Thrive Charter School Society
Privacy Management Plan

Version 30.06.2026

Thrive Charter School Society Privacy Management Plan

Updated: June 3, 2026
Last Board Review: April 30, 2026

Privacy Officer:
Michael Hladun
SVP Go Auto, Vice Chairman, Thrive Charter School Society
mhladun@goauto.ca
(780) 908-1125

Contents:

Thrive Elementary Charter School Society

Policy 214: Access to Information and Protection of Privacy

Policy Statement

Thrive Elementary Charter School Society (TCSS) is committed to ensuring that information is managed in a transparent, responsible, and privacy-protective manner. As a public body under Alberta's Access to Information Act (ATIA) and Protection of Privacy Act (POPA), the Society recognizes its dual responsibility to support public access to information while safeguarding the personal information of students, families, employees, volunteers, and community members.

The Society values open, accountable governance and believes that access to information strengthens public trust and reinforces the principles of the Thrive Concept Model and the Thrive Student Model. Protection of privacy is essential to fostering safe, respectful, and student-centered learning environments. The Society will collect, use, disclose, retain, and secure personal information in accordance with ATIA, POPA, the Education Act, and all applicable regulations.

This policy reflects the Society's commitment to good governance, legal compliance, and the thoughtful stewardship of information in support of the success and well-being of all members of the Thrive community.

Definitions

Access Request: A request made under the Access to Information Act (ATIA) for access to records held by the Society.

Personal Information: Recorded information about an identifiable individual, as defined under POPA.

Privacy Management Program: A coordinated set of policies, procedures, and controls required under POPA.

Record: Any form of recorded personal information created, received, or maintained by the Society.

Student Record: Information maintained in accordance with the Student Record Regulation (AR 97/2019).

Delegation of Authority

The Board retains ultimate accountability for ensuring organizational compliance with all applicable access to information and protection of privacy legislation. This responsibility includes approval of new privacy governance policies, designating a Privacy Officer, receiving reports regarding significant privacy matters, breaches, investigations and compliance issues.

Furthermore, the Board, in accordance with the Education Act and Alberta's applicable access to information and protection of privacy legislation, delegates authority and assigns responsibilities related to the administration of access to information, privacy protection, records management, and information security as follows:

Privacy Officer (Board Vice-Chair)

The Privacy Officer is delegated authority to develop, implement and manage the Privacy Management Plan and to oversee and coordinate the Society's access to information, privacy, records management, and privacy compliance functions in accordance with applicable legislation, policy, and administrative procedures.

Superintendent

The Superintendent is delegated responsibility to ensure organizational practices, procedures, and operations support compliance with access to information and protection of privacy requirements.

School Data Administrator / Information Management Administrator

The School Data Administrator is delegated the responsibility for supporting the secure management, access, protection, and administration of organizational data systems and records containing personal information.

Employees, Staff, Volunteers, and Service Providers

Employees, staff, volunteers, and service providers are responsible for complying with all applicable privacy, confidentiality, records management, cybersecurity, and access to information requirements in the performance of their duties.

Guidelines

Roles and Accountabilities:

Thrive Charter School Society Board:

- **Resource allocation:** Ensures that the designated privacy officer has the necessary financial, human, and technical resources to establish, implement, and periodically review, assess and update a Privacy Management Program (PMP).

- **Mandatory compliance:** Compliance with POPA is a legal obligation and requires sufficient support is given to meet the requirements under this Act.

- **Public trust:** Proper funding and executive support is given for Thrive Charter School's (Thrive CSS) Privacy Management Plan development, implementation and ongoing maintenance.

Privacy Officer:

- **Liaison:** Serves as the primary point of contact for privacy inquiries and concerns.

- **Policy development:** Supports the creation, implementation, and maintenance of a Privacy Management Program (PMP) and relating privacy policies and procedures.

- **Compliance oversight:** Ensures the Thrive CSS adheres to AITA and POPA and oversees the management of the PMP.

- **Central Management:** Effectively coordinates with necessary support (IT professionals, legal counsel and communication advisors) in the resolving of privacy matters.

- **Practice:** Is accountable for Thrive CSS' privacy practices. The specific duties and activities include:
    - Establishing and regularly reviewing program controls (policies, procedures, etc.).
    - Developing and delivering employee training and education.
    - Documenting, monitoring, and auditing the implementation of the PMP.
    - Representing the public body during investigations by the Office of the Information and Privacy Commissioner (OIPC).
    - Together with the Superintendent and school leadership, champion a workplace culture that prioritizes privacy.

Superintendent:

- **Privacy Management Program development**: Working with the Privacy Officer, leads documentation development of a Privacy Management Program.

- **Policy and Procedure development:** Leads the creation, implementation, and maintenance of privacy policies and procedure documentation in accordance with the AITA and POPA Act.

- **Delegation and Oversight:** Assigns and manages the role of the Thrive school data coordinator for POPA and AITA related records administration tasks.

- **Training:** Ensures that training is scheduled and delivered to all teaching and administration staff annually.

School Data Administrator:

- **Personal Information Inventory:** Maintains an accurate and up-to-date inventory of data to manage information sharing agreements and personal information banks.

- **Use:** Personal information may only be used for the purpose for which it was collected or if the individual that the information is about has identified the information and has consented.

- **Disclosure:** Personal information may only be disclosed as outlined in section 13(1) of Protection of Privacy Act.

Employees, Staff and Volunteers:

- **Compliance**: Are adequately trained and adhere to procedures for accessing, using, storing and disposal of all personal information that Thrive CCS is in possession of.

- **Authorization:** Collects, discloses and uses only information that is authorized by Thrive CCS.

- **Reporting:** Immediate reporting of any suspected or actual privacy breaches to school leadership, the Superintendent or Privacy Officer.

- **Responsibility:** Strict protection of the confidentiality of student, parent/caregiver, and staff personal data at all times.

Documents and References

- *Access to Information Act (ATIA)*
- *Protection of Privacy Act (POPA)*
- *Education Act*
- *Charter Schools Regulation (AR 118/1995)*
- *Student Record Regulation (AR 97/2019)*
- Policy 210 – Student Records
- Administrative Procedure 214 – Access to Information and Privacy Protection

Approval Date: January 27, 2026
Policy 214 (Inclusive of 214.1 – 214.6) Review Date: September 2028

Administrative Procedure 214

Access to Information and Privacy Protection

Purpose

To establish system-wide procedures governing access to information, privacy protection, information governance, records management, privacy breach response, vendor oversight, automated systems safeguards, correction requests, privacy training, and Privacy Management Program implementation in accordance with the Access to Information Act (ATIA), the Protection of Privacy Act (POPA), the Education Act, related regulations, and Policy 214 and associated sub-policies 214.1 through 214.6.

Procedures:

1. The Society shall collect, use, disclose, retain, and destroy information only where authorized by legislation.
2. The Society shall protect personal information through administrative, physical, and technical safeguards.
3. The Society shall maintain transparent and accountable information governance practices.
4. The Society shall limit access to personal information to authorized individuals with a legitimate educational or operational need.
5. The Society shall ensure all employees, contractors, volunteers, and service providers understand and fulfill their privacy obligations.
6. The Society shall maintain a Privacy Management Program (PMP) that supports legislative compliance and continuous improvement.
7. The Society shall respond promptly and appropriately to privacy breaches, correction requests, and access requests.
8. The Society shall ensure information management practices support safe, respectful, and student-centered learning environments.

Scope

This Administrative Procedure applies to all employees, contractors, volunteers, trustees, service providers, consultants, third-party vendors, and all individuals acting on behalf of the Society who collect, access, use, disclose, retain, store, transmit, or destroy information under the custody or control of the Society.

Governance and Administration

Privacy Officer

1. Coordinate Society privacy compliance activities.
2. Support implementation of the Privacy Management Program and related policy(s).
3. Oversee privacy investigations and breach management.
4. Coordinate responses to access and correction requests.
5. Support Privacy Impact Assessments.
6. Monitor legislative compliance.
7. Support privacy training and awareness activities.
8. Maintain required privacy documentation.
9. Ensure all contracted service provider contracts have required contract language pertaining to AITA and POPA.
    a. The articles included in the contracts must state that when the service provider performs a service on behalf of a public body and in doing so has access to personal information subject to the Protection of Privacy Act (POPA) it must take all necessary steps to protect the personal information including administrative, physical, and technical safeguards.
    b. That contracts also include provisions regarding an individual's right of access to their own personal information under the Access to Information Act (AITA).
10. Liaise with the Office of the Information and Privacy Commissioner where required.

Superintendent

1. Ensure implementation of this Administrative Procedure.
2. Establish operational processes and forms required to support compliance.
3. Ensure staff training occurs annually.
4. Ensure appropriate safeguards are implemented.
5. Ensure monitoring and corrective action processes are established.
6. Ensure oversight of access to and protection of information governance practices.
7. Approve or delegate authority respecting privacy operational procedures.

School Data Administrator

1. Coordinate operational privacy administration tasks.
2. Maintain records inventories and privacy documentation.
3. Support correction request processing.
4. Support breach documentation and tracking.
5. Maintain privacy-related logs and records.
6. Support records management retention and destruction processes.

Procedures:

Collection, Use and Disclosure of Information

1. Personal information shall only be collected where authorized by legislation and required for educational, operational, legal, or safety purposes.
2. The Society shall limit collection to the minimum amount of information necessary.
3. Personal information shall only be used or disclosed:
    a. for the purpose for which it was collected;
    b. where authorized by legislation; or
    c. where consent has been obtained.
4. Employees shall only access information required for authorized duties.
5. Confidential information shall not be shared through unauthorized systems, devices, applications, or communication methods.

Records Management and Security

1. The Society shall maintain safeguards appropriate to the sensitivity of information.
2. The Society shall ensure secure storage, transmission, retention, and destruction of records.
3. The Society shall maintain records retention schedules consistent with legislative requirements.
4. The Society shall restrict access to confidential information using role-based access controls where appropriate.
5. The Society shall maintain secure practices for passwords, authentication, remote access, device security, cloud-based systems, and records disposal.

Privacy Impact Assessments

1. Privacy Impact Assessments (PIAs) shall be completed where required under legislation or Society procedures.
2. PIAs may be required for:
    a. new technologies;
    b. software platforms;
    c. vendor relationships involving personal information;
    d. automated systems;
e. data-sharing arrangements; or
f. programs involving personal information.
3. The Privacy Officer shall review PIAs for completeness and compliance.

Access Requests

1. Formal access requests shall be processed in accordance with ATIA requirements.
2. Requests shall be directed to the Privacy Officer or designate.
3. Records searches, review processes, timelines, and responses shall comply with legislated requirements.
4. Appropriate exemptions or exceptions may be applied where authorized by legislation.
5. Records related to requests shall be documented and retained appropriately.

Privacy Breach Management

1. All suspected or confirmed privacy breaches shall be reported immediately to school leadership, the Superintendent, or the Privacy Officer.
2. The Society shall:
    a. contain the breach;
    b. investigate the incident;
    c. assess risks;
    d. determine notification requirements;
    e. implement corrective actions; and
    f. document all actions taken.
3. Significant breaches shall be reported in accordance with legislative requirements.
4. The Society shall maintain a privacy breach register.

Direction to Related Sub-Policies and Procedures

The following related procedures and operational requirements are governed through the associated Policy 214 sub-policy suite:

- Policy 214.1 – Vendor Management and Oversight
- Policy 214.2 – Data Breach Management, Notification and Reporting
- Policy 214.3 – Response to Correction of Personal Information
- Policy 214.4 – Creation, Use and Disclosure of Non-Personal Data
- Policy 214.5 – Automated Systems Safeguards
- Policy 214.6 – Privacy Management Training and Program Review

Training and Compliance

1. All employees, contractors, and volunteers shall participate in required privacy training.
2. Employees shall acknowledge their privacy responsibilities annually where required.
3. Non-compliance with privacy requirements may result in corrective or disciplinary action.

Documents and References

Access to Information Act (ATIA)
Protection of Privacy Act (POPA)
Education Act
Student Record Regulation (AR 97/2019)
Policy 214 – Access to Information and Protection of Privacy
Policies 214.1 through 214.6
Thrive Charter School Society Privacy Management Program
Thrive Charter School Society Privacy Impact Assessment Process

Approval Date: _____ **Review Date:** _____

Policy 214.1 – Vendor Management and Oversight

Policy Statement

Thrive Elementary Charter School Society recognizes that service providers, contractors, consultants, software vendors, cloud-based providers, and third-party partners may collect, access, store, use, disclose, transmit, or otherwise manage personal information on behalf of the Society. It is also recognized that as defined in the legislation, contractors providing service for the Society are deemed employees when having access to or collect, use or disclose personal information on behalf of Thrive Charter School Society and are subject to the AITA and POPA requirements regarding access to personal information. The Society remains accountable for all personal information in its custody or under its control, including personal information managed by its service providers.

The Society is committed contractually to ensuring that all third-party relationships involving personal information comply with the Access to Information Act (ATIA), the Protection of Privacy Act (POPA), the Education Act, and all related legislation, regulations, and standards. Appropriate governance, oversight, contractual safeguards, monitoring, and privacy controls shall be implemented prior to and throughout the duration of any vendor relationship.

The Society shall ensure that privacy, confidentiality, security, records management, and legal compliance considerations are integrated into procurement, contracting, implementation, monitoring, renewal, and termination processes involving third-party service providers.

Definitions

Service Provider: Any external organization, contractor, consultant, volunteer, or individual providing services to the Society under a contractual or agency relationship.
Note: If a service provider under a contract for services is tasked with providing access to personal information on behalf of the public body, it will be an "employee" of that public body for that purpose and subject to ATIA requirements regarding access to the personal information.

Vendor: A third-party provider of goods, services, applications, software, cloud-based systems, infrastructure, or operational supports.

Personal Information: Recorded information about an identifiable individual as defined under POPA.

Privacy Impact Assessment (PIA): A formal assessment process used to identify, evaluate, and mitigate privacy risks associated with a program, service, initiative, or technology.

Data Residency: The physical or geographic location where information is stored, processed, or accessed.

Procedures

Privacy Officer

Vendor Management:

- Provide direction and procurement oversight when engaging with contracted services involving collecting, using or sharing personal information.
- Direct employees to only use approved vendors, systems, and software applications.
- Provide direction and oversight to ensure service contracts meet the following:
    - The Thrive Charter School Society retains "control" and "ownership" over all information that will be in the custody of the service provider.
    - Ensures contracts include privacy, confidentiality, correction, retention, breach reporting, audit, and security provisions that align with POPA requirements.
    - Contracts address how any complaints alleging unauthorized access, collection, use or disclosure by the contractor (or their employees or subcontractors) will be handled, within a complaint management process managed by the Privacy Officer.
    - Contracts include terms and conditions that requires the service provider to cooperate with the Thrive Charter School Society for the preparation of PIAs, or if the public body is under investigation by a regulatory authority.
    - Contracts establish retention periods for the information stored by the service provider and a process for the service provider to certify to the public body when personal information has been destroyed at the end of its retention term.
    - Contracts, involving personal, school or society data, are required to clearly specify requirements of the service provider whenever it experiences a breach of personal information it holds on behalf of the public body, including timelines.
        - Ensures contracts outline clear expectations that if the service provider ceases to operate or the contract terminates, all records from the service provider are returned, deleted or destroyed to the Thrive Charter School Society along with assurance that no records are retained or can be accessed by the service provider.
- Directs the complaints management process.
- Review Privacy Impact Assessments for compliance.

Oversight:

- Ensure all contracted service providers are meeting the contractual obligations through annual reviews of the contracts and the specified deliverables.
- Ensure that investigations and/or audits are initiated due to complaints or issues identified for not meeting contract requirements.
- Ensure system cooperation in the event of a request for review under AITA or POPA.
- Ensure processes for all audits are clearly documented, retained and there are clearly defined steps on how to escalate issues of non-compliance.

Superintendent

Vendor Management

Pre-contract and Planning:

- Develop a vendor management plan identifying the following:
  - Determine the service and why it is needed.
  - Identify the personal information that the service provider will be asked to collect, use, disclose on behalf of the Thrive Charter School Society to perform its services.
  - Identify the legal authority for the collection and disclosure of the personal information.
  - Determine the classification of personal information that the service provider will collect, use or disclose on behalf of the public body.
  - Determine capability of considered service to meet requirements under the AITA and POPA Acts.
- Prior to selecting a vendor, ensure that employees review and conduct appropriate privacy and security reviews for each potential service provider and determine, using a PIA, if the service provider(s) will be in compliance with POPA.
- Review and evaluate Privacy Impact Assessments to ensure they are completed where required.
- Once a vendor is selected, ensure that Thrive Charter School Society Article 1 and 2 conditions are included as conditions within the service contract to ensure compliance with AITA and POPA requirements.

Oversight

- Ensure appropriate oversight and monitoring of vendor compliance as outlined in the contract.
- Initiate responses or reporting related to:
  - Safeguards and retention.
  - Complaints.
  - Termination of contract.
  - Requests for access or Correction
  - Control and accountability.
- Ensure all required annual contract and policy reviews are completed as required.
- Ensure corrective action is taken to completion where vendor non-compliance is identified.

Employees and Authorized Personnel

- Strict adherence to procurement, approval, and privacy review procedures.
- Conduct appropriate due diligence prior to engaging a vendor.
- Assess the privacy and security posture of vendors. Define the specific security requirements that contractor must meet. Escalate perceived risks to the Superintendent
- Evaluate data residency, storage, subcontracting, and cloud-hosting arrangements.
- Complete a Privacy Impact Assessment to ensure compliance with all privacy requirements.
- Oversight requirements:

    a. Maintain oversight processes for vendor compliance.
    b. Timely reporting of vendor-related privacy concerns, incidents, or non-compliance.
    c. Establish defined monitoring processes for each part of the life cycle of the project (e.g. Project development (weekly); Implementation (weekly); Ongoing (semi-annually or earlier if required)
- The employee ensures that they have received proper training at address AITA and POPA requirements before handling any personal information.
- Prioritize the protection of confidential and personal information at all times.

Documents and References

Access to Information Act (ATIA)
Protection of Privacy Act (POPA)
Education Act • Student Record Regulation (AR 97/2019)
Policy 214 – Access to Information and Protection of Privacy
Administrative Procedure 214 – Access to Information and Privacy Protection
Thrive Charter School Society Privacy Management Plan

Policy 214.2 – Data Breach Management, Incident Notification, Reporting, Containment and Progress Tracking

Policy Statement

Thrive Elementary Charter School Society is committed to protecting personal information from unauthorized access, collection, use, disclosure, alteration, loss, theft, destruction, or other forms of privacy breach.

The Society recognizes that privacy breaches may create significant harm to students, families, staff members, volunteers, and community stakeholders. The Society shall respond promptly, consistently, and responsibly to all suspected or confirmed privacy breaches in accordance with the Protection of Privacy Act (POPA), the Access to Information Act (ATIA), and all applicable legal and regulatory requirements.

The Society shall establish procedures for breach containment, investigation, risk assessment, notification, documentation, mitigation, monitoring, and corrective action. It will also maintain a privacy breach register documenting all suspected and confirmed breaches, investigations, notifications, mitigation measures, and corrective actions. The Society shall respond to and report privacy breaches to the required bodies as soon as practicable.

Definitions

Privacy Breach: Unauthorized access to, collection, use, disclosure, loss, theft, modification, destruction, or disposal of personal information.

Containment: Immediate actions taken to stop or reduce the impact of a breach.

Progress Tracking: The process the system uses to document steps taken to contain a breach and to properly notify required bodies of any breach.

Affected Individual: A person whose personal information may have been involved in a breach.

Significant Breach: A privacy breach that creates a real risk of significant harm to an individual or the Society. To assess whether a breach creates a real risk of significant harm, the Society shall consider:

- whether the information has been or may be misused;
- whether the breach involved malicious intent;
- the sensitivity of the information;
- mitigating measures taken; and
- any other relevant factors.

Significant Harm: Significant Harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, identity theft, financial loss, negative impacts on insurability or credit rating, damage to property, or other legal or financial harms.

Notification: The informing of affected individuals, the Privacy Commissioner and the Minister in the event of a privacy breach.

Procedures

Privacy Officer

Data Breach Management:

1. Establish processes to collect personal information in accordance with all requirements identified in the POPA legislation and regulation.
2. Establish processes to protect personal information that is in the custody of the public body (Thrive Charter School Society and Thrive Elementary Charter School).
3. Direct the development of a Privacy Management Plan and use of Privacy Impact Assessment as stipulated in the POPA legislation and regulation. Where appropriate, privacy breaches may trigger review or revision of an existing Privacy Impact Assessment.
4. Directs employees to ensure data collection and retention be limited to the data required to support the Society's Charter Document and requirements established by Alberta Education for registration and assurance purposes.
5. Directs employees to establish administrative and technological controls to protect personal information and data from a privacy breach.
6. Develop and implement a Privacy Management Program.
7. All breach documentation shall be retained in accordance with the Society's records retention schedule and applicable legislation.

Data Breach:

1. Ensure the implementation of privacy breach response procedure practices.
2. Receive reports regarding significant breaches where appropriate.
3. Review breaches to identify root causes and required corrective actions.
4. Ensure governance oversight for privacy risk management.
5. Direct the development of safeguards to reduce recurrence.
6. Ensure administration complete appropriate monitoring, progress tracking and follow-up.

Notification:

1. In the event of a data breach, ensure proper notification is made to:
    a. The individual to whom there exists a real risk of significant harm;
    b. Any other stakeholders impacted by the breach;
    c. The Commissioner; and
    d. The Minister.

2. Notification and reporting, made in writing, must include:
    a. Name of the public body;
    b. Description of the circumstances of the loss of personal information due to unauthorized access or disclosure;
    c. Date or period of time on which the loss occurred including the date of loss discovery;
    d. Date when the loss or the unauthorized access or disclosure was discovered and ended;
    e. Description of how the loss or the unauthorized access or disclosure was discovered, including the physical location of the breach (if applicable);
    f. Description of the type of personal information accessed due to unauthorized access or disclosure;
    g. Additional written description to the Commissioner about the loss of information is to include an assessment of the risk of harm and the estimated number of individuals affected;
    h. List of steps the public body has taken to reduce the risk of harm to the affected individuals because of the loss, unauthorized access or unauthorized disclosure of personal information;
    i. List of steps the public body has taken to prevent a subsequent similar loss or unauthorized disclosure of personal information;
    j. Contact information for the public body who will respond on behalf of the public body; and
    k. Copy of the notice of the individual's rights to request a review by the Commissioner under section 37 of the Act.

Superintendent

Data Breach Management:

1. Implement the Privacy Management Program.

2. Establish procedures for privacy breach response.

3. Develop and implement a data management plan to ensure only required data is collected and maintained, including a documented plan for use of and destruction of personal information or non-personal data.

4. Ensure personal information and related data are assigned security classification levels proportional to their sensitivity.

5. Personal information respecting minors and parent financial information shall be treated as high-sensitivity information requiring enhanced safeguards.
6. Ensure staff receive privacy breach response training.
7. Conduct risk assessments and investigations

Data Breach:

1. Work with staff to respond immediately in the event of a data breach, by implementing immediate containment measures to prevent further loss or disclosure of information.
2. Ensure timely investigation and management of the breach.
3. Conduct breach assessments to determine risk and impact.
4. Effectively contain the breach using strategies such as disabling accounts or access, recover records, recover devices, suspend unauthorized disclosure, preserve evidence and work with IT providers to ensure breach is contained.
5. Document breach investigations and actions taken.
6. Ensure corrective actions are implemented to prevent future data breaches. Document all incidents, corrective actions, reporting documentation and follow-up decisions and activities.

Notification and Reporting:

1. Ensure significant breaches are immediately escalated to the system's Privacy Officer.
2. Review the incident and report to the Privacy Officer with the information required for reporting to the Privacy Commissioner and any other required stakeholders.

Employees, Contractors, and Volunteers

1. Contractors, service providers, and third-party custodians shall immediately notify the Society of any suspected or confirmed privacy breach involving the Society's personal information records. This is a contract obligation for all service providers.
2. Priority cooperation with investigations and containment efforts.
3. Follow all privacy and information security procedures.
4. Prioritize protection of confidential information at all times.

Documents and References

Access to Information Act (ATIA)
AITA Regulation
Protection of Privacy Act (POPA)
POPA Regulation
Education Act
Policy 214 – Access to Information and Protection of Privacy
Administrative Procedure 214 – Access to Information and Privacy Protection
Thrive Charter School Society Privacy Management Plan

Policy 214.3 – Response to Correction of Personal Information

Policy Statement

Thrive Elementary Charter School Society recognizes the importance of maintaining accurate, complete, and reliable personal information. Individuals have the right to request correction of their personal information in accordance with the Access to Information Act (ATIA), the Protection of Privacy Act (POPA), and related legislation.

The Society shall establish fair, timely, transparent, and legally compliant processes for responding to requests for correction of personal information.

Correction of personal information is an important part of the Protection of Privacy Act. Ensuring personal information collected and shared, as required, should be correct. Individuals needing to make corrections to their personal information will be provided with reasonable access to make the required corrections. It is important to note that the corrections made must be documented and maintained. Individuals making a correction request will be required to provide identification and verification prior to corrections being made.

Definitions

Correction Request: A request by an individual to correct personal information held by the Society.

Personal Information: Recorded information about an identifiable individual as defined under POPA.

Applicant: An individual making a correction request.

Procedures

Privacy Officer

Data

1. Support transparent and accountable information management practices.
2. Ensure data procedures support compliance with legislation.
3. If a correction cannot be made due to its being ruled as an opinion, the Privacy Officer of the public body must annotate or link the personal information with that part of the requested correction that is relevant and material to the record in question.
4. On correcting, annotating or linking personal information under this section, the head of the TCSS must notify any other public body or any third party to whom that information

has been disclosed unless it is not material or the individual requesting the change agrees that the request is not material. Provide written notice to the individual requesting the correction that it has been made or an annotation or link has been made.

Superintendent

1. Establish procedures for responding to correction requests.
2. Ensure correction requests are processed in accordance with legislative requirements.
3. Ensure records management practices support information accuracy.

School Data Administrator

1. Receive and process correction requests.
2. Coordinate review and response activities.
3. Maintain documentation of correction requests and outcomes.
4. Ensure timelines and legal obligations are met.
5. Review supporting documentation provided by applicants.
6. Correct information where appropriate and authorized.
7. Document decisions where corrections are denied.
8. Allow statements of disagreement where required.
9. Maintain records of correction requests and outcomes.
10. Protect confidentiality throughout the process.
11. Respond to correction requests within legislated timelines.

Employees and Contractors

1. Maintain accurate and complete records.
2. Cooperate with correction review processes.
3. Protect confidentiality during all review activities.

Documents and References

Access to Information Act (ATIA)
Protection of Privacy Act (POPA) • Education Act
Student Record Regulation (AR 97/2019)
Policy 214 – Access to Information and Protection of Privacy
Administrative Procedure 214 – Access to Information and Privacy Protection

Policy 214.4 – Consent, Creation, Use and Disclosure of Non-Personal Data

Policy Statement

Thrive Elementary Charter School Society recognizes the importance of responsible information governance practices relating to non-personal, anonymized, aggregate, statistical, and de-identified information.

The Society may create, use, disclose, analyze, and report non-personal data to support operational planning, educational improvement, accountability, research, reporting, governance, funding requirements, and organizational effectiveness, provided such use is lawful, ethical, and consistent with applicable legislation.

The Society shall ensure that appropriate safeguards are implemented to minimize risks associated with re-identification, misuse, unauthorized disclosure, or inappropriate data handling.

Definitions

Non-Personal Data: Information that does not identify an individual directly or indirectly.

De-identified Information: Information from which direct identifiers have been removed or altered.

Aggregate Data: Combined information presented in summarized form.

Re-identification: The process of linking de-identified information back to an identifiable individual.

Consent: The voluntary, informed, and specific authorization of an individual, or their authorized representative, for the collection, use, disclosure, retention, or disposal of personal information for an identified and reasonable purpose. Consent may be express or implied where authorized by legislation and must be obtained in a manner that a reasonable person would understand. An individual may withdraw consent, subject to legal, regulatory, or operational requirements.

Procedures

Privacy Officer

1. Support responsible and ethical information governance practices.
2. Support ethical and responsible data collection and use.

3. Ensure governance oversight regarding data management including the creation, use and disclosure of non-personal data.
4. Ensure data sharing arrangements include appropriate safeguards.
5. Compliance and oversight on matters of quality assurance, auditability and bias mitigation.

Superintendent

1. Establish procedures governing the consent, use and disclosure of non-personal data. Ensure personal information collection tools contain information about the collection, retention and disclosure of personal information and its purpose.
2. Ensure safeguards are implemented to mitigate re-identification risks.
3. Ensure compliance with legislation and organizational requirements.
4. Ensure de-identification practices are appropriate and reasonable.
5. Assess risks associated with data use and disclosure.
6. Restrict unauthorized re-identification activities.
7. Authorize the disclosure of any non-personal data in accordance with section 23(1) of the Protection of Privacy Act.
8. Review practices periodically to ensure continued compliance.

School Data Administrator

1. Limit access to authorized individuals.
2. Ensure parents are informed of the purpose of the personal information collected and consent (oral, written or electronic) is provided prior to collecting information. Include a consent descriptor for all documents that are used for parents to provide personal information to the school.
3. Maintain appropriate records management and retention practices.
4. Disclose non-personal data created under section 23(1) to another public body for any purpose, or to a person other than a public body only if it meets the requirements as set out in section 23(1) and is approved by the Superintendent.

Employees and Authorized Personnel

1. Use non-personal data only for authorized purposes only.
2. Follow procedures for de-identification and data protection.
3. Prioritize the protection of confidential and sensitive information.

Documents and References

Access to Information Act (ATIA)
Protection of Privacy Act (POPA)
Education Act • Policy 214 – Access to Information and Protection of Privacy
Administrative Procedure 214 – Access to Information and Privacy Protection

Policy 214.5 – Automated Systems Safeguards

Policy Statement

Thrive Elementary Charter School Society recognizes that automated systems, digital technologies, cloud-based services, artificial intelligence tools, analytics systems, and other electronic platforms may create privacy, security, operational, and ethical risks when collecting, using, storing, processing, or disclosing information.

The Society is committed to implementing safeguards, oversight mechanisms, and responsible governance practices to ensure automated systems are used lawfully, securely, ethically, and in alignment with the Protection of Privacy Act (POPA), the Access to Information Act (ATIA), and all applicable legislation.

Definitions

Automated System: Any digital, software-based, algorithmic, cloud-based, or technology-enabled system used to process, manage, analyze, store, or communicate information.

Artificial Intelligence (AI): Technology capable of generating outputs, analysis, recommendations, or content using automated computational processes.

Safeguards: Administrative, technical, operational, and physical controls designed to protect information and systems.

Procedures

Privacy Officer

1. Support responsible governance and oversight of automated systems.
2. Ensure privacy and security considerations are incorporated into governance decisions.
3. Restrict access based on authorized roles and responsibilities.
4. Ensure secure authentication and access controls.
5. Ensure systems support records retention and destruction requirements.
6. Ensure appropriate oversight of artificial intelligence or automated decision-support tools.
7. Conduct periodic reviews of automated systems and associated safeguards.

Superintendent

1. Ensure all operational procedures governing automated systems and digital technologies are followed.

2. Ensure privacy, security, and risk assessments are completed where appropriate.
3. Ensure approved systems meet organizational and legal requirements.
4. Ensure monitoring and oversight processes are maintained.
5. Assess privacy and security risks prior to implementation.
6. Implement technical, physical, and administrative safeguards.
7. Monitor systems for security and compliance concerns.
8. Limit the use of unapproved applications or technologies.

Employees and Authorized Personnel

1. Use only approved digital tools and systems.
2. Follow procedures governing technology and information use.
3. Protection of personal and confidential information.
4. Report security concerns, incidents, or unauthorized system use in a timely manner.

Documents and References

Access to Information Act (ATIA)
Protection of Privacy Act (POPA)
Education Act • Policy 214 – Access to Information and Protection of Privacy
Administrative Procedure 214 – Access to Information and Privacy Protection

Policy 214.6 – Privacy Management Training and Privacy Management Program Review

Policy Statement

Thrive Elementary Charter School Society recognizes that ongoing privacy awareness, education, accountability, and continuous improvement are essential components of effective information governance.

The Society shall maintain a Privacy Management Program (PMP) that supports compliance with the Protection of Privacy Act (POPA), the Access to Information Act (ATIA), and all related legislation. The Society shall ensure that privacy training, program review, policy review, and monitoring activities occur regularly and are documented appropriately.

Definitions

Privacy Management Program (PMP): A coordinated set of policies, procedures, safeguards, governance practices, training activities, and oversight processes designed to support privacy compliance.

Privacy Training: Formal or informal learning activities designed to improve awareness and understanding of privacy obligations and responsibilities.

Procedures

Privacy Officer

1. Support governance oversight for the Privacy Management Program and training.
2. Review Policy 214 and related policies regularly.
3. Support a culture of privacy awareness and accountability.
4. Monitor legislative and regulatory changes.

Superintendent

1. Ensure the Privacy Management Program is maintained and reviewed.
2. Ensure privacy training is provided to school staff annually.
3. Ensure policies, procedures, and safeguards remain current.
4. Conduct periodic reviews of privacy practices and safeguards.
5. Ensure compliance monitoring and internal review processes are implemented.
6. Ensure corrective actions are implemented where required.

7. Maintain inventories, breach logs, and related privacy documentation.

School Data Administrator

1. Maintain records of training participation.
2. Ensure appropriate documentation and record retention for all data collected.

Employees, Contractors, and Volunteers

1. Participate in required privacy training and understand your obligations under the AITA , POPA, Education Act and other relevant regulations.
2. Follow privacy and information management procedures.
3. Protect confidential and personal information.
4. Report privacy concerns or incidents.

Documents and References

Access to Information Act (ATIA)
Protection of Privacy Act (POPA) • Education Act
Policy 214 – Access to Information and Protection of Privacy
Administrative Procedure 214 – Access to Information and Privacy Protection
Thrive Charter School Society Privacy Management Plan