- ✓ Alignment with agency values and mission
- ✓ Other

*Done? Move on to Step #3.*

**GROUP ACTION STEP #3: Read the revision below and further modify your prompt accordingly and run it again.**

#### **Revision:**

The event will only be held for 4 hours each day, and your budget was cut to \$3500.

*Done? Move on to Step #4.*



**GROUP ACTION STEP #4: Discuss as a group whether the final AI output is ready for implementation/use. Does it require editing, verification, or additional information? No computer work is needed here.**

**Verification and Editing Tips:**

- ✓ Does the output require a human touch? (i.e. add language to convey thoughtfulness, care, etc.)
- ✓ Is the output free of bias?
- ✓ Does the output meet workplace/professional standards?
- ✓ Does the output contain language typically used at work?
- ✓ Does it need to be simplified or summarized?
- ✓ Is there anything contained in the output that needs to be fact-checked with a reliable source?

*Done? Move on to Step #5.*

**GROUP ACTION STEP 5: Present to the class!**

1. Give a short summary of your group's scenario.
2. What was the AI request or prompt that you entered?
3. How did you revise your prompt based on the new information?
4. How did you protect the privacy and confidentiality of the person you are supporting or the employee?
5. What (if anything) needs to be done with the AI output before you use this in supports and/or documentation?





## Scenario Worksheet for Group Exercise: Writing and Revising Prompts & Verifying and Editing AI Outputs

### **Topic #5: Community Partner Communication**

#### **Scenario Description:**

Use ChatGPT to assist you in writing an e-mail to RSA. This email should include the following: staff noting new challenging behaviour the person supported is experiencing (self-injurious behaviors in the form of headbanging and picking skin) and you would like guidance in how to proceed. Ask them for an updated data sheet. You also want to request an in-person meeting with the entire support team to go over strategies together.

**GROUP ACTION STEP #1: Draft a request/prompt for AI to complete the task and run it.**

*Once you're done move on to Step #2.*

**GROUP ACTION STEP #2: Ask it to modify your request/prompt and run it again.**

**Things to Consider** (*can your prompt be modified to address any of the following, as applicable?*)

- ✓ **Unique needs of the person**
- ✓ **Barriers that need to be overcome or addressed**
- ✓ **Budget constraints**
- ✓ **Alignment with agency values and mission**
- ✓ **Other**

*Done? Move on to Step #3.*

**GROUP ACTION STEP #3: Read the revision below and further modify your prompt accordingly and run it again.**

#### **Revision:**

Include that the person supported has had an increase in PRN usage and has had one trip to the hospital due to SIB's. Note that this person recently experienced the loss of their family pet.

*Done? Move on to Step #4.*

**GROUP ACTION STEP #4: Discuss as a group whether the final AI output is ready for implementation/use. Does it require editing, verification, or additional information? No computer work is needed here.**

**Verification and Editing Tips:**

- ✓ Does the output require a human touch? (i.e. add language to convey thoughtfulness, care, etc.)
- ✓ Is the output free of bias?
- ✓ Does the output meet workplace/professional standards?
- ✓ Does the output contain language typically used at work?
- ✓ Does it need to be simplified or summarized?
- ✓ Is there anything contained in the output that needs to be fact-checked with a reliable source?

*Done? Move on to Step #5.*

**GROUP ACTION STEP 5: Present to the class!**

1. Give a short summary of your group's scenario.
2. What was the AI request or prompt that you entered?
3. How did you revise your prompt based on the new information?
4. How did you protect the privacy and confidentiality of the person you are supporting or the employee?
5. What (if anything) needs to be done with the AI output before you use this in supports and/or documentation?

**Below, please find an e-mail sent to all employees announcing the Generative AI training module and lab, with additional information.**

---

**From:** Julie LaSorda [REDACTED]  
**Sent:** Thursday, October 5, 2023 4:25 PM  
**To:** all [REDACTED]  
**Subject:** A Message from the AI Working Group - AI Labs Registration  
**Importance:** High

Good afternoon,

The AI (Artificial Intelligence) Working Group has been busy preparing an introduction to AI for our employees and a policy to govern its use. You may already be familiar with generative AI tools like ChatGPT and BingChat.

AI is simply another tool we can make use of to do things, such as:

- achieve efficiencies in administrative work
- generate ideas
- increase productivity
- expedite repetitive or time-consuming tasks
- enhance the quality of our written work
- assist us with planning and the preparation of documents

AI must be approached with caution, as there are some risks associated with its use. There has been no shortage of news headlines regarding AI over the past 6 months – both good and bad. Rather than ignore it, we must address it, issue policy, and provide our employees with training to ensure it's used safely and wisely.

**The AI Working Group has developed an AI policy and it will be released to all employees on Monday, October 23<sup>rd</sup> along with an informative OTR Training Module.**

To further support the introduction of AI in our organization, **the AI Working Group will be offering AI Labs in phases over the next 6 months, beginning the week of October 30<sup>th</sup>.**

#### **What are AI Labs?**

Small classroom style, hands-on learning sessions to help you become more familiar with AI, its potential benefits, and how to use it responsibly and in compliance with our policy.

**Our first round of AI Labs will begin Monday, October 30<sup>th</sup> and will be offered to SSW, FT, PT2, and Admin and HR Officers.** There will be 9 sessions, each 3 hours in length, held at the Riverdance Community Centre on Front Rd in LaSalle. You do not need to bring anything to the session. We will offer AI Labs again in early January 2024 and April 2024 to everyone who is not participating in this first phase.

All managers will be participating in an AI Lab on Friday, October 20<sup>th</sup>. Managers must bring their own laptop. In all other AI Labs laptops will be provided.

#### **Session Dates and Times are as follows (20 participants per session):**

Monday, October 30<sup>th</sup>

8:30 am – 11:30am

12:30pm – 3:30pm

4:30pm – 7:30pm

Wednesday, November 1<sup>st</sup>

8:30am – 11:30am

12:30pm – 3:30pm

4:30pm – 7:30pm

Thursday, November 2<sup>nd</sup>

8:30am – 11:30am

12:30pm – 3:30pm

4:30pm – 7:30pm

**If you are a SSW, FT, PT2, or an Admin or HR Officer, please sign up for one of the sessions using this [link](#) no later than Thursday, October 12<sup>th</sup>.** To avoid disruption at support locations, please try to arrange so that there are not multiple people from your location attending the same session.

Thank you for your attention to this deadline and we look forward to seeing you!

Julie on behalf of the AI Working Group

Below, please find an e-mail sent to all employees asking interested staff to secure their spot in the Generative AI Lab by registering for one of the available sessions.

---



**Don't wait... Register now to secure a spot in the AI Labs!**

Spots for our second session of labs are filling up! Register today to secure your spot in one of the AI Labs and explore the potential of using this technology in the workplace! Sessions will be held at the Essex Centre.

**Register Now!**

**The remaining session dates and times are listed below:**

**Tuesday, January 16<sup>th</sup>**

- 4:30pm – 7:30pm (5 spots left)

**Wednesday, January 17<sup>th</sup>**

- 4:30pm – 7:30pm

**Thursday, January 18<sup>th</sup>**

- 8:30am – 11:30am
- 12:30pm – 3:30pm (5 spots left)
- 4:30pm – 7:30pm

**Please sign up for one of the sessions no later than Thursday, December 7<sup>th</sup>.**

To avoid disruption at support locations, please try to select slots so there are not multiple people from your location attending the same session.



Below, please find a reminder e-mail sent to registered employees for their upcoming Generative AI Lab, which also includes important information about the session.

---



Good Afternoon,

This is a friendly reminder that you are scheduled to attend the following AI Lab at Essex Centre:

**Address:** 372 Talbot St N, Essex

**Parking:** Available at the front and back of the building

**Note:**

- Each session is 3 hours in length, so please arrive promptly
- AI Labs laptops will be provided, you do not need to bring a laptop to the session

**What to do before the session?**

- **Please make sure you have completed the Intro to AI OTR module** that was added to OTR in October 2023 **before attending the session.** The content of the OTR module forms the foundation of knowledge upon which AI Labs activities will build.
- **NEW:** All lab attendees must create a ChatGPT account using your work email address (as per policy) **before** attending your lab session.

[Create your ChatGPT account now](#)

For a generic tutorial video, [click here](#) to view.

**Note:** You must use your work email account to create a ChatGPT account for work purposes. It is very important that the password you use for your work ChatGPT is different than the one you normally use to log-in at work.

## Create your account

Email address

yourname@communitylivingessex.org

Continue

Already have an account? [Log in](#)

OR



Continue with Google



Continue with Microsoft Account



Continue with Apple

