



Privacy Policy

Document Number: Privacy Policy - 001

Date Issued: January 2, 2019

Revision: 01

1. POLICY

Belchim is committed to protecting the privacy of its employees, clients/customers/suppliers and confidential business information.

- 1.01 Employees are obligated to ensure that personal information, to which they may have access remains confidential, is only used for the purposes for which it was collected, is not disclosed without authorization or used for personal gain.
- 1.02 Employees are required to follow all procedures regarding collection, use, and disclosure of personal information as set out in this policy.
- 1.03 Employees who disclose personal information, contrary to this policy will be subject to disciplinary measures, up to and including discharge for cause.
- 1.04 The Privacy Manager is accountable for the implementation of this policy. Any issues or questions regarding this policy should be directed to the Privacy Manager.

2. PURPOSE

- 2.01 All employees at one time or another may receive personal, privileged and/or confidential information which may concern other employees, company operations or clients/customers. The purpose of this policy is to preserve the privacy of employees, clients and Belchim, by outlining employee obligations and procedures for dealing with personal, privileged and/or confidential information.

3. SCOPE

- 3.01 This policy applies to all employees, contractors, subcontractors of Belchim or anyone else who is granted access to personal, privileged and/or confidential information.

4. RESPONSIBILITY

- 4.01 **Employees** are responsible for:
Keeping their own employee files current regarding name, address, phone number, dependents, etc. being familiar with and following policies and procedures regarding personal information; obtaining the proper consents and authorizations prior to disclosure of personal, privileged and/or confidential information; immediately reporting any breaches of confidentiality to their manager and/or Privacy Manager; keeping private passwords and access to personal, privileged and/or confidential data; explaining this policy to clients and referring them to the Privacy Manager if necessary; relinquishing any personal, privileged, confidential or client information in their possession before or immediately upon termination of employment.

[35]

Privacy Policy

Document Number: Privacy Policy - 001

Date Issued: January 2, 2019

Revision: 01

4.02 Managers are responsible for:

Obtaining consent to the collection and use of personal information from employees; ensuring policies and procedures regarding collection, use and disclosure of information of personal information is consistently adhered to; responding to requests for disclosure after the proper release is obtained; cooperating with the Privacy Manager (HR/Administration Manager) to investigate complaints or breaches of policy; obtaining from terminating employees prior to their termination any personal, privileged, confidential or client information in their possession. ensuring that disclosure of personal information or personal health information to a third party is done with the approval of the Privacy Manager (General Manager) in order to minimize risk of non-compliance with applicable legislative or regulatory regimes.

4.03 Human Resources and/or Administration/Payroll personnel are responsible for:

Ensuring that appropriate consents have been obtained from employees with respect to the collection and use of personal information; maintaining systems and procedures to ensure employee records are kept private; obtaining the proper consents and authorizations prior to disclosure of information contained in employee records; responding to employees' requests for access to their files; ensuring proper disposal of unnecessary files/information. maintaining separate files to ensure that personal health information is protected. ensuring that disclosure of personal information or personal health information to a third party is done with the approval of the Privacy Manager in order to minimize risk of non-compliance with applicable legislative or regulatory regimes. ensuring that reasonable steps are taken to ensure that information delivered through the mailbox system remains confidential. This can include using a sealed envelope with a signature or stamp printed across the seal.

4.04 Privacy Manager is Human Resources/Payroll Administration is responsible for:

Internal compliance with applicable policies or legislation; cooperating with managers, human resources and/or payroll personnel in developing internal policies for the collection, use and disclosure of personal information and personal health information of employees; monitoring and responding to third party requests for personal information or personal health information; ensuring appropriate consents are obtained for the collection, use and disclosure of personal information and personal health information; where collection, use or disclosure is permitted without prior consent, notifying individuals of the collection, use and disclosure of personal information and/or personal health information after such occurrence.

5. DEFINITIONS

5.01 "Personal information" is any information about an identifiable individual and includes race, ethnic origin, colour, age, marital status, family status, religion, education, medical history, criminal record, employment history, financial status, address, telephone number, and any numerical identification, such as Social Insurance Number. Personal information also includes information that may relate to the work performance of the individual, any allegations, investigations or findings of wrongdoing, misconduct or discipline. Personal information does not include job title, business contact information or job description.

Privacy Policy

Document Number: Privacy Policy - 001

Date Issued: January 2, 2019

Revision: 01

5.2 **“Personal health information”** is information about an identifiable individual that relates to the physical or mental health of the individual, the provision of health care to the individual, the individual's entitlement to payment for health care, the individual's health card number, the identity of providers of health care to the individual or the identity of substitute decision-makers on behalf of the individual.

5.3 **“Third parties”** are individuals or organizations other than the subject of the records or representatives of Belchim. Note that in certain circumstances, the company may be entitled to provide personal information to an external party acting as an agent of Belchim.

6. REFERENCES AND RELATED STATEMENTS OF POLICY AND PROCEDURE

6.1 Personal Information Protection and Electronic Documents Act (PIPEDA)

7. PROCEDURE

7.01 Employee Records

- a) An employee's immediate manager, higher level managers, human resources and payroll personnel shall have access to employee records containing personal information. Higher level managers, human resources and payroll personnel will have access to an employee's personal health information if the Privacy Manager determines that such access is permissible and necessary. Personal information and personal health information will not be disclosed outside of the organization without the knowledge and/or approval of the employee. Notwithstanding the foregoing, Belchim will cooperate with law enforcement agencies and will comply with any court order or law requiring disclosure of personal information without the employee's consent.
- b) Employees may request access to review their own file by making arrangements with the Human Resources department. Employees shall provide at least seventy-two (72) hours notice to the Human Resources department. Employees may obtain a copy of any document in their file which they have signed previously. No material contained in an employee file may be removed from the file. A representative of the Human Resources department will be present during viewing of the file.
- c) An employee may provide a written notice of correction related to any data contained in the employee's file. The notice of correction shall be provided to the Human Resources department.
- d) Employee requests for disclosure of their own personal information to third parties must be accompanied by a completed, signed and dated Authorization to Release Information form. This form should also be used in dealings with insurance companies with respect to employee benefits and to provide confirmation of earnings to financial institutions for lending purposes.

[37]

Privacy Policy

Document Number: Privacy Policy - 001

Date Issued: January 2, 2019

Revision: 01

- e) Unless retention of personal information is specified by law for certain time periods, personal information that is no longer required to fulfil the identified purpose shall be destroyed, erased or made anonymous within twelve (12) months after its use.
- f) Managers may have a need to maintain certain records, related to employees, near their own work station as opposed to the Employee File. This information may include, work schedules, absence requests, attendance records and notes related to performance. Managers should not maintain employees' personal information outside the Employee File and any information kept at a workstation, should be kept securely locked.

7.02 Client/Supplier Information

- (a) Personal, privileged and/or confidential information about customers and clients may only be collected, used, disclosed and retained for the purposes identified by Belchim as necessary.
- (b) Employees must ensure that no personal, privileged and/or confidential client information is disclosed without the client's consent and then only if security procedures are satisfied.
- (c) Client information is only to be accessed by employees with appropriate authorization.
- (d) Unless retention of personal information is specified by law for certain time periods, personal information that is no longer required to fulfil the identified purpose shall be destroyed, erased or made anonymous within twelve (12) months after its use.

7.03 Notwithstanding Paragraphs 7.01(e) and 7.02(d) personal information that is the subject of a request by an individual or a Privacy Commission shall be retained as long as necessary to allow individuals to exhaust any recourse they may have under PIPEDA.

7.04 Concerns or complaints related to privacy issues must be made, in writing, to the Privacy Manager setting out the details of the concern or complaint. The Privacy Manager shall investigate the matter forthwith and make a determination related the resolution of the concern(s) or complaint(s).

7.05 No employee shall be disadvantaged or denied any benefit of employment by reason that Belchim believes that an employee will do anything referred to paragraphs (a), (b), or (c) below or by reason that an employee, acting in good faith and on the basis of reasonable belief;

- (a) has disclosed to the Privacy Commissioner of Canada that Belchim or any other person has contravened or intends to contravene a provision of PIPEDA related to the protection of personal information;
- (b) has refused or stated the intention of refusing to do anything that it is in contravention of a provision of PIPEDA related to the protection of personal information;
- (c) has done or stated an intention of doing anything that is required to be done in order that a provision of PIPEDA related to the protection of personal information not be contravened.

[38]



Privacy Policy

Document Number: Privacy Policy - 001

Date Issued: January 2, 2019

Revision: 01

7.06 An employee who is found to be in breach of this policy will be subject to discipline up to and including termination for cause.

8. ATTACHMENTS

Privacy Concern Resolution Form