Adopted: 2019-12-03
Revised: 2023-06-27; 2024-05-07

Policy EH

INFORMATION SECURITY & PRIVACY

1. CONTEXT

1.1. The *Act respecting Access to documents held by public bodies and the Protection of Personal Information* ("ARA"), the *Act respecting the governance and management of the information resources of public bodies and government enterprises* and the *Directive gouvernementale sur la sécurité de l'information* imposed obligations on educational institutions in their capacity as public bodies. Every school board is required to have a chief information security officer (CISO) and two (2) coordinators for incident management (COMSI).

1.2. The Information Security and Privacy Policy (Policy) enables the New Frontiers School Board (NFSB) to maintain its reputation, comply with legal requirements, and reduce risks while protecting the information it creates or receives, and for which it is responsible. This information pertaining to human, physical, technological, and financial resources is accessible in digital and non-digital formats; risks threatening the accessibility, integrity and privacy of that information can have consequences that compromise:

- The health or wellbeing of individuals;
- The protection of Personal Information and privacy;
- The delivery of services to the public;
- The image of the school board and of the government.

1.3. This Policy must be read in conjunction with guidelines, frameworks, or other tools in effect at the NFSB regarding information security and the protection of Personal Information.

2. SCOPE

2.1. This Policy applies to "Information Users", such as staff and any natural or legal person who, as an employee, member of the Council of Commissioners, consultant, partner, supplier, student, volunteer, or member of the public, uses NFSB information assets. All Information Users have an obligation to protect information assets made available to them by the NFSB.

2.2. To this end, Information Users must:

- Be aware of and adhere to this Policy, as well as any directives, procedures, and other guidelines arising therefrom, and comply with provisions therein;
- Use the information assets made available to them solely for the intended purposes, and this in accordance with assigned access rights and only when necessary to the performance of their duties;
- Respect the security measures installed on their workstation, and on any other equipment containing information that needs to be protected, and never modify their configuration or deactivate them;
- Comply with legal requirements governing the use of products for which intellectual property rights may exist;
- Report and record, using the appropriate form (Annex I), with their immediate supervisor any act of which they become aware that may constitute a real or presumed violation of security regulations, as well as any problem that might threaten the security of the NFSB's information assets.

2.3. This refers to all information (digital, non-digital, verbal) that Information Users hold in the context of their activities, whether storage of that information is managed by the NFSB or by a third party.

2.4. This Policy provides the NFSB with governance rules regarding Personal Information to enable all persons covered by this Policy to know and understand the legal requirements and protection of Personal Information principles applicable under the ARA. It is also intended to inform any person likely to transmit Personal Information to the NFSB of the rules applicable to its collection, use, release, and retention.

2.5. This Policy:
- Identifies the roles and responsibilities of the individuals covered by this Policy;
- States the legal requirements and principles governing the protection of Personal Information collected, used, released, and kept in the exercise of the duties of the NFSB;
- Identifies specific protective measures applicable to Personal Information collected or used as part of a survey;
- Establishes a complaints processing mechanism regarding this Policy and the protection of the Personal Information at the NFSB;
- Describes the training and awareness activities regarding the protection of Personal Information offered to NFSB;
- Affirms the NFSB's commitment to fully discharge its obligations pertaining to the security of information, wherever it is stored and however it is communicated.

2.6. The NFSB is responsible for:
- The availability of information so that it is accessible in a timely manner to authorized person(s);
- The integrity of information such that it is neither destroyed nor altered in any way without authorization and that the medium used to store it provides the desired stability and sustainability;
- The privacy of information by limiting its disclosure and use to authorized persons, especially when it contains Personal Information.

2.7. This Policy applies to all Personal Information collected by technological means by the NFSB. In the event that the technological means refers to a website or technological means of another organization, the privacy policy of that site or other technological means applies.

2.8. Appendices A through D form an integral part of this Policy and address the following:
- Appendix A: Special Protective Measures for Surveys
- Appendix B: Personal Information Voluntarily Submitted through an Online Form
- Appendix C: Particular Projects
- Appendix D: Training & Awareness Activities

3. GUIDING PRINCIPLES

The following guiding principles inform the NFSB's actions pertaining to information security:
- Develop a full understanding of the information that needs to be protected, including a clear identification of holders and their security profile;
- Understand that the technological environment for digital and non-digital information assets changes constantly and is interconnected with the world;
- Protect information throughout its life cycle (creation, processing, destruction);
- Ensure that employees have access only to information that is required to perform their normal duties;
- Ensure users are informed as to the appropriate utilization of digital and non-digital information assets;
- Ensure users do not share confidential information, or their access to it, unless specific authorization has been granted.

4. DEFINITIONS

The terms used are those of the ARA and other applicable legal frameworks, unless otherwise indicated.

Committee on Access (Law 25 Committee)	Committee on access to information and the protection of Personal Information of the *NFSB,* composed of the person in charge of access to documents and of the protection of Personal Information, the Archivist, and representatives of the following: Systems & Information Technology, Building Services, schools and centres.
Commission	*Commission d'accès à l'information du Québec*
Consent	Agreement, acquiescence, voluntary assent of an authorized person to the collection, use or release of Personal Information. To be valid, subject to other legal requirements, consent must be expressed, free, enlightened and given for specific purposes. It must be requested in clear terms. It is valid only for as long as is necessary to achieve the purposes for which it is requested.

Privacy Impact Assessment	A preventive assessment process that consists of considering all the factors of a project that could have positive or negative consequences on the privacy of the people concerned, in order to identify measures that will better protect their Personal Information and respect their privacy.
Confidentiality Incident	**1.** Access to Personal Information not authorized by law **2.** Use of Personal Information not authorized by law **3.** Release of Personal Information not authorized by law **4.** Loss of Personal Information **5.** Any other breach of the protection of such information
Information User	Person covered by the scope of application of this Policy acting on behalf of the NFSB in the exercise of their duties.
User of NFSB Services	Natural person concerned by the Personal Information collected, used or released who is capable of giving Consent, or when applicable, his or her legal representative or the person having parental authority. Without limiting the generality of the foregoing, and barring exceptions, the person having parental authority Consents for a minor under the age of 14. The minor aged 14 and over or person having parental authority Consents for the minor aged 14 and over.
Personal Information	Information concerning a natural person that directly or indirectly enables that person to be identified.
Anonymized Personal Information	Personal Information for which it is at all times reasonable to foresee in the circumstances that it will no longer make it possible, in an irreversible manner, to directly or indirectly identify the person concerned.
Depersonalized Personal Information	Personal Information that no longer directly identifies the person concerned.
Sensitive Personal Information	Personal Information that, because of its medical, biometric or other intimate nature, or because of the context in which it is used or released, gives rise to a high reasonable expectation of privacy.
Person in Charge	Person designated as person in charge of access to documents and protection of Personal Information.
Applicant	Person submitting a request for access to documents, a request for release of Personal Information or a request for correction under the ARA.

5. ROLES & RESPONSIBILITIES

5.1. Highest Authority

5.1.1. The Highest Authority exercises or delegates in writing the functions of Person in Charge. At NFSB the Highest Authority is Director General who has delegated the function of Person in Charge to the Secretary General;

5.1.2. The Highest Authority must:

- See to it that such exercise of functions is facilitated for the Person in Charge;
- Implement measures to preserve the autonomy of the Person in Charge;
- As soon as possible, notify the Commission in writing of the title, contact information and starting date of the person who exercises the function of Person in Charge;
- Transmit all written requests for access to documents, requests for release or requests for correction to the Person in Charge with diligence;
- Ensure that the Committee on Access is set up and functions properly;
- Establish, by organizational guide, the terms and conditions under which information may be released without the Consent of the persons concerned, in order to prevent an act of violence, including suicide, by members of the personnel;
- Adopt the governance rules and any other policy or framework required to ensure compliance with the ARA, and update them as needed.

5.2. Committee on Access

5.2.1. The Committee on Access:

- Supports the NFSB in the exercise of its responsibilities and the performance of its obligations under the ARA;
- Approves the governance rules regarding Personal Information;
- Is consulted at the beginning of any project to acquire, develop, or overhaul an information system or the electronic service delivery system involving the collection, use, release, retention or destruction of Personal Information, and suggests, at any stage of the project, Personal Information protection measures;
- Exercises any other function related to the protection of Personal Information at the request of the Highest Authority.

5.3. Person in Charge

5.3.1. The Person in Charge:

- Receives requests for access to documents, releases or corrects Personal Information, ensures that they are processed in accordance with the provisions of the ARA, including the transmission of any notice required by the ARA, and renders a decision within the time limits prescribed;
- Assists the Applicant when their request is not sufficiently precise, or when they so request, in identifying the document likely to contain the information sought;
- Assists the Applicant, on request, in understanding the transmitted decision;
- Sees to it that every document that has been the subject of a request for access, release or correction be kept for as long as is required to enable the Applicant to exhaust the recourses provided for in the ARA;
- Coordinates and participates as required in Privacy Impact Assessments for NFSB projects that require it;
- Analyzes and takes position on the application of an exception provided for in the ARA regarding the collection, use, release or retention of Personal Information;
- Where applicable, oversees the drafting of a mandate, agreement, or contract between the NFSB and a person or body involving Personal Information for which they are responsible, when required by the ARA;
- Exercises the responsibilities vested in them by the Organizational Guide Respecting Roles and Responsibilities in the Event of a Confidentiality Incident at the NFSB;
- Ensures that the required data is set up, maintained and entered in the various registers provided for in the ARA ;
- Establishes and keeps up to date, in collaboration with principals and directors of schools/centres, an inventory of its Personal Information files, including in particular, the categories of persons who have access to each file in carrying out their duties;
- Set up and keep up to date the classification plan for the documents it holds;
- Handle complaints regarding the protection of Personal Information in accordance with this Policy;
- Ensure the awareness and training of Information Users with respect to the protection of Personal Information in compliance with this Policy;
- Ensure the development, implementation and dissemination of tools, templates, reference documents or other materials to promote compliance with the ARA by the NFSB and the Information Users;
- Provide support and advice on all matters relating to access to documents or to the protection of Personal Information;
- Act as a representative with other public bodies and the Commission for all matters relating to access to documents and the protection of Personal Information;
- Exercise any other function provided for in the ARA or at the request of the Highest Authority.

5.4. Administration of Schools, Centres, and Services

5.4.1. The Administration of Schools, Centres and NFSB services:

- Ensure compliance with this policy by Information Users under their responsibility;
- Identify, for their school, centre or service, the Personal Information it holds;
- Identify the categories of Information Users under their responsibility who have access to Personal Information, as well as the categories of Personal Information that are accessible to them;

- Implement in their school, centre or service, Personal Information protection measures that are reasonable in light of, among other things, the sensitivity of the information, the purpose for which it is to be used, its quantity, distribution and medium, and ensure that it is disseminated and applied by the Information Users under their responsibility;
- Subject to the preservation calendar of the NFSB or any applicable law, implement in their school, centre or service a procedure for the secure destruction of Personal Information when the purposes for which it was collected or used have been achieved;
- Exercise the responsibilities assigned to them in accordance with the Organizational Guide Respecting Roles and Responsibilities in the Event of a Confidentiality Incident at the NFSB;
- In collaboration with the Person in Charge, ensures that the training and awareness activities provided for in this policy are offered to the Information Users under their responsibility and that they participate in them;
- Collaborate with the Person in Charge to develop, implement and disseminate tools, model documents, reference documents or other materials to promote compliance with the ARA in their school, centre or service;
- Communicate, as required, with the Person in Charge for any question relating to requests for access to documents or the protection of Personal Information in their school, centre or service.

5.5. Information Users

5.5.1. Information Users must:

- Be aware of and comply with this Policy, in particular the legal requirements and principles concerning the protection of Personal Information set out in this Policy;
- Participate in the training and awareness activities provided for in this Policy;
- Use tools, model documents, reference documents or any other documents made available to them to promote compliance with applicable rules, where appropriate;
- Collaborate, upon request, with the Person in Charge when processing a request for access to documents, release or correction of Personal Information or any other similar procedure under the ARA;
- Collaborate, upon request, with the Person in Charge when dealing with a complaint covered by this Policy;
- Communicate, as needed, with their supervisor with respect to this policy to obtain clarification, advice or to inform them of a problem in the application of this Policy or of a specific case involving the protection of Personal Information.

6. LEGAL REQUIREMENTS AND PRINCIPLES CONCERNING THE PROTECTION OF PERSONAL INFORMATION

6.1. Collection

6.1.1. An Information User shall only collect Personal Information that is necessary for the exercise of the rights and powers of the NFSB or for the implementation of a program under its management;

6.1.2. Any collection carried out for another purpose will be permitted in the cases provided for by law and must be authorized in advance by the Person in Charge.

6.1.3. Generally, the information is collected from the person concerned, or his or her representative, and the following information must be provided:

- The name of the public body on whose behalf the information is being collected;
- The purposes for which the information is collected;
- The means by which the information is collected;
- The fact that a reply is obligatory, or that it is optional;
- The consequences in case of a refusal to reply to the request or a withdrawal of Consent to the release or use of information collected following an optional request;
- The rights of access and correction provided by the ARA;
- Where applicable, any other information required by the ARA and applicable to the situation in question.

6.1.4. Any user of NFSB Services who provides their Personal Information in the course of collection under the ARA Consents to its use and release for the purposes disclosed at the time of collection.

6.1.5. If the collection is performed from the person concerned using technology that includes functions allowing the person concerned to be identified, located, or profiled, the person concerned must be informed beforehand:
- Of the use of such technology;
- Of the means offered to activate the functions that allow a person to be identified, located or profiled.

6.1.6. Any collection of Personal Information concerning a minor under 14 years of age may not be made from them without the Consent of the person having parental authority or of the tutor, unless collecting the information is clearly for the minor's benefit. In this case, the Person in Charge must be informed in advance.

6.1.7. Any collection of Personal Information when offering to the public a technological product or service having privacy settings must be carried out in such a way that those settings provide the highest level of confidentiality by default, without any intervention by the person concerned. This does not apply to privacy settings for browser cookies.

6.2. Use

6.2.1. An Information User may use Personal Information for the purposes for which it was collected;

6.2.2. Use for another purpose will be permitted with the Consent of the authorized person;

6.2.3. Wherever possible, such Consent should be obtained expressly, preferably in writing. However, when Sensitive Personal Information is involved, Consent must be obtained expressly;

6.2.4. Use for another purpose may be permitted, without the Consent of the authorized person, in situations provided for in the Act;

6.2.5. Any other use based on an exception provided for by law must be authorized in advance by the Person in Charge;

6.2.6. An Information User has access, without the Consent of the authorized person, to Personal Information when they are qualified to receive it and it is necessary for the discharge of their duties;

6.2.7. When Personal Information is used to render a decision based exclusively on an automated processing of such information, the Information User responsible for the decision must inform the person concerned accordingly no later than the time at which they inform them of the decision. This Information User must also, at the request of the User of NFSB Services concerned, inform them:
- Of the Personal Information used to render the decision;
- Of the reasons and the principal factors and parameters that led to the decision;
- Of their right to have the Personal Information used to render the decision corrected.
- Of their right to submit observations to an Information User who is in a position to review the decision.

6.3. Release

6.3.1. An Information User shall not release Personal Information without the Consent of the authorized person;

6.3.2. Wherever possible, Consent should be obtained expressly, preferably in writing. However, when Sensitive Personal Information is involved, Consent must be obtained expressly;

6.3.3. An Information User may release Personal Information without the Consent of the person concerned in the cases provided for by law, taking into account, where applicable, any internal framework measures that may exist at the NFSB;

6.3.4. The release of Personal Information without the Consent of the authorized person in the cases provided for by law must be authorized in advance by the Person in Charge.

6.4. Retention and Destruction

6.4.1. An Information User must know and apply the security measures determined by the NFSB for each Personal Information to which they have access, reference Organizational Guide EHB "Archives".

6.4.2. Failing this, an Information User shall take such security measures as are appropriate to ensure the protection of Personal Information to which they have access, and as are reasonable in light of the sensitivity of the information, the purpose for which it is to be used, its quantity, distribution and medium;

6.4.3. An Information User who has knowledge of a Confidentiality Incident must apply the Organizational Guide Respecting Roles and Responsibilities in the Event of a Confidentiality Incident at the NFSB.

6.4.4. When an Information User becomes aware or has reasonable cause to believe that the Personal Information kept by them is no longer up to date, accurate and complete for serving the purposes for which it was collected or used, they shall promptly notify their school, centre, or service management so that appropriate action can be taken;

6.4.5. An Information User shall be aware of and apply the retention calendar (time period and manner prescribed) of the NFSB or any other similar measure implemented in their school, centre or service with respect to Personal Information to which they have access ;

6.4.6. Failing this, an Information User must take measures to securely destroy any Personal Information they keep once the purposes for which it was collected or used have been accomplished. Such measures must be reasonable in light particularly of the sensitivity, quantity and medium of the Personal Information concerned;

6.4.7. The use of Anonymized Personal Information is permitted for purposes of public interest, when the purposes for which it was collected or used have been accomplished and with the authorization of the Person in Charge.

7. COMPLAINTS PROCESSING

7.1. Filing a Complaint & Contents

7.1.1. A person may file a complaint with the Person in Charge regarding the NFSB's non-compliance with its obligations under this policy and the protection of Personal Information.

7.1.2. Such complaint should be sent by e-mail to the following address: secgen@nfsb.qc.ca .

7.1.3. The complaint must include a description of the event leading to the complaint, including the period concerned, the issue or Personal Information involved, and the nature of the remedy sought.

7.1.4. If the complaint involves the conduct of the Person in Charge, it will be addressed and handled by the Director General.

7.2. Processing a Complaint

7.2.1. The Person in Charge acknowledges receipt of the complaint within a reasonable time of receipt.

7.2.2. The Person in Charge may summarily reject any complaint that is frivolous, vexatious or made in bad faith. They must then inform the person who lodged the complaint.

7.2.3. The Person in Charge may refuse to process a complaint if the event has been the subject of legal proceedings, including any application before the Commission.

7.2.4. The Person in Charge analyses the complaint with diligence and transmits his or her conclusion to the person who lodged the complaint within 30 days of receiving it.

7.2.5. Where applicable, the Person in Charge ensures that the appropriate corrective action is taken.

8. MEASURES TAKEN TO ENSURE THE CONFIDENTIALITY & SECURITY OF PERSONAL INFORMATION

8.1. The NFSB is committed to protecting the Personal Information entrusted to it, in accordance with its obligations and this policy.

8.2. Personal Information is kept for as long as necessary to carry out NFSB activities and in accordance with applicable legislative provisions.

8.3. To this end, the NFSB implements security measures to adequately ensure the confidentiality of the Personal Information it collects, such as computer software or strict procedures for accessing this information, as well as control and verification measures.

8.4. The NFSB also has strict Confidentiality Incident procedures designed to limit the consequences of such an incident and ensures that Personal Information is destroyed in a secure manner to maintain confidentiality.

8.5. All NFSB employees are required to respect the confidentiality of Personal Information collected.

9. RIGHT OF ACCESS & CORRECTION

9.1. Users may request access to their Personal Information held by the NFSB, in accordance with the provisions of the ARA. They may also request the correction of any Personal Information concerning them that is inaccurate, incomplete, or equivocal, or when the collection, communication or retention of such Personal Information is not authorized by law.

9.2. This request must be made in writing to the person responsible for access to information and protection of Personal Information: Secretary General: secgen@nfsb.qc.ca .

10. SANCTIONS

10.1. Any information user who contravenes this Policy, or the information security measures resulting from it, is subject to sanctions in accordance with the nature, severity, and consequences of the contravention as prescribed by applicable law or internal disciplinary regulations (including those stipulated in collective agreements and school board policies). Any resulting penalty or fine may be transferred to the information user.

11. APPROVAL, AMENDMENTS, PUBLICATION & INFORMATION

11.1. This policy, and any amendments thereto, are approved by the Council of Commissioners, on the recommendation of the Committee on Access.

11.2. The Person in Charge shall ensure that this policy is published on the NFSB website.

11.3. Amendments are subject to public notice on the NFSB website. Amendments will come into effect 15 days after the date of publication of the notice. The notice must indicate the general purpose of the changes made to the policy, which must be specified in a section dedicated to this policy on the website and indicate the date on which the changes take effect.

11.4. Users of NFSB services are therefore requested to consult the NFSB website and this Policy regularly to check for any changes.

11.5. All Users of NFSB services are deemed to have read, accepted, and acknowledged the validity of this Policy. Users of NFSB services are deemed to have accepted the modifications if they continue to use the Sites or participate in NFSB activities after the amendments come into effect.

11.6. For any questions about this policy, you can contact the Secretary General: secgen@nfsb.qc.ca .

End
+ 5 Annexes

Adopted: 2019-12-03
Revised: 2023-06-27; 2024-05-07

Policy EH

INFORMATION SECURITY & PRIVACY

APPENDIX A:
Special Protective Measures for Surveys

A.1 Surveys Covered

Only a survey involving the use or collection of Personal Information is covered by this policy. Where applicable, all types of survey (e.g. opinion, satisfaction, service quality measurement, market research) are covered, whatever their form (e.g. individual or group interview, questionnaire survey, automated survey).

A.2 Necessity

An Information User must, before beginning a survey, assess the necessity of conducting the survey as part of the mission of the NFSB. In doing so, an Information User must:

- Establish the purpose and objectives of the survey;
- Verify the possibility of conducting the survey without using or collecting Personal Information;
- Assess the ethical aspect of the survey, taking into account, in particular, the nature of the survey, the persons concerned, the sensitivity of the Personal Information collected and the purpose for which it is to be used, with the support of a person with knowledge of ethics, if necessary.

A.3 Protective Measures

An Information User must also, before beginning a survey:

- Identify the Personal Information to be used and obtain the necessary authorizations;
- Ensure that the quantity of Personal Information used or collected is limited and avoid the collection of Sensitive Personal Information;
- Determine who will have access to the Personal Information used or collected in the course of the survey, the security measures that will be applied to ensure its protection, the length of time it will be kept and destroyed, all in accordance with legal requirements and the principles set out in this policy;
- If necessary, carry out a Privacy Impact Assessment.

A.4 Approval and Consultation

Before conducting the survey, an Information User must obtain the approval of the management of the school, centre or service concerned. The Person in Charge or the Committee on Access may be consulted.

Adopted: 2019-12-03
Revised: 2023-06-27; 2024-05-07

Policy EH

INFORMATION SECURITY & PRIVACY

APPENDIX B:
Personal Information Voluntarily Submitted Through an Online Form

B.1
In the event that a user of School Board services voluntarily releases personal or otherwise confidential information using an online form, only the information required to respond to the user's request or message will be collected and used. Only "Information users", as defined above, will have access to the information submitted.

Adopted: 2019-12-03
Revised: 2023-06-27; 2024-05-07

Policy EH

INFORMATION SECURITY & PRIVACY

APPENDIX C:
Particular Projects

C.1 Particular Projects

An Information User responsible for a project hereinafter mentioned shall ensure that a Privacy Impact Assessment is carried out under the coordination of the Person in Charge and that all conditions set out in the ARA with respect to such project are complied with:

a) Any project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, release, retention or destruction of Personal Information;

b) Collection of Personal Information for another public body if it is necessary for the exercise of the rights and powers or for the implementation of a program of the public body with which it cooperates to provide services or to pursue a common mission;

c) Release of Personal Information without the Consent of an authorized person for study or research purposes or for the production of statistics;

d) Release of Personal Information without the Consent of an authorized person:
   - To a public body or an agency of another government if it is necessary for the exercise of the rights and powers of the receiving body or the implementation of a program under its management;
   - To a public body or an agency of another government if it is clearly for the benefit of the person to whom it relates;
   - To a person or a body where exceptional circumstances justify doing so;
   - To a person or body if it is necessary for the purposes of a service to be provided to the person concerned by a public body, in particular for identifying the person;

e) Release of Personal Information outside Québec;

An Information User responsible of a project hereinafter mentioned shall ensure that a written agreement or contract has been concluded under the direction of the Person in Charge and is in force before proceeding with any collection, use or release of Personal Information:

- In the situations referred to in sections b), c), d), and e) immediately above;
- For the release Personal Information without the Consent of the authorized person to any person or body if the information is necessary for carrying out a mandate or performing a contract for work or services entrusted to that person or body by the public body.

Adopted: 2019-12-03
Revised: 2023-06-27; 2024-05-07

Policy EH

INFORMATION SECURITY & PRIVACY

APPENDIX D:
Training & Awareness Activities

D.1
When an Information User is hired at NFSB, and as needed thereafter, their superior must provide them with a copy of this policy and the Organizational Guide Respecting Roles and Responsibilities in the Event of a Confidentiality Incident at the NFSB, and provide information needed to understand them.

D.2
On an annual basis, the school, centre or service management, in collaboration with the Person in Charge, ensures that the Persons under their responsibility are made aware of the requirements and principles surrounding the protection of Personal Information, for example:

- Their roles and responsibilities with regard to the protection of Personal Information;
- The security measures for the protection of Personal Information;
- The rules governing the retention and destruction of Personal Information;
- The identification and management of Confidentiality Incidents.

D.3
Awareness activities are carried out in a variety of ways: training, discussion sessions, e-mail information capsules, etc.

D.4
If necessary, the Person in Charge may identify training or awareness activities that need to be implemented for a category of people, a school, a centre or a service, on one or more subjects that they determine.

Policies EH & EHB
Annex I

Potential Violation of a Security Regulation

This form is to be used to record a real or presumed violation of our security regulations. It is related to Policy EF "Information Security and Privacy" and Policy EHB "Archives" (Breach of Confidentiality, A.). Once completed by the supervisor, it is to be forwarded to the Secretary General.

Date of Act/Issue	**Date of Act/Issue becoming known**

DESCRIPTION OF ACT/ISSUE

DID THE ACT/ISSUE INVOLVE PERSONAL INFORMATION?
No ____ Yes____

MEASURES TAKEN SINCE ACT/ISSUE

OTHER COMMENTS

NAMES & SIGNATURES			
Name		Name	
Signature		Signature	
Employee	Date	Supervisor	Date