# ADR EDUCATION – PRIVACY POLICY

***FOR PARTNERS, ASSOCIATES AND EMPLOYEES OF ADR EDUCATION***

***VERSION 1.5. – 2026-02-27***

## 1. OVERVIEW

**ADR EDUCATION** is a national dispute resolution firm. This policy outlines our Privacy Management Program, which ensures the protection of any personal information collected, used, or accessed by ADR Education partners, associates, or employees in the course of their work.

The Privacy Management Program includes:

1. Purpose of the Program and Applicable Laws and Contracts
2. Consent and Limited Collection of Personal Information
3. Appropriate Use of Personal Information
4. Appropriate Safeguards for Personal Information
5. Openness of the Privacy Management Program
6. Access Requests to Personal Information
7. Challenges to Compliance

This policy should be read together with ADR EDUCATION's IT Security Policy, which details the technical and procedural safeguards used to enact this policy.

## 2. PURPOSE OF THE PROGRAM, APPLICABLE LAWS AND CONTRACTS

ADR Education collects personal information through the normal course of its dispute resolution and training work. Personal Information refers to recorded information about identifiable individuals (excluding business contact details), collected, created, or accessed as a result of the work.

Collection can occur when individuals share details about themselves during services such as training, coaching, mediation, workplace assessments, or investigations. Clients may also provide background materials—like participant lists, job descriptions, or prior reports that contain identifying or employment-related information. In delivering services, ADR Education may generate records, such as interview notes, reports, and correspondence, that contain personal information.

Much of this information is collected directly from participants, while some is provided by client organizations to support the work. The personal information handled can range from basic identifiers (e.g., name, role, department) to more sensitive details about workplace situations, relationships, or

formal complaints. These records are managed in compliance with applicable privacy laws and any specific contractual requirements, which may set conditions for how the information is stored, accessed, retained, and ultimately returned or destroyed. All personal information collected in the course of our work remains the property of the client. ADR Education has temporary custody for contractual purposes and manages such information in accordance with client direction.

ADR Education is responsible for all personal information under its control and has appointed a Privacy Officer with decision-making authority for privacy matters. Other individuals may be designated to act on behalf of the Privacy Officer from time to time.

## PRIVACY OFFICER:

**BRIN HAMILTON,** *Partner, ADR Education* – bhamilton@adreducation.ca

The Privacy Officer will review this policy annually and amend it as necessary. This review will consider:

- Risks associated with new activities, processes, or client work
- Updates in applicable legislation
- Technology-related considerations (in conjunction with ADR Education's IT Security Policy)

All ADR Education Partners, Associates, and Employees receive an orientation and refresher training on the policy and the Privacy Management Program. Training covers:

- How to respond to privacy-related inquiries
- What constitutes valid and meaningful consent, and how it is obtained
- How to recognize and process access requests
- Where to direct privacy complaints
- Updates on initiatives to protect personal information
- The IT Security Policy (which requires a signature of acknowledgement)

## APPLICABLE LAWS

ADR EDUCATION works across all provinces and territories, with clients subject to a combination of federal and provincial privacy laws. Applicable law depends on the nature and location of the client and the work and may involve multiple jurisdictions.

The Privacy Management Program is designed to comply with the following substantially similar privacy laws. Where more than one law or contractual requirement applies, ADR Education will apply the interpretation or requirement that provides the greatest protection for personal information:

- **FEDERAL:** *Personal Information Protection and Electronic Documents Act (PIPEDA)*
- **BRITISH COLUMBIA:** *Personal Information Protection Act (PIPA)*
- **ALBERTA:** *Personal Information Protection Act (PIPA)*
- **SASKATCHEWAN:** *Freedom of Information and Privacy Protection Act (FOIP)*

- **ONTARIO:** *Freedom of Information and Protection of Privacy Act (FIPPA) – public institutions only; private institutions follow PIPEDA*
- **QUEBEC:** *Act Respecting the Protection of Personal Information*

### CONTRACTS

In addition to complying with applicable laws, ADR Education enters into contracts with clients, including standing offers for specific services. These contracts may contain additional privacy or IT security provisions. Where a contractual provision is stricter than this policy (e.g., shorter retention timelines, specific breach notification requirements, storage restrictions), the contractual provision will apply.

## 3. CONSENT & LIMITED COLLECTION OF PERSONAL INFORMATION

ADR Education identifies the purposes for collecting personal information at or before the time of collection, and before using or disclosing it for those purposes.

The purposes are typically outlined during the contracting phase with clients. The type and amount of information collected varies by service. Participants are informed about:

- How their personal information will be used
- Who will have access to it
- Applicable confidentiality terms

Consent may be express (written or verbal) or implied, depending on the service, applicable law, and client contract. Implied consent occurs when an individual voluntarily provides information for a known purpose after being informed of its use, disclosure, and storage. For example:

- In workplace assessments or group training, consent is typically implied through participation, supported by ADR Education's process and the client's own communication.
- For services involving more sensitive information (e.g., workplace investigations, mediations), written consent is obtained from primary participants; witnesses may provide written or implied consent, depending on context.
- Personal information for minors will not be collected, unless they are of the age of legal employment in the Province of Ontario and are employed by the City of Mississauga. In such an event, their personal information will be collected both directly and indirectly, as noted above.

### EXAMPLES:

- **TRAINING:** Name, employee number, job title, organization, department – generally implied consent.
- **COACHING:** Same as training, plus workplace context and personal views - confidentiality detailed in coaching agreements.

- **MEDIATION:** Conflict-related details – consent and confidentiality are detailed in signed participation agreements.
- **WORKPLACE ASSESSMENT:** Survey or interview responses – consent implied through process explanation and client communication.
- **INVESTIGATION:** Formal complaint information – written consent from complainants/respondents; witness consent may be implied.

Only information reasonably necessary for service delivery is collected on paper or electronically as evidence to determine situational facts and investigative findings, or to inform workplace assessment or resolution processes to seek recommendations, resolution, or reconciliation. Personal information such as one's name, phone number, email address, job title, job duties, team/department/organization, and relationships with others (colleagues, family, friends) will be used, disclosed, and retained only as long as needed for the stated purposes and as permitted or required by law. Access is limited to those with a legitimate need-to-know. It will not be disclosed to unauthorized parties or transferred outside Canada (including via cloud storage).

## 4. APPROPRIATE USE OF PERSONAL INFORMATION

Personal information will only be used or disclosed for the purposes for which it was collected, unless the individual consents otherwise or law permits. ADR Education strives to keep information accurate, complete, and up to date.

ADR Education retains records for 5 years to accommodate potential follow-up, unless the client directs earlier transfer or destruction. Any records requests by the city will be encrypted using AES-256 and transferred securely using TLS 1.2+ protocols.

### RETENTION

- **DEFAULT:** Five (5) years after file closure, unless otherwise directed by the client or law.
- **CONTRACT-SPECIFIC:** Client contract requirements override the default.

### STORAGE

All personal information must be stored in Canada (including cloud-based storage) at secure sites that comply with the standards of the IT Security Policy. Storage outside of Canada is prohibited unless specifically authorized in writing by the client and subject to equivalent or higher security standards.

### DESTRUCTION/RETURN

Records are retained securely until returned to the client or securely destroyed (in accordance with the schedule outlined above). All destruction will comply with NIST 800-88 ("Guidelines for Media Sanitization" by the U.S. National Institute of Standards and Technology) standards. A log will be maintained of destructed files. A Certificate of Destruction will be provided if required.

## 5. APPROPRIATE SAFEGUARDS FOR PERSONAL INFORMATION

ADR EDUCATION implements reasonable security arrangements, including technological, physical and administrative safeguards, to prevent theft, loss, or unauthorized access, use, or disclosure of personal information. ADR EDUCATION applies safeguards proportionate to the sensitivity of the information. These include:

### TECHNICAL SAFEGUARDS

- Unique user IDs and passwords, updated at least every six months
- Multi-factor authentication for remote access
- Encryption for all mobile devices, removable media, and data in transit
- Audit trails for system access

### PHYSICAL SAFEGUARDS

- Locked storage for paper records
- Restricted office access

### ADMINISTRATIVE SAFEGUARDS

- Access granted on a need-to-know basis
- Immediate revocation of access when no longer required
- Confidentiality agreements for all personnel with access to personal information

### PRIVACY INCIDENT HANDLING

In the event of a suspected or actual privacy breach:

1. Immediate reporting to the Privacy Officer and Director of Operations at:
    a. Privacy Officer - bhamilton@adreducation.ca
    b. Director of Operations - admin@adreducation.ca
2. Include:
    a. Date and time discovered
    b. Brief description of the issue
    c. Affected systems and information
    d. Steps already taken
    e. Contact details for follow-up
3. The Privacy Officer/Director of Operations will:
    a. Acknowledge receipt
    b. Conduct an initial assessment

c. Investigate, resolve, and document the incident through consultation with ADR Education's IT Consultant and IT Security Insurer
d. Notify the affected client as required under law or contract and cooperate fully in investigation, recovery, and mitigation efforts

4. Incident data will be reviewed to update this policy or procedures as needed.

## 6. OPENNESS OF THE PRIVACY MANAGEMENT PROGRAM

ADR Education makes information about this policy and related practices publicly available. The most current version of this policy is posted on ADR Education's website and is linked to in the ADR Education process form for written or implied consent.

IT-related concerns are first identified and then directed to ADR Education's managed service provider (MSP), 365CloudServices. The MSP initiates containment procedures, including isolating affected endpoints using SentinelOne's rollback and quarantine features, disabling compromised accounts or services, and blocking malicious IPs or domains through firewall or endpoint policies.

Any privacy-related complaints or inquiries are directed to ADR Education's Privacy Officer, who is responsible for identifying and investigating the issue, taking action if warranted, and communicating the outcome to the individual. All requests will be answered within 30 days, with a possible extension to 60 days if necessary. If an extension is required, requestors will be informed of the reasons for the delay.

## 7. ACCESS REQUESTS TO PERSONAL INFORMATION

### INDIVIDUAL REQUESTS

Individuals may request access to their personal information by submitting a written request to the Privacy Officer, specifying the information sought. Identity will be verified before release.

Requests will be answered within 30 days, with possible extension to 60 days if necessary; requestors will be informed of the reasons for any extension.

### FOI / ACCESS REQUESTS

When clients are subject to access-to-information laws, ADR Education will assist them in locating and providing relevant records to support access or correction requests

## 8. CHALLENGES TO COMPLIANCE

Individuals may submit complaints or concerns about ADR EDUCATION's privacy practices to the Privacy Officer in writing, including their name, contact information, and a description of the concern.

ADR EDUCATION will investigate all complaints, take corrective action if warranted, and inform the individual of the outcome. Unresolved complaints may be referred to the appropriate provincial or federal privacy commissioner.

## 9. REFERENCES

- Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada)
- Freedom of Information and Protection of Privacy Act (FIPPA) (British Columbia)
- Personal Information Protection Act (PIPA) (British Columbia)
- Personal Information Protection Act (PIPA) (Alberta)
- Freedom of Information and Privacy Protection Act (FOIP) (Saskatchewan)
- Freedom of Information and Protection of Privacy Act (FIPPA) (Ontario)
- Act respecting the protection of personal information (Quebec)

NIST 800-88 ("Guidelines for Media Sanitization" by the U.S. National Institute of Standards and Technology)