Chellsey Institute of Beauty & Health Inc. Data Protection Policy

Contents

CHELLSEY INSTITUTE OF BEAUTY & HEALTH INC.

Data Protection Policy

Scope of this policy

1. Introduction

1.1 This policy concerns the obligations of the Chellsey Institute of Beauty & Health Inc. (the **school**) under the Canadian Privacy Act (R.S.C., 1985, c. P-21) (the **Act**). The Act covers issues such as data security, an individual's rights to access information about themselves and the use and disclosure of personal information.

1.2 Staff should read this policy alongside the Information Security Policy. Information security is especially important, and the policy sets out the steps which staff must take to help ensure that personal information is not lost, misplaced, or accidently disclosed to third parties. **Please make sure that you have read and understood the Information Security Policy in addition to this policy.**

2. **Application**

2.1 This policy is aimed at all staff including temporary staff, agency workers, volunteers and all other people when working in or for the school (whether directly or indirectly). It also applies to Governors. It explains the general approach of the school to data protection and provides practical guidance which will help to ensure that the school complies with the Act.

2.2 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.3 We reserve the right to change this policy at any time. Where appropriate, we will notify staff of those changes by mail or email.

3. **Responsibility**

3.1 Compliance with this policy will help the school to meet its obligations under the Act but this policy does not commit the school to a higher standard than is required by the Act. In some circumstances, e.g., situations involving safeguarding concerns, strict compliance with the Act will be subsidiary to other considerations.

3.2 The person with overall responsibility for compliance with the Act is Owner/Director/ Manager (Business Operations) (the **Data Protection Officer or DPO**). All queries concerning data protection matters should be raised with the Data Protection Officer.

3.3 All staff are responsible for complying with this policy. Any questions or concerns about the operation of this policy should be referred to the DPO.

4. **Links to other policies**

4.1 This policy is intended to give an overview of the Act and staff obligations. This policy should be read alongside the following:

4.1.1. Information, communication and technology (ICT) Acceptable Use Policy for Staff.
4.1.2. Information security policy (including remote working and bring your own device to work); and
4.1.3. Record Keeping Policy.
4.1.4. Privacy Notice for students

5. What information falls within the Act

5.1. The Act applies to personal information about individuals (called **Personal Data** in the Act).

5.2. Personal Data is:

5.2.1. personal information that has been, or will be, word processed or stored electronically (e.g., in computer databases and CCTV recordings). If a record containing Personal Data is held on a computer, then it will be covered by the Act. This is the case regardless of how the information is held. For example, Personal Data stored in an email, in a spreadsheet or on a smartphone, are all caught by the Act.

5.2.2. personal information that is, or will be, kept in a file which relates to an individual or in a filing system that is organized by reference to criteria which relate to the individuals concerned (e.g., name, department, pay scale etc.). Some paper records are not covered by the Act although there are so many exceptions that best practice is to treat all paper records as being covered; and

5.2.3. some health records prepared by a doctor, nurse, or other health professional (even if not held on computer or held as part of an organized file).

5.3. Virtually any information about someone is likely to be Personal Data. All of the following examples are likely to contain Personal Data and are therefore subject to the Act:

5.3.1. information about a student protection incident.

5.3.2. a record about disciplinary action taken against a member of staff.

5.3.3. photographs of students.

5.3.4. a tape recording of a job interview.

5.3.5. contact details and other personal information held about students and staff and their families.

5.3.6. contact details of a member of the public who is enquiring about placing their student at the school.

5.3.7. financial records of a student; and

5.3.8. information on a student's performance.

6. Summary of the obligations under the Act

6.1. The main obligations under the Act relevant to staff are as follows:

6.1.1. compliance with the eight data protection principles: the Act contains eight principles which set out how organizations should handle Personal Data. These cover issues such as fairness, transparency, keeping information up-to-date and security. Please see the schedule to this policy which summarizes the principles and gives examples.

6.1.2. subject access requests: the Act gives individuals a number of rights including a right to request a copy of the Personal Data the School holds about them. Please see section 14 below.

6.1.3. sensitive personal data: there are extra obligations in relation to Sensitive Personal Data. Sensitive Personal Data is information about an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life and information relating to actual or alleged criminal activity; and

6.1.4. informing the individual: the school must ensure that individuals are told how their Personal Data will be used (unless it is obvious). Please see section 9 below.

6.2. What these obligations mean in practice is explained below.

7. Processing Personal Data

7.1. The Act applies to the "processing" of Personal Data, which covers virtually everything which is done in relation to that Personal Data including using disclosing, copying, and storing Personal Data. This means that the school will be caught by the Act just by storing the Personal Data.

7.2. The school shall only process Personal Data for specific and legitimate purposes. These are:

- 7.2.1. ensuring that the school provides a safe and secure environment.
- 7.2.2. providing pastoral care.
- 7.2.3. providing education and learning for our students.
- 7.2.4. providing additional activities for students.
- 7.2.5. protecting and promoting the school's interests and objectives - this includes fundraising.
- 7.2.6. safeguarding and promoting the welfare of our students; and
- 7.2.7. to fulfil the school's contractual and other legal obligations.

7.3. Staff must not process Personal Data for any purpose other than those listed above without the DPO's permission.

8. Use of Personal Data

8.1. Staff should seek advice from the DPO before using Personal Data for a purpose which is different from that for which it was originally acquired. If information has been obtained in confidence for one purpose, it must not be used for any other purpose without authorization from the DPO.

8.2. Personal Data must be processed in a way that is fair to individuals. Compliance with this policy is likely to mean that the processing is fair in most cases. However, the concept of fairness can be quite difficult to define, and staff should inform the DPO if they are concerned that any processing of Personal Data appears to be unfair to any individual in any way even if the processing appears to comply with the letter of this policy.

8.3. Staff should only keep Personal Data for as long as is reasonably necessary, and in accordance with the School's Record Keeping Policy, but staff should not delete records containing Personal Data without authorization. Staff should consult with the DPO for guidance about how long to retain different categories of Personal Data.

8.4. Staff should ensure that Personal Data is complete and kept up to date by notifying the relevant owner of the data. For example, if a student notifies a member of staff that their contact details have changed, the member of staff should inform the relevant Head's PA so that the school's records can be updated.

8.5. The school and staff must ensure that any Personal Data is sufficient. For example, a teacher writing a report about a student should ensure that he/she has all the student's relevant records to hand.

8.6. Personal Data must not be processed in a way that is excessive or unnecessary. For example, should 8 students out of a possible 20 attend a lunch event, the member of staff should only take records (such as information about allergies and emergency contact details) of those 8 students.

9. Informing the individual

9.1. Individuals must be told what data is collected, and what it is used for, unless it is obvious. This is sometimes called a privacy notice or statement (sometimes also called a fair processing notice or statement).
9.2. The privacy notice must explain what information will be collected, what it will be used for, which third parties (if any) it will be shared with and anything else which might be relevant.
9.3. Staff are not expected to routinely provide students, and others with a privacy notice as this should have already been provided. Copies of the School's privacy notice can be obtained from the DPO or accessed on the school's website.
9.4. Having said this, staff should inform the DPO if they suspect that the school is using Personal Data in a way which might not be covered by an existing privacy notice. This may be the case where, for example, staff are aware that the school is collecting medical information about students without telling the students (if age appropriate) and/or their emergency contact what that information will be used for.

10. Accessing, disclosing, and sharing Personal Data

10.1. The general position is that Personal Data should only be shared on a "need to know" basis. Before sharing Personal Data outside of the school, staff should:
10.1.1. make sure they are allowed to share it.
10.1.2. ensure adequate security (please see section 11 below and the Information Security Policy); and
10.1.3. make sure that the sharing is covered in the school privacy notice (please see section 9).

11. Sharing Personal Data within the School

11.1. This section applies when Personal Data is shared within the school. It also applies when Personal Data is shared between the campuses in the Chellsey Institute of Beauty & Health Inc.
11.2. Personal Data must only be shared within the school on a "need to know" basis although this will not prevent sharing Personal Data where doing so is reasonable and proportionate and is done in accordance with this policy. Staff should think about whether the person(s) they wish to share the Personal Data with needs access to the information.
11.3. Examples of sharing which are likely to comply with the Act:
11.3.1. a teacher discussing a student's academic progress with other members of staff (for example, for advice on how best to support the student.
11.3.2. informing an exam invigilator that a particular student suffers from panic attacks; and
11.3.3. disclosing details of an assistant's allergy to bee stings to colleagues so that they will know how to respond (but more private health matters must be kept confidential).
11.4. Examples of sharing which are unlikely to comply with the Act:
11.4.1. the Head being given access to all records kept by nurses working within the school (seniority does not necessarily mean a right of access);
11.4.2. informing all staff that a student has been diagnosed with dyslexia (rather than just those who teach the student); and
11.4.3. disclosing personal contact details for a member of staff without their prior consent (e.g., their home address and telephone number) to other members of staff (unless the member of staff has given permission or unless it is an emergency).
11.5. The Act does not prevent the sharing or disclosure of Personal Data where failing to do so could cause serious harm (for example, in relation to student protection and safeguarding matters).

12. **Sharing Personal Data with individuals and organizations outside of the school (for example, with other schools, social services, the Police, and contractors)**

12.1. Sharing Personal Data with others is often permissible so long as doing so is fair and lawful under the Act but staff should always speak to the DPO if in doubt, or if staff are being asked to share Personal Data in a new way.
12.2. Before sharing Personal Data outside of the school, staff should:
12.2.1. make sure that they are allowed to share it.
12.2.2. ensure adequate security (please see section 13 below). What is adequate will depend on the nature of the data. For example, if the school is sending a student protection report to social services on a memory stick, then the memory stick must be encrypted; and
12.2.3. make sure that the sharing is covered in the privacy notice (please see section 9).
12.3. Please see the Information Security Policy for guidance on when encryption should be used before sending information by email.
12.4. Staff should not disclose Personal Data to the Police without permission from the DPO (unless it is an emergency).
12.5. Staff must not disclose Personal Data to contractors without permission from the DPO. This includes, for example, sharing Personal Data with an IT contractor (e.g., where the contractor is to carry out a data cleansing exercise).
12.6. Training is provided to staff on the publishing of information containing Personal Data, such as photographs on the school's website or on Twitter with names. If in doubt permission should be sought from the Director External Relations before publishing anything containing Personal Data (for example, uploading photographs of a trip organized by the School to the School's website).
12.7. Staff should be aware of "bagging". This is the use of deceit to obtain personal data from people or organizations. Staff should seek advice from the DPO where staff are suspicious as to why the information is being requested or if they are unsure of the identity of the requester.

13. **Information security**

13.1. Information security is the most important aspect of data protection compliance. Most of the fines under the Act relate to security breaches such as:
13.1.1. leaving an unencrypted memory stick in a public place.
13.1.2. sending sensitive documents to the wrong fax recipient.
13.1.3. disposing of confidential documents without shredding them first; or
13.1.4. accidentally uploading confidential information to the web.
13.2. The Act requires the school to take organizational measures (for example, ensuring that staff are trained on information security), and technical measures (for example, encryption and secure shredding etc) to ensure that Personal Data is kept secure. These requirements are explained in more detail below and should be read in conjunction with the Information Security Policy (including remote working and bring your own device to work).

14. <u>Requests for information (Subject Access Requests)</u>

14.1. Individuals are entitled to know whether the School is holding any Personal Data which relates to them, what that information is, the source of the information, how the School uses it, and who it has been disclosed to. The individual is also entitled to request a copy of the Personal Data which the School holds about them. This is known as a **Subject Access Request**.

14.2. Any member of staff who receives a request for information covered by this policy from a member of staff, students or any other individual must inform the DPO as soon as is reasonably possible, which should in most cases be the same day. This is important as there is a statutory procedure and timetable which the school must follow. Staff must never respond to a Subject Access Request themselves unless authorized to do so.

14.3. Staff should be aware that there is no obligation to refer to the "Data Protection Act" or use the phrase "Subject Access Request" when making a request. By way of an example, an email which simply states "Please send me copies of all emails you hold about me" is a valid Subject Access Request.

14.4. Subject to a number of limited exceptions, all information about an individual may be disclosed should a Subject Access Request be made. There is no exemption for "embarrassing" information. For example, an exchange of emails containing gossip about an individual will usually be disclosable. **As such staff should be aware that anything they put in an email is potentially disclosable.**

15. Other rights

15.1. Individuals have a number of rights under the Act in addition to the right to make a Subject Access Request. This includes a right to:

15.1.1. prevent the use of their data for marketing.

15.1.2. ask to have inaccurate data amended;

15.1.3. prevent the use of data in a way that is likely to cause unwarranted substantial damage or unwarranted substantial distress to themselves or anyone else; and

15.1.4. object to any significant decision which is taken solely by a computer or other automated process. For example, basing salary increases solely on a pre-determined formula without giving the employee an opportunity to object or make representations.

15.2. Any members of staff who receive a request which relates to any of the above must promptly forward it to the DPO.

16. Further information

16.1. If staff have any questions about this policy or about data protection they should speak to the DPO.

16.2. Similarly, all staff have an obligation to assist the School and colleagues to comply with the Act. Therefore staff should also report any concerns, or any evidence of non-compliance, to the DPO.

16.3. We have registered our use of Personal Data with the Information Commissioner's Office and further details of the Personal Data we hold, and how it is used, can be found in our register entry on the Information Commissioner's website at www.ico.gov.uk under registration number ZA080432. This website also contains further information about data protection.

17. Breach of this policy

17.1. Any breach of this policy will be taken seriously and may result in disciplinary action.

17.2. A member of staff who deliberately or recklessly discloses Personal Data held by the School without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

The eight data protection principles	Comment and examples
1. Processed fairly and lawfully	This means being fair, clear, and transparent about how Personal Data is used. For example, letting people know how their Personal Data will be used and who it will be shared with.
2. Processed for limited purposes and in an appropriate way	If students are told that they will be photographed to enable staff to recognize them when writing references, it would be a breach to use that photograph for another purpose (e.g. in the School's prospectus).
3. Adequate, relevant, and not excessive for the purpose	"Adequate and relevant" means not making decisions based on incomplete data, for example, disciplining a student without getting the student's side of the story. This also covers collecting unnecessary data. For example, the School should only collect information about student hobbies if that has some relevance (e.g. if relevant to PE lessons).
4. Accurate	For example, ensuring that emergency contact person details are kept up-to-date by asking students to confirm their contact details once every year.
5. Not kept longer than necessary for the purpose	Avoid keeping Personal Data on the off-chance it might be needed for some unknown purpose in future. Specific retention periods can be found in the School's Record Keeping Policy.
6. Processed in line with the data subjects' rights	Please see sections 14 and 0 above.
7. Secure	This is the most important principle. Please see section 13 above.