

Privacy and Data Protection

Professional Research Standards | General company policy

1. Purpose and responsibility

Atlantic Research and Field Services (ARFS) is committed to responsible handling of personal and confidential information. This policy applies to website inquiries, field network applicants, research participants, client records and information handled by employees or contractors. Charles Batstone, Owner and Director, is responsible for privacy oversight and responding to concerns.

2. Collection and permitted use

ARFS collects only information reasonably needed for an identified purpose. This may include contact details, applicant skills and availability, research responses and project information. At collection, ARFS explains the purpose and obtains consent where required, or confirms another lawful authority. Information is used for the stated purpose, including responding to inquiries, coordinating assignments and delivering agreed research. A materially different use requires appropriate authorization. ARFS does not sell personal information.

3. Consent and confidentiality

People may ask questions about the collection or use of their information and withdraw consent, subject to applicable legal or contractual limits. ARFS explains any resulting effect on participation or services. Identifiable responses and confidential client material are not published without appropriate authority. Reports use aggregated or deidentified information where suitable, with attention to identification risks in small communities.

4. Access and sharing

Access is limited to people who need the information for authorized work. Employees and contractors must follow confidentiality obligations and project instructions. Information may be shared with an authorized client or service provider where necessary for the stated purpose, with appropriate safeguards, consent or other lawful authority. Disclosures required by law are limited to what is required. ARFS remains accountable for information entrusted to service providers.

5. Safeguards and service providers

ARFS selects safeguards appropriate to the sensitivity and volume of information. These include restricted accounts, strong passwords, multifactor authentication where available, protected devices, secure transfer methods and locked storage for paper records. Encryption is used where appropriate to the risk and contract. Access is removed when no longer needed. Lost devices, misdirected messages and suspected unauthorized access must be reported promptly to the Owner and Director. Before selecting a hosting, email, survey, cloud or other processing service, ARFS reviews its privacy terms, access controls and storage and access locations. Personal or confidential information must not be entered into public AI tools or unapproved services without appropriate authorization and safeguards. Ordinary email is not the default method for transferring sensitive research records.

6. Government and client project requirements

Before work begins, ARFS confirms the client's requirements for collection authority, permitted users, data location, transfers, subcontractors, incident reporting, ownership and return or disposal of records. Applicable privacy law and authorized contract requirements take precedence over general procedures. For Nova Scotia public sector work, ARFS checks any applicable restrictions under the Personal Information International Disclosure Protection Act before permitting storage or access outside Canada. ARFS does not assume that a standard email or cloud account meets those requirements.

7. Retention and secure disposal

Information is retained only as long as needed for its identified purpose and applicable legal or contractual obligations. ARFS documents a suitable retention period for each project or record category, reviews inactive applicant records and securely deletes, destroys or returns information when no longer needed. Relevant backup retention and any legal preservation requirements are considered. Client records are returned or disposed of as agreed.

8. Privacy incidents

ARFS will promptly contain suspected incidents, protect remaining information, document the circumstances and assess potential harm. The affected client is notified according to the contract. Individuals and regulators are notified when required by applicable law. Required breach records are maintained, and corrective measures are reviewed to reduce recurrence.

9. Access, correction and concerns

Contact Charles Batstone at charles@atlanticresearch.ca or 902-249-0002 to ask about privacy practices, request access or correction, withdraw consent or raise a concern. ARFS verifies identity proportionately, responds within applicable time limits and explains any lawful restriction. Requests involving client controlled records may be directed to the responsible client. ARFS reviews this policy annually and when practices or requirements materially change.