## Definitions

| Term | Definition |
|---|---|
| Personal Information | For the purposes of this policy personal information is defined as information not specifically related to Corus and working at Corus. For example, home address and phone number, education, ethnicity, gender, etc. |
| Manager | As referenced in this policy, a manager is the person to whom an employee directly reports. |

## Overview

Corus is committed to protecting the personal information of its employees against loss or theft, unauthorized access, disclosure, copying, use or modification, regardless of the format in which it is held. Corus strictly follows the guidelines outlined in PIPEDA (see http://www.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00464e.html for more information about PIPEDA).

## Policy

Employees will be informed of the reason for the collection of personal information. Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the employee or as required by law.

Personal information is defined as information about an identifiable individual employee of Corus, including (but not necessarily limited to) any of the following:

- Age
- ID numbers
- Ethnic origin
- Evaluation
- Comments
- Social Status
- Disciplinary Actions
- Employee Files
- Credit Records
- Loan Records
- Medical Records

Personal information does not include the name, title, business address or business telephone number of a Corus Entertainment Inc. employee.

Corus will make every reasonable effort to ensure that employees understand how their personal information will be collected, used and disclosed by Corus and that the employee has consented to this. Employees may be asked to express their consent in several ways, such as verbally, in writing or electronically.

Withdrawing or refusing consent to collect, use or disclose personal information may prevent Corus from providing the employee with employment benefits that they currently receive. It is not the intention of Corus to withhold benefits, services or information from employees who refuse or withdraw consent, however refusal or withdrawal of consent in the case of benefits and pension plans could impede enrolment and ongoing coverage.

The following outlines the rules surrounding information that can be **collected** without employee consent:

- If it is clearly in the individual's interests and consent is not available in a timely way
- If knowledge and consent would compromise the availability or accuracy of the information and collection is required to investigate a breach of an agreement or contravention of a federal or provincial law
- For journalistic, artistic or literary purposes
- If it is publicly available as specified in the regulations

Personal information is primarily collected from the individual, however we reserve the right to collect it from sources such as: criminal background checks where required as a condition of employment, educational to confirm accreditations, personal and employment references prior to the hiring process or for internal transfers and promotions, and medical information for short-term and long-term disability adjudication.

Organizations may **use** personal information without the individual's knowledge or consent only:

- If the organization has reasonable grounds to believe the information could be useful when investigating a contravention of a federal, provincial or foreign law and the information is used for that investigation
- For an emergency that threatens an individual's life, health or security
- For statistical or scholarly study or research (the organization must notify the Privacy Commissioner of Canada before using the information)
- If it is publicly available as specified in the regulations
- If the use is clearly in the individual's interest and consent is not available in a timely way
- If knowledge and consent would compromise the availability or accuracy of the information and collection was required to investigate a breach of an agreement or contravention of a federal or provincial law

Organizations may **disclose** personal information without the individual's knowledge or consent only:

- To a lawyer representing the organization
- To collect a debt the individual owes to the organization
- To comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction
- To the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as required by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act
- To a government institution that has requested the information, identified its lawful authority to obtain the information, and indicates that disclosure is for the purpose of enforcing, carrying out an investigation, or gathering intelligence relating to any federal, provincial or foreign law; or suspects that the information related to national security, the defense of Canada or the conduct of international affairs; or is for the purpose of administering any federal or provincial law
- To an investigative body named in the Regulations of the Act or government institution on the organization's initiative when the organization has reasonable grounds to believe that the information concerns a breach of an agreement, or a contravention of a federal, provincial, or foreign law, or suspects the information relates to national security, the defence of Canada or the conduct of international affairs
- If made by an investigative body for the purposes related to the investigation of a breach of an agreement or a contravention of a federal or provincial law
- In an emergency threatening an individual's life, health or security (the organization must inform the individual of the disclosure)
- For statistical or scholarly study or research (the organization must notify the Privacy Commissioner of Canada before disclosing the information)
- To an archival institution
- 20 years after the individual's death or 100 years after the record was created
- If it is publicly available as specified in the regulations
- If required by law

Upon request, an employee will be informed of the existence, use and disclosure of their personal information and will be given access to that information. Employees will be able to challenge the accuracy and completeness of the information and have it amended as appropriate. Access to and amendment of your personal information will be made within a reasonable timeframe. It is the employee's responsibility to ensure that all personal information is kept up-to-date and changes are communicated to Corus promptly.

Organizations must refuse access to personal information:

- If it would reveal personal information about another individual* unless there is consent or a life threatening situation
- If the organization has disclosed information to a government institution for law enforcement or national security reasons. Upon request, the government institution may instruct the organization to refuse access or not to reveal that the information has been released. The organization must refuse the request and notify the Privacy Commissioner of Canada. The organization cannot inform the individual of the disclosure to the government institution, or that the institution was notified of the request, or that the Commissioner was notified of the refusal.

Organizations may refuse access to personal information if the information falls under one of the following:

- Solicitor-client privilege
- Confidential commercial information*
- Disclosure could harm an individual's life or security*
- It was collected without the individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law (the Privacy Commissioner of Canada must be notified)
- It was generated in the course of a formal dispute resolution process

**If these details can be removed from any requested documentation, Corus must then release the remaining information in the document.*

As e-mails and voicemails stored on Corus equipment are intended for the purpose of work related activity only, they are not considered private. See the Information Technology section on Corus Central for more information about company e-mails and voicemails.

No employees or managers shall disclose or release any personal employee information (including private phone numbers, addresses, salary information, etc.) to any individual, outside source or body unless required by law or as directed through written authorization of the employee or their representative.

Corus will only keep personal information for as long as necessary for the purpose collected. When personal information is no longer needed for its specified purpose or legal requirements, it will be destroyed.

All requests for employee information must be directed to the Human Resources Department.

## Practices and Procedures

All new employees are required as a condition of employment to sign this employee Privacy Policy within their first two weeks of employment with Corus. Also, all employees are asked to review and sign this policy on an annual basis. A copy of this policy can be found on **Corus Central**, under Policies & Forms at all times.

Employees or managers who are aware of or suspect a violation of the Privacy Policy are expected to contact Human Resources immediately.

**Resolving Your Concerns**

Corus has policies and procedures in place to investigate and respond to employees' concerns and questions relating to privacy.

If you have any questions or concerns about your privacy you are encouraged to contact any one of our Privacy Officers.

All concerns will be investigated and we will try to resolve them. If necessary, we will take the appropriate measures, including changing our policies and procedures to ensure that other employees will not experience the same problem. For information on our Privacy Protection Principles and a list of Corus Privacy Officers, please visit Corus Central / Policies & Forms.

If a manager or employee is uncertain as to whether personal information can be shared, contact Human Resources.

**What personal information does the company need?**

Corus requires personal information for a variety of reasons – these include but are not limited to:

1. To send private employment information, such as paycheques, T4's, benefits statements, to an employee's home.

2. To manage benefits (e.g. beneficiaries and dependents).

3. Emergency contact information.

4. Contacting employees upon exiting Corus for T4's, exit questionnaires and other communication.

5. To report employment equity statistics as required to the government of Canada and the CRTC.

6. To measure retention and attraction by a variety of demographics.

**How does Corus store personal information?**

The majority of personal information is stored with Human Resources. Most information is stored electronically – significant security has been created to protect this information. The company is required to maintain certain information in hard copy – all hard copy files are stored in locked cabinets. Corus is required to store employee information for a minimum of 7 years.

Corus is accountable for safeguarding employee personal information from loss, theft, unauthorized access, disclosure, modification or duplication.

Secure locks on filing cabinets, restricted access to offices, electronic security such as passwords, PIN numbers and encryption are methods used to safeguard employee personal information. These controls are reviewed on a regular basis to ensure security is maintained.

Each employee also has the obligation to safeguard the privacy of other employees' personal information to which he/she might have access. This remains in effect when you leave Corus. Employees are asked to treat co-workers' personal information the same way you would want your own information treated.

## Related Policies

Code of Conduct Policy