

ACCEPTABLE USE POLICY

1. Definitions

“Confidential Information” means any business or technical information which is proprietary to the Ministry, whether it is received, accessed or viewed by the recipient in writing, visually, electronically or orally. Confidential Information shall include, without limitation, technical information, business plans, databases, specifications, prototypes, sketches, specifications, software (source and object codes).

“End User” or **“you”** or **“your”** means you, the individual who has signed into the Solution, and who has been authorized by your User Organization to access and use the Solution.

“Ministry” means the Ontario Ministry of Health.

“Personal Information” means any recorded information about an identifiable individual or that may identify an individual and includes “personal health information” as such term is defined in the *Personal Health Information Protection Act, 2004* (Ontario).

“Purpose” means reporting COVID-19 vaccine administration, demographic and adverse event information to the Chief Medical Officer of Health, or a Medical Officer of Health of a Board of Health as authorized or permitted under PHIPA or the HPPA, and for other purposes permitted or required by law.

“Solution” means the platform called “COVAX” or and such extensions and upgrade to the platform, as may be owned by, licensed or subscribed to by the Ministry and made available to your User Organization.

“Policy” means this Acceptable Use Policy.

“User Organization” means the legal entity who authorized you to access and use the Solution.

2. Scope and Application

This Policy governs your access to and use of the Solution. The Ministry may revise this Policy from time-to-time at its sole discretion, by providing notice to your User Organization. By continuing to access and use the Solution after a revised version of the Policy has been provided to your User Organization, you agree to comply with the latest version of the Policy.

When you click the “Accept” button when entering the Solution, you are agreeing to be bound by this Policy. Please review the following terms carefully. If you do not agree with these terms you cannot use or gain access to the Solution.

3. Accountability

- Your User Organization is responsible for your access to and use of the Solution.
- You must obtain your credentials, or other system access tools required to access the Solution as well as related hardware (mobile devices) and technology components only as authorized by your User Organization.
- You are responsible for complying with this Policy.

4. Acceptable Use

You may access and use the Solution solely for the Purpose. You agree to access and use the Solution in compliance with all applicable laws, regulations or policies including the *Personal Health Information Protection Act, 2004* and all guidelines, policies, and manuals prescribed by your User Organization.

5. Inappropriate and Unacceptable Use

You shall not use the Solution in any manner that constitutes inappropriate or unacceptable use, which includes, but is not limited to:

- (a) Collecting, using, or disclosing Personal Information in contravention of the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act*, the *Personal Health Information Protection Act, 2004*, or any other applicable law.
- (b) Accessing the Solution and the Personal Information contained within the Solution for any purpose other than the Purpose.
- (c) Collecting, using or disclosing Personal Information in the Solution which is not required for your use of the Solution.
- (d) Accessing, viewing, editing, updating or modifying any information or data in the Solution unless such access, viewing, editing, updating or modification is for the Purpose.
- (e) Destroying or encrypting data and visual aids except as expressly permitted in documentation supplied by the Ministry or as required by applicable law.
- (f) Making, possessing or distributing computer programs that are designed to assist in obtaining access to the Solution in violation of any agreement, this Policy or applicable laws.
- (g) Wilfully bypassing or subverting physical, logical or procedural safeguards such as firewalls, web-filtering software or other access controls or attempting to gain access to the Solution other than through your access contemplated by this Policy.
- (h) Sharing passwords, or other system access tools with un-authorized individuals or entities for any purpose.
- (i) Facilitating the violation of this Policy.
- (j) Violating or facilitating the violation of a third party's acceptable use policy during your use of the Solution.
- (k) Infringing intellectual property rights including copyrights, trade secrets, or trademarks.
- (l) Disclosing Confidential Information about the Solution, except as required by law.
- (m) Posting or submitting any material or information into the Solution that:
 - (i) is abusive, defamatory, discriminatory, offensive, irrelevant or unlawful;
 - (ii) you do not have the legal right to post in the Solution, or otherwise to publish or distribute;
 - (iii) is for advertising or commercial purposes; or

(iv) you know to be false, inaccurate or misleading.

6. Security

You are responsible for safeguarding your login credentials. Any password or ability to access the Solution given to you is not transferable.

You must immediately notify your User Organization if you suspect or know that passwords or other system access tools have been or may be breached or compromised and change your password as soon as possible in such circumstances.

You agree to provide all assistance in regard to any privacy complaints of individuals and reviews conducted by the Information and Privacy Commissioner of Ontario.

You will take all reasonable steps to safeguard confidential information from unauthorized use or disclosure.

You will only enter information into the Solution that you know to be accurate.

You will report any errors in the Solution to the Ministry.

You will promptly report any breach or suspected breach of privacy to your User Organization.

You are responsible for the security of the device that you are using to access Solution.

7. Collection, Use and Disclosure of Confidential Information

By using the Solution you confirm that you are authorized by your User Organization to access the Solution and you and your User Organization have the legal authority to access the Solution pursuant to PHIPA.

You acknowledge that in using the Solution, you may have access to Confidential Information.

You will not access, collect, use, disclose, retain or dispose of any information in Solution unless authorized by law to do so and as required in the proper discharge of your duties. In particular, you understand that you are only authorized to access, collect, use, disclose, retain or dispose of personal health information as it relates to the Purpose, and as directed by your User Organization.

8. Non-Compliance with this Policy

You must report all instances of suspected or actual breaches of this Policy to your User Organization.

The Ministry reserves the right to investigate suspected or actual breaches of this Policy. You shall fully cooperate with any such investigation. For greater certainty, you shall:

- (a) Provide access to all documentation requested orally or in writing by the Ministry; and
- (b) Provide any other assistance that may reasonably be requested by the Ministry in connection with an actual or suspected breach.

The Ministry or your User Organization may, at their sole discretion, suspend or revoke your access to the Solution as a result of your actual or suspected breach of this Policy.

Breaches of this Policy may result in criminal prosecution or civil liability and/or other sanctions deemed appropriate by the Ministry or your User Organization.

9. Third Party Rules

Your access to the Solution includes access to third party services that publish rules, guidelines or agreements to govern their use. You must adhere to any such rules, guidelines or agreements. Such third party services include, but are not limited to:

(a) Salesforce and MuleSoft: Acceptable Use Policy

· https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/legal/Agreements/policies/ExternalFacing_Services_Policy.pdf

(b) Amazon Web Services: Acceptable Use Policy

· <https://aws.amazon.com/service-terms/>

10. Liability, Intellectual Property and General

The Ministry shall not be liable for any losses, expenses, costs, claims, damages or liabilities howsoever arising in connection with or as a result of a User's End User's access to or use of the Solution.

Nothing in this Policy or your access to the Solution will transfer any right, title or interest in or to Solution to you, including any intellectual property rights.

Any failure by the Ministry to enforce any part of this Policy shall not constitute waiver by the Ministry of any right to do so at any time. If any provision of this Policy is found to be invalid or unenforceable, then that provision will be enforced to the extent permissible, and all other provisions will remain in full force and effect.

Acceptance

By selecting the 'Finish' button you are acknowledging that you have read, understood, accept and will comply with the terms of use set out above.