ONTARIO ARTS COUNCIL

Effective Date: February 1, 2017
Approved By: OAC Board

Title: ***FIPPA* COMPLIANCE**

1.0 INTRODUCTION

As an agency of the government of Ontario covered under the *Freedom of Information and Protection of Privacy Act (FIPPA)*, the Ontario Arts Council (OAC) must comply with the requirements set out under the *Act* regarding information/records in its custody and control. The purpose of *FIPPA* is two-fold: i) provides a right of **access to general information** under the control of institutions with necessary exemptions (mandatory and discretionary) and; ii) requires institutions that have personal information to **protect the privacy of the individuals** to whom this information relates and provide individuals with the right of access to their information. *The Act* also appoints an Information and Privacy Commissioner (IPC) who is independent of government and provides oversight of the legislation.

This policy should not preclude responding to informal verbal or written inquiries and providing information that is publicly available, otherwise known as Routine Disclosure.

This policy is consistent with OAC's Code of Conduct Principles concerning the violation of federal or provincial law (Section 1.3.1 (viii)); Confidentiality (Section 1.3.7); Privacy and Security of OAC Records (1.3.13); Procedure for Reporting on Breach of the Code (Sections 1.4.3 to 1.4.8); and Disciplinary Action for Violating the Code (Section 1.4.9).

1.1 SCOPE OF APPLICATION

This policy applies to all staff (full-time, part-time, casual and contract) at all levels, student placements, members of the board of directors, volunteers, assessors, recommenders and service providers/vendors to OAC.

1.2 DEFINITIONS

Active Dissemination (AD)
This is the periodic release of OAC records in the absence of a formal request to access information.

Agency of the Government of Ontario
Under *FIPPA,* an "institution" includes any agency, board, commission, corporation or other body designated in the regulations.

Agency Head
OAC's Director & CEO is the Agency Head for the purpose of this policy and any decisions made related to access to information requests.

Breach
The result of an unauthorized access to, or collection, use or disclosure of personal information.

Business Identity Information
Personal information does not include the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity. Contact information is defined as information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, address, email or fax number of the individual. For greater certainty, this applies even if an individual carries out business, professional or official responsibilities from their dwelling and the contact information for the individual relates to that personal dwelling.

Consistent Purpose
A consistent purpose is only if the individual might reasonably have expected such a use or disclosure of the information/record.

Control (of a record)
Means the power or authority to make a decision about the use or disclosure of the record.

Custody (of a record)
Means the keeping, care, watch, preservation or security of the record for a legitimate business purpose. While physical possession of a record may not always constitute custody, it is the best evidence of custody.

Formal Access Request
This is used by the public where information is not available through OAC's usual channels.

Frivolous and Vexatious (requests)
Is where the request is part of a pattern of conduct that amounts to an abuse of the right of access or where responding to the request would interfere with the operations of the institution.

Exemptions
An important principle of *FIPPA* is that necessary exemptions from the right of access should be limited and specific. Therefore, the organization must disclose as much of the record as can reasonably be severed without disclosing the information that falls under one of the exemptions identified in *the Act*. Certain types of records either must not (mandatory) or may not (discretionary) be disclosed in response to a request for access.

Personal Information
Means recorded information about an identifiable individual, including:

- information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;
- information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual, or information relating to financial transactions in which the individual has been involved;
- any identifying number, symbol or other particular assigned to the individual;
- the address, telephone number, fingerprints or blood type of the individual;

- the personal opinions or views of the individual except if they relate to another individual;
- correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the individual; and
- the individual's name if it appears with other personal information relating to the individual or where disclosure of the name would reveal other personal information about the individual.

Privacy
The principle that an individual has the right to control their own personal information. Custodians of the personal information have a duty of care to safeguard the personal information in their control.

Routine Disclosure (RD)
This is the routine or automatic release of certain types of administrative and operational records in response to informal rather than formal requests under the *FIPPA.*

Third Party
Any person, group of persons, or organization whose interests might be affected by disclosure other than the person making a request for access or OAC, for example. Where the third party is an individual, his/her rights may in some cases be exercised by another person.

1.3 ACCESS TO INFORMATION

1.3.1 OAC provides the right of access to existing records, in whole or in part, that are in its custody or control except for limitations allowed under *FIPPA*. These limitations include allowable exemptions (mandatory and discretionary) and if the request is considered frivolous or vexatious.

1.3.2 This right of access and correction extends to individuals with regard to information about themselves, that is in OAC's custody or control, subject to exemptions and exclusions under *FIPPA*.

1.3.3 All formal access requests must be in writing and include the name and contact information of the requester, details of the records being requested as well as the time period, and any other background/context that will assist in locating the requested records.

1.3.4 Any fees charged will be according to allowable fees prescribed by regulations.

1.3.5 Anyone who makes a request for information or contacts OAC about a privacy breach has the right to remain anonymous to individuals outside of OAC unless the individual gives permission. Within the organization, the person's identity may be disclosed only to employees who need the information to perform the duties of their job.

1.3.6 OAC will follow the allowable timelines under *FIPPA* for responding to formal access requests.

1.3.7 OAC ensures that reasonable measures are in place to comply with the *Archives and Recordkeeping Act, 2006*, and other government records management

directives, best practices or relevant legislation concerning the records in its custody or control.

1.3.8 In the event of an emergency disclosure due to environmental, health or safety hazard to the public, if practical, OAC will provide notice to those individuals/organizations to whom the information relates.

1.4 PRIVACY AND PROTECTION OF PERSONAL INFORMATION

1.4.1 Collection of personal information must be authorized by statute, used for purpose of law enforcement or necessary to the proper administration of a lawfully authorized activity.

1.4.2 It is preferable to collect personal information directly from an individual. If information is collected indirectly from another source, then the individual to whom the information relates should be made aware unless the indirect collection is permitted under *FIPPA*.

1.4.3 OAC provides notice when it collects personal information (either directly from the individual or indirectly from another source) unless it is waived or falls under an exception under *FIPPA*. At a minimum, the notice will provide the authority for the collection, the purpose for collecting the personal information, and contact information for further inquiries.

1.4.4 OAC collects, uses, discloses and retains in its custody or control only the minimum personal information necessary to fulfil the stated purpose.

1.4.5 OAC takes reasonable steps to ensure that personal information is accurate and up-to-date.

1.4.6 OAC uses personal information for the purpose identified at time of collection, or for a consistent purpose or otherwise, with the individual's consent.

1.4.7 OAC discloses personal information where permitted under *FIPPA*.

1.4.8 OAC ensures that only those individuals who need a record for the performance of their duties have access to it, and takes the necessary steps to protect the organization's personal information records from accidental destruction.

1.4.9 OAC takes the necessary administrative, technical and physical safeguards/ precautions to protect personal information (at rest, in motion, in use) from a privacy breach, including unauthorized access, linkage, disclosure or alteration.

1.4.10 OAC ensures that every contract for data collection and processing be subject to a Threat Risk Assessment and Privacy Impact Assessment.

1.4.11 OAC board members and staff must sign a Code of Conduct Acknowledgement.

1.4.12 In the event of a privacy breach, all board members and staff will follow OAC's privacy breach protocol.

1.4.13 OAC provides contact information for questions or concerns about any collection, use or disclosure of personal information or about a request for access to personal information.

1.5 TRAINING

The requirements under *FIPAA* relating to access to OAC's general information and OAC's responsibility to protect personal information are complex. Sometimes it is not until a privacy breach occurs or an FOI request is received that staff become fully aware of how they need to adjust their everyday practices in order to fulfil their legal obligations. OAC has built its

FIPPA compliance program with a view to making compliance a part of OAC's organizational culture.

At OAC, we want to ensure that all staff (full-time, part-time, casual and contract) at all levels, student placements, members of the board of directors, volunteers, assessors, recommenders and service providers/vendors to OAC, know what their legal responsibilities are, in order to comply with the law when dealing with records and personal information in OAC's custody and control. We acknowledge that those noted above will be involved in *FIPPA* compliance to varying degrees depending upon their position or function and therefore the approach to training or awareness will take this into consideration.

1.5.1 Mandatory *FIPPA* training will help responsiveness to *FIPPA*, and reduce the time and resources required to search for records, consult with affected parties, and make more accurate decisions about whether information is to be disclosed under *the Act*.

1.5.2 Additional *FIPPA* training will be based on triggers such as a privacy breach, new/revised best practices, decisions/resolutions arising from the Information and Privacy Commissioner's Office (IPC), or changes to OAC's policies/procedures concerning records/information.

1.6 PROCEDURE FOR CONTRAVENTION OR DISREGARD

Any breach of this policy will be considered a serious matter and will be dealt with accordingly. If it is believed that anyone to whom this policy relates has not been in compliance with this policy, an investigation will be conducted under the auspices of the Director & CEO or delegate, based on the circumstances. Failure to comply with this policy could lead to disciplinary action, up to and including dismissal.