PRIVACY POLICY

INTERNATIONAL BUREAU FOR CHILDREN'S RIGHTS

Version 1.0

December 1, 2023

BUREAU
INTERNATIONAL
DES DROITS DES ENFANTS

INTERNATIONAL
BUREAU
FOR CHILDREN'S RIGHTS

OFICINA
INTERNACIONAL
DE LOS DERECHOS DEL NIÑO

المكتب الدولي لحقوق الطفل

Table of contents

Purpose of policy 4
Scope of application....4
Governance of the policy....5
Responsibilities 5
Access to Information and Privacy Committee 5
Definitions....6
IBCR affiliates 6
The principles of privacy protection 6
Personal information 6
Publicly available personal information 7
Sensitive personal information 7
Personal information categories....8
Privacy breaches 9
Meaningful consent 9
The IBCR's obligations....10
Providing a confidentiality notice to third parties....10
Providing a notice of consent for the collection of non-sensitive personal information 10
Obtaining valid consent for the collection of sensitive personal information 10
Transparent consent management practices 11
Requesting a copy or correction of personal information 11
Refusal to provide or share personal information 11
Withdrawal of consent....12
Type of personal information collected 13
Management and protection of personal information....14
Management of personal information 14
Use of personal information 14
When the information is shared 15
Personal information categories 17
Personal information categories 17
Personal information categories 19
In the event of a privacy breach 19

Contact information of persons responsible for the policy 20
APPENDIX 2
Access to Information and Privacy Committee 20
APPENDIX 3 21
INVESTIGATION PROTOCOL 21
Protocol for investigating privacy breaches 21
Fact-checking 21
Analysis of facts 21
Conclusions and recommendations 22
Decisions resulting from an investigation 22
APPENDIX 4 23
Sample privacy notice and consent notice 23
Privacy notice for email communications 23
Notice of consent for databases (lists) 23
Notice of consent for the collection of personal information 23
APPENDIX 1 20

Purpose of the policy

The International Bureau for Children's Rights (IBCR) is committed to protecting the privacy of all individuals who entrust the organisation with their personal information. The IBCR has therefore established a clear and binding framework to ensure that personal information is used, stored and destroyed appropriately.

This policy is based on the principles of confidentiality, professionalism and transparency. It aims to:

1. Provide a framework for the collection, use and protection of personal information
2. Describe the IBCR's practices so that everyone whose personal information is collected knows their rights and the IBCR's obligations
3. Ensure that the IBCR only collects whatever personal information is essential for its activities

Scope of application

The Privacy Policy applies to all personal information collected by IBCR. It applies for as long as the personal information is used and retained; that is, until the information is permanently destroyed by the IBCR.

The IBCR is committed to only collecting personal information when needed to:

- Carry out its activities, including those related to awareness-building and public engagement
- Fulfil the organisation's moral, administrative or legal obligations

Only the IBCR and its employees, interns and volunteers are bound to the terms of this policy on the collection, use, storage and destruction of personal information. The policy is not binding on other persons affiliated with the IBCR.[1]

Any obligations set out in Quebec privacy laws take precedence over this policy.

[1] See the definition of IBCR affiliates below

Governance of the policy

Responsibilities[2]

The policy is the subject of a resolution of the IBCR's Board of Directors. It will be reviewed every two years or as needed for administrative or legal compliance updates.

The Director General is responsible for ensuring that the policy is properly disseminated and adhered to by all employees, interns and volunteers. The Director General also responsible for ensuring that any reported privacy breaches are addressed.

The Director of Human Resources, Administration and Security is responsible for ensuring that the policy is properly understood and applied.

The Director of Programmes and Education is responsible for ensuring that the personal information of all children who participate in IBCR activities is collected, used and protected in accordance with the standards set out in the IBCR's Child Safeguarding Policy.

Access to Information and Privacy Committee

The Access to Information and Privacy Committee[3] (known by its French acronym, CAIPR) is responsible for making sure the Privacy Policy is properly applied. It also issues recommendations on how current practices can be improved or rectified. In addition, the CAIPR plays a role in the investigation of privacy breaches.[4]

[2] The contact information for the individuals occupying these positions is available in the Appendix

3 Details about the CAIPR, including its composition, are available in Appendix 3

[4] See Appendix 3

Definitions

IBCR affiliate

The following are considered IBCR affiliates:

Child	Any person under the age of 18 who participates in or benefits from the IBCR's activities.
Legal guardian	The legal guardian of a child whose personal information was obtained under a request for consent in relation to an IBCR activity.
Employee	An individual who is employed under contract by the IBCR. **This may include their dependents and emergency contact persons.*
Intern or volunteer	An individual who carries out work for the IBCR under an internship contract or volunteer agreement.
Foreign assignment volunteers	An individual who carries out work for the IBCR under a foreign assignment volunteer agreement.
Supplier	A person or entity that is bound by a contract, purchase order or other agreement to provide goods or services to the IBCR in exchange for financial compensation.
Partner	An individual or legal entity that maintains a relationship with the IBCR as a partner, collaborator or beneficiary of the IBCR's activities or advocacy work.
Observer	Anyone person who participates in an event organised by the IBCR. This includes individuals who observe the IBCR's activities and who, in doing so, come into contact with children, employees and stakeholders associated with these activities.
Funding partner	Granting agencies, private donors, foundations, etc.

The principle of privacy protection

In principle, privacy protection means ensuring that any information or data that the IBCR shares with a third party, including related entities and individuals,[5] is used and stored in a manner that complies with the consent.

Personal information

The following is a translation of the definition provided on the Government of Quebec's website:[6]

[5] Definition inspired by: Definition of data privacy – Glossary CDP.com

[6] Key concepts related to personal information | Gouvernement du Québec (quebec.ca)

Personal information is any information which relates to a natural person and directly or indirectly allows that person to be identified. Here are its defining characteristics:

- *It lets someone know something*
- *It is related to a natural person*
- *It allows for a person to be distinguished from another or provides insights into their nature*

Publicly available personal information

This information is made available to the public or found in media publications. This policy does not deal with publicly available information.

Sensitive personal information

Some personal information is sensitive. The IBCR uses the Quebec government's definition of sensitive information:[7]

Personal information is sensitive if, due to its nature, in particular its medical, biometric or otherwise intimate nature, or the context of its use or communication, it entails a high level of reasonable expectation of privacy.

Sensitivity therefore relates to the degree to which it is reasonable to expect that the personal information will be kept confidential. When the expectation is high, the information is considered sensitive personal information.

In other words, sensitive personal information is any information that may expose an individual to a higher level of risk because of:

- *The source*
- *The degree of sensitivity*
- *The potential repercussions if it is disclosed or used*

Both the context and nature of the information must be considered when assessing the sensitivity of personal information. Information that will generally be considered sensitive includes:

- *Financial information*
- *Genetic or biometric information*
- *Health information*
- *Sex life or sexual orientation*
- *Religious or philosophical beliefs*
- *Political opinions*
- *Ethnic and racial origins*

[7] Key concepts related to personal information | Gouvernement du Québec (quebec.ca)

Personal information categories

The IBCR uses the following categories of personal information to assess their sensitivity and determine specific practices related to their use, disclosure, retention and destruction.

Category	Nature of personal information
Personally identifiable information **Including those of persons considered minors under the law*	Date of birth, home address, telephone number, work permit number, criminal record, passport number, ID card number, health card number, driver's license number, photo, biometric information Home addresses and telephone numbers of legal guardians and emergency contact persons
Information about the work and activities carried out by the IBCR	First name, last name, personal email address Request for a leave of absence (all types), first and last names and contact information for references provided in applications, content of résumé, academic and professional certifications/credentials, contract, training, performance appraisals, compensation and benefits, salary, disciplinary file, recruitment file
Personally identifiable financial information	Bank details, Quebec business number, social insurance number or equivalent, and voided cheque (in IBCR offices where required by law), full names and dates of birth of beneficiaries, place of residence for tax purposes, financial transaction amounts and dates, contact information of the person in charge of payments, contract details including the contract value and terms of payment
Information related to cookies and digital interactions	Emails, folders and documents stored in and accessible via the work computer, browsing history, location information; applications and the content of applications used for business interactions, including OneDrive, SharePoint, chat and videoconferencing (...)
Travel information	Passport and/or identity card, travel visa, travel vaccinations, medical records and details, immunisations, date of birth, home address, emergency contact details and nature of relationship, information contained in "proof of life" documents (where applicable), full names and dates of birth of children and dependents

Privacy breaches

The following is a translation of the definition provided on the Government of Quebec's website:[8]

The unlawful access, use, disclosure or loss of personal information, as well as any other failure to protect such information.

Examples of privacy breaches:

- *An employee who overrides their access rights to view someone's personal information even though it's not necessary for the performance of their job, or a hacker who gains access to a system*
- *An employee who takes personal information from a database that they use for work and uses it to impersonate another person*
- *An employer that mistakenly sends a communication to the wrong person*
- *A person who loses documents containing personal information or who has such documents stolen from their possession*
- *A person who gains access to a database containing personal information in order to alter the information*

Meaningful consent

The organisation is required to obtain meaningful consent for the collection of sensitive personal information.

The following is a translation of the definition provided on the Government of Quebec's website:[9]

To be valid, the consent obtained must be:

- *Express: explicit and unequivocal consent granted with a positive action that clearly demonstrates agreement. Having a document signed is the best method.*
- *Free: consent given without the influence of a constraint or undue pressure.*
- *Informed: consent given after receiving complete information about what is involved, including sufficient information to assess the scope.*
- *Specific: consent that is limited to clearly defined objectives.*
- *Time-limited: consent that is given for a predefined period of time.*

All persons involved must be given complete information and their questions must be answered.

[8] Key concepts related to personal information | Gouvernement du Québec (quebec.ca)
[9] Consent to the use of biometrics | Commission d'accès à l'information du Québec (gouv.qc.ca)

The IBCR's obligations

Providing a privacy notice to third parties

Whenever we deal with a third party, the IBCR will send them a privacy notice detailing the terms surrounding the use and disclosure of information and data.

Providing a notice of consent for the collection of non-sensitive personal information

The IBCR will send a notice of consent[10] to any individual whose non-sensitive personal information will be collected. The notice will outline the procedures for modifying, refusing or withdrawing consent.

Obtaining valid consent for the collection of sensitive personal information

The IBCR complies with Quebec laws and regulations relating to obtaining valid consent for the collection of sensitive personal information.[11]

Sensitive personal information cannot be used without first obtaining valid consent from the persons concerned, except as provided for by law.

When performing their duties, all IBCR employees, trainees and volunteers must obtain the valid consent of any person whose sensitive personal information is collected before this information is use, stored or disclosed.

To obtain valid consent, IBCR will:

- Prepare a written request describing how sensitive personal information is collected, used and stored.
- Include, where necessary, the valid request for consent in the forms, emails, documents and other documents made available via its website.
- Have a consent form signed by a person with parental authority[12] over a child who participates in or is the beneficiary of an IBCR activity, after having provided the required information to that person and the child in question.
- Inform all users of its website, ibcr.org, of the collection of information and the use of cookies.
- Translate all documents used to obtain valid consent so that consent is obtained in the language used by the concerned individual, including children.

Valid consent from children

At all times and in all countries where it operates, the IBCR will comply with the laws in effect, including those related to obtaining consent from children and their legal guardians.

---

[10] Available in the appendix
[11] Consent to the use of biometrics | Commission d'accès à l'information du Québec (gouv.qc.ca)
[12] As defined by law

Transparent consent management practices

The IBCR will ensure that individuals have the option to accept or refuse consent to the collection, use and disclosure of personal information, sensitive or otherwise.

To support this commitment, the IBCR will make this policy available and establish conditions allowing individuals to refuse or accept consent, or to make changes to their consent or personal information.

Requesting a copy or correction of personal information

The IBCR endeavours to keep personal information as complete and up-to-date as possible. However, individuals who have shared their information are responsible for providing updates as necessary.

Any individual may request access to or correction of their personal information, except as provided for by law or under certain confidentiality obligations related to the nature of certain files.

To make such requests, an individual or their legal guardian must send a request bearing their handwritten or electronic signature:[13]

- By mail: 805 Rue Villeray, Montreal, Quebec, H2R 1J4, or
- By email: protectiondonnées@ibcr.org.

The IBCR has mandated its Access to Information and Privacy Committee to respond to such requests within 30 days. After this period and as provided by law, the personal information access request is considered refused.

- If a request is accepted, the IBCR will mail the requester a list of the personal information it has on file for them.
- If a request is refused, the IBCR will have to justify its decision based on the cases provided for by law.

Employees, interns or volunteers wishing to obtain or correct their personal information must submit a request to the appropriate internal staff member, depending on the nature of the information.

Refusal to provide or share personal information

Individuals have the right to refuse to provide their personal information or to refuse to allow certain forms of use or disclosure of their personal information.

To do so, an individual or their legal guardian must send a request bearing their handwritten or electronic signature:[14]

- By mail: 805 Rue Villeray, Montreal, Quebec, H2R 1J4, or

[13] Electronic signatures must be verifiable and certificate-based (Adobe, Microsoft or other)
[14] Electronic signatures must be verifiable and certificate-based (Adobe, Microsoft or other)

- By email: protectiondonnées@ibcr.org

The refusal must be provided in writing to the person who requested it. It must also explicitly outline which the information cannot be shared, used or disclosed to a third party.

The IBCR will respect the wishes of the refusing party, inform them of its implications and ensure that the terms are applied within 30 days, subject to all applicable legal and administrative obligations in force.

If consent is refused

If an individual refuses to consent, the IBCR may not be able to establish or maintain a collaborative or contractual relationship with them. A refusal may also prevent an individual from participating in IBCR activities and/or from collecting any associated allowances, per diems or expense reimbursements.

If a refusal prevents the IBCR from fulfilling its administrative or legal obligations or from carrying out internal control procedures or other activities, the IBCR reserves the right to terminate the collaborative relationship.

Withdrawal of consent

Consent may be withdrawn at any time. Like requests to modify or correct information, withdrawal of consent requests must be sent to the IBCR.

To do so, an individual or their legal guardian must send a request bearing their handwritten or electronic signature:[15]

- By mail: 805 Rue Villeray, Montreal, Quebec, H2R 1J4, or
- By email: protectiondonnées@ibcr.org

The IBCR has mandated its Access to Information and Privacy Committee to respond to such requests within 30 days. After this period and as provided for by law, the personal information access request is considered refused. If you wish to withdraw your consent to the use of cookies, you can update your consent on the IBCR website.

If you withdraw consent, the IBCR will stop collecting and/or using your personal information. If a withdrawal of consent prevents the IBCR from fulfilling its administrative or legal obligations or from carrying out internal control procedures or other activities, the IBCR reserves the right to terminate the collaborative relationship.

[15] Electronic signatures must be verifiable and certificate-based (Adobe, Microsoft or other)

Types of personal information collected

As part of its commitment to acting in an ethical and transparent manner, the IBCR will only collect the personal information described in this policy and, where applicable, will inform the persons concerned by specifying the nature of the information, how it is used and the privacy protection measures associated with it.

Category	Type of personal information	Sensitivity level
Personally identifiable information **Including those of persons considered minors under the law*	Date of birth, home address, telephone number, work permit number, criminal record, passport number, ID card number, health card number, driver's license number, photo, biometric information Home addresses and telephone numbers of legal guardians and emergency contact persons	Sensitive personal information
Information about the work and activities carried out by the IBCR	First name, last name, personal email address Request for a leave of absence (all types), first and last names and contact information for references provided in applications, content of résumés, academic and professional certifications/credentials, contract, training, performance appraisals, compensation and benefits, salary, disciplinary file, recruitment file	Non-sensitive personal information
Personally Identifiable Financial Information	Bank details, Quebec business number, social insurance number or equivalent, and voided cheque (in IBCR offices where required by law), full names and dates of birth of beneficiaries, place of residence for tax purposes, financial transaction amounts and dates, place of residence for tax purposes, contact information of the person in charge of payments, contract details including the contract value and terms of payment, financial transaction amounts and dates	Sensitive personal information
Information related to cookies and digital interactions	Emails, folders and documents stored in and accessible via the work computer, browsing history, location information Applications and the content of applications used for business interactions, including OneDrive, SharePoint, chat and videoconferencing	Sensitive personal information

Travel information	Passport and/or identity card, travel visa, travel vaccinations, medical records and details, immunisations, date of birth, home address, emergency contact details and nature of relationship, information contained in "proof of life" documents (where applicable), full names and dates of birth of children and dependents	Sensitive personal information

Management and protection of personal information

The IBCR takes various measures to control access to any personal information entrusted to it, from the moment the information is collected until it is destroyed. These measures include:

- Assessing the sensitivity of the information based on the definitions established by the Government of Quebec[16]
- Using a decision tree for classifying and archiving digital files, with access limits determined by user, file and authorised person, to ensure that access is only granted to those relevant persons
- Using physical archiving in dedicated spaces kept under lock and key or equivalent to restrict access to authorised persons only

Any failure in relation to the usage, management and protection factors listed below will be considered a privacy breach and will be addressed in accordance with the established investigation protocol.[17]

Management of personal information

Use of personal information

The IBCR will only use your personal information for the following purposes:

Information category	What it is used for
Personally identifiable information	HR files Administrative and legal compliance Service or purchase contracts Payroll and insurance profiles Operations and projects External accounting Health and safety management Accounting documents Consent records
Information about the work and activities carried out by the IBCR	Recruitment Administrative and payroll management Performance management Disciplinary management Complaints management Participation in IBCR activities
Personally identifiable financial information	Payment of all types of compensation, including remuneration, purchase costs, service fees, administrative fees or legal fees Payment of all types of honorariums, per diems, donations or transfers of funds related to the organisation's activities

[16] Key concepts related to personal information | Gouvernement du Québec (quebec.ca)
[17] See Appendix 3

Information related to cookies and digital interactions	Backup and protection of all types of documents, images, emails and correspondence owned by the IBCR (domaine@ibcr.org)
International travel information	Complying with administrative and legal requirements related to persons entering and leaving the country Purchasing airline tickets and booking accommodation Repatriation health insurance Health and safety management

When the information is shared

In order to operate effectively, carry out activities and fulfil its mission, the IBCR collaborates with various affiliated persons.[18] In doing so, the IBCR may disclose some personal information in accordance with the terms and conditions set out below.

Obtaining consent

The IBCR discloses personal information in accordance with applicable consent requirements. More specifically:

- Sensitive personal information is only disclosed if the IBCR has obtained prior valid consent from the person concerned.
- A notice of consent[19] is issued if non-sensitive personal information is disclosed.

The IBCR will not collect any personal information for promotional or advertising purposes or in order to sell the information to a third party without first obtaining valid consent from the concerned person.

Rules concerning the disclosure of personal information

The IBCR takes into account the privacy policies and data protection practices of all third parties and IBCR affiliates with which it collaborates, whether they be individuals or legal entities.

In addition, the IBCR will ensure that all of its contractual agreements include a clause on confidentiality and the protection of personal information. The clause will be consistent with this policy and the laws of Quebec.

Service providers

To support its operations, the IBCR collaborates with various types of service providers.[20]

[18] See the Definitions section
[19] The notice of consent is appended to this policy
[20] Referred to herein as "services"

Service providers may have access to certain types of personal information, as listed below:

Information category	Service provider with access to information
Personally identifiable information	HR* services Payroll services IT* services Criminal record check services Financial and banking services Health insurance services
Information about the IBCR's work and activities	HR services Payroll services IT services Financial and banking services VRSP services
Personally identifiable financial information	IT services Financial and banking services Payroll services HR services RRSP services
Information related to cookies and digital interactions	Digital services IT services Communications services Other services
International travel information	HR services Travel services State administrative services Insurance services IT services HR services

**For reasons related to service functionality and data backup, the IT and Administration services have unrestricted digital access.*

Service providers outside Quebec

The IBCR may use the services of individuals or entities established outside Quebec or whose data is hosted outside Quebec. For example, the IBCR uses the services of Google, Microsoft and HealthBox HR. When personal information is shared with them, the applicable privacy laws fall under a different legal framework.

The IBCR will mention these or similar providers when obtaining consent.

Public agencies and competent authorities

Wherever it operates, the IBCR endeavours to comply with the legal and administrative regulations in effect. The IBCR will therefore share personal information with public agencies and competent authorities when required to do so. For example, the information may be disclosed in tax returns, salary reporting or other filings.

Protection of personal information

Retention of personal information

The IBCR is committed to retaining personal information for a predetermined period of time, using methods that are both secure and conducive to protecting confidentiality.

Information category	Retention period	Storage method
Personally identifiable information	7 years after the end of the contract Or 7 years after project completion	Online file hosted on the IBCR's intranet, with access restricted based on file sensitivity Saved on the IT firm's intranet server Server hosting e-mails containing this information Physical archives kept under lock and key, with restricted access
Information about recruitment activities Administrative and payroll management Performance management Disciplinary management Complaints management IBCR activities	2 years after applications are received 7 years after the end of the contract 3 years after the end of the contract 3 years after a complaint has been closed 7 years after end of project (for activities)	Online file hosted on the IBCR's intranet, with access restricted based on file sensitivity Saved on the IT firm's intranet server Server hosting e-mails containing this information Physical archives kept under lock and key, with restricted access

Personally identifiable financial information	7 years after the end of the contract	Online file hosted on the IBCR's intranet, with access restricted based on file sensitivity Saved on the IT firm's intranet server Server hosting e-mails containing this information Physical accounting archives kept under lock and key, with restricted access
Information related to cookies and digital interactions Digital interactions Cookies	 7 years after the end of the contract 2 months	 Online file hosted on the IBCR's intranet, with access restricted based on file sensitivity Saved on the IT firm's intranet server Server hosting e-mails containing this information Server of the website management company (cookies)
International travel information	6 years after the end of the contract	Online file hosted on the IBCR's intranet, with access restricted based on file sensitivity Saved on the IT firm's intranet server
All sensitive information, at all times:	Can only be accessed by relevant personnel, limited to a maximum of 5 persons.	

Destruction of personal information

The IBCR will retain information in accordance with the time periods specified in this policy. After this time, the information will be destroyed using the following methods:

- Digital files:
    - Documents are moved to a dedicated archive folder for a period of 3 months
    - Documents in the archive folder are deleted after a period of 4 months
    - Documents are backed up on the cloud for a period of 30 days
    - Documents are permanently destroyed on the 31st day

- Physical files (paper):
    - Documents are moved to dedicated archiving boxes kept under lock and key for a period of 3 months
    - Documents are permanently removed from the archives after a period of 4 months and shredded to prevent any information from being recognised
    - The shredded paper is then recycled

Some personal information cannot be destroyed and must be always be retained, particularly in the following circumstances:

- The information is of critical importance
- Destroying the information is not in the best interest of the person involved
- The information must be kept to ensure compliance with legal or administrative obligations
- Destroying the information could be harmful to the IBCR or the person involved

In the event of a privacy breach

Anyone who suspects a real or potential privacy breach can report it to the IBCR by sending an email to:

protectiondonnées@ibcr.org

Emails sent to this address can be seen by the Director General and the Director of Human Resources, Administration and Security.

All information received will be kept confidential and used for the purposes of verification and/or investigation,[21] depending on the nature of the reported information.

21 The protocol for investigating privacy breaches is appended to this policy.

APPENDIX 1

Contact information of persons responsible for the policy

Chairman of the Board of Directors	Théophane Nikyema theophane@nikyema.net
Director General	Martin Causin m.causin@ibcr.org
Director of Human Resources, Administration and Security	Morgane Faber m.faber@ibcr.org
Director of Programmes and Education	Julie Dénommée j.denommée@ibcr.org

APPENDIX 2

Access to Information and Privacy Committee

The committee members are IBCR employees with at least one complete year of service. Members are appointed by the Director General and include representatives from all IBCR departments. Participation is voluntary. Anyone can decline an appointment to the committee without being subject to sanctions.

Members can sit of the committee for a two-year term, which can be renewed once.

Member contact information is available on the IBCR's APCO intranet and the IBCR website www.ibcr.org. In the event of a change, the IBCR will update this information.

The committee is made up of three (3) people who occupy the following roles, as defined by law:[22]

Member's role within the CAIPR	Member's role at the IBCR
Information Access and Privacy Officer	Director of Human Resources, Administration and Security
Information Security and Document Management Manager	Procurement and Logistics Advisor
Any other person (employed by the IBCR or not) whose expertise is required	Child Protection Advisor or Child Safeguarding Advisor

[22] Comité sur l'accès à l'information et la protection des renseignements personnels | Commission d'accès à l'information du Québec

(gouv.qc.ca)

APPENDIX 3

INVESTIGATION PROTOCOL

Protocol for investigating privacy breaches

This protocol supplements the IBCR's Complaints Management and Reporting Policy.

Privacy breaches must be reported as follows:

- Employees, interns and volunteers — In accordance with the Complaints Management and Reporting Policy:
  - In writing by email to solidaires@ibcr.org or protectiondonnées@ibcr.org
  - Verbally or in writing, in person or by email to the Human Resources, Administration and Security Department
- Persons outside the IBCR — By email to protectiondonnées@ibcr.org

Investigation protocol:

The various steps that precede a decision to investigate a privacy breach are aligned with the mechanisms set out in the Complaints Management and Reporting Policy. An investigation is initiated when a complaint has been deemed admissible and the protocol applies for the entire investigation procedure.

In such situations, the Complaints Assessment and Management Committee works jointly with the Access to Information and Privacy Protection Committee to define the investigation framework and to appoint the person or entity responsible for conducting the investigation.

When the committee appoints an employee to lead the investigation, subject to the conditions set out in the Complaints Management and Reporting Policy, the following steps must be followed:

Fact-checking

If the incident involves digital files: obtain digital tracing data from the IT services (indicating who had access and when)

If the incident involves physical files: obtain the physical tracing data concerning the opening of the archive

Analysis of facts

The purpose of the analysis is to determine whether:

- The personal information was stored and used in accordance with the policy
- Access permissions and restrictions were in force
- Only authorised persons had access to the personal information
- The privacy breach occurred because personal information was collected or used in a manner that contravenes the provisions of this policy

Conclusions and recommendations

Based on the analysis of the facts, the CAIPR issues conclusions as to whether a privacy breach occurred. If so, the committee also issues recommendations for remedying the privacy breach.

These recommendations must include corrective and prevention measures to be implemented over time, as well as formal follow-ups to make sure the measures are applied.

The CAIPR must also specify whether or not the incident was accidental or intentional.

The conclusions and recommendations will be presented to the Director of Human Resources, Administration and Security, who will then submit them to the Director General for final approval.

In the event of an intentional incident, the Director of Human Resources, Administration and Security will issue, in addition to the recommendations, a request for disciplinary action or non-disciplinary measures, or report the situation to the appropriate authorities.

Decisions resulting from an investigation

The Director General alone decides on the conclusions and recommendations of the investigation.

The Director of Human Resources, Administration and Security is responsible for maintaining an up-to-date incident log, which is presented annually to the Board of Directors.

The investigation protocol and its contents are considered sensitive information and can only be accessed by members of the Complaints Assessment and Management Committee, the CAIPR, the Director General and the Director of Human Resources, Administration and Security.

APPENDIX 4

Sample privacy notice and consent notice

Privacy notice for email communications

The IBCR will include the following confidentiality notice in all of its email communications to ensure that information is kept confidential:

This message, as well as any attachments, is intended exclusively for its recipient(s). It may contain confidential information and must be treated as such. Any use, reproduction or distribution of this message and any attached files is strictly forbidden without the express authorisation of the sender. If this message has been sent to you in error, please notify the sender by returning the message and then destroy the message and any attached files, without keeping any copies.

Consent notice for contact databases (lists)

The IBCR will communicate the following consent notice to any person whose personal email address is included in its mailing lists:

The International Bureau for Children's Rights (IBCR) cares about your privacy and is committed to keeping your personal information confidential, including your email address. If you no longer wish to receive emails from the IBCR at this email address and would like to be removed from our mailing lists, please write to us at protectiondonnées@ibcr.org.

Notice of consent for the collection of personal information

The IBCR will include the following notice of consent in all forms, documents and emails resulting directly or indirectly from the collection of non-sensitive personal information:

The IBCR respects your privacy and is committed to keeping confidential the personal information collected herein, which will be used for the purposes of RECRUITMENT/IBCR ACTIVITIES/NEWSLETTERS/COMMUNICATIONS AND PROMOTIONS/FUNDRAISING.
Your personal information will not be used for any other reason without your prior valid consent. If you would like to modify, delete or withdraw this consent, please write to us at the following email address: protectiondonnées@ibcr.org or by mail at 805 Rue Villeray, Montreal QC, Canada, H2R 1J4.

The IBCR collects and uses personal information in accordance with its Privacy Policy, which is available on the organisation's website at www.ibcr.org.

To report a privacy breach, please write to: protectiondonnées@ibcr.org