PERSONAL INFORMATION PROTECTION POLICY

1. Purpose and Scope

Multihexa College (the "College") is committed to protecting the privacy of personal information of its students, prospective students, employees, contractors, and other individuals. This policy sets out how the College collects, uses, discloses, retains, and protects personal information in accordance with British Columbia's Personal Information Protection Act, S.B.C. 2003, c. 63 ("PIPA"). PIPA sets out the rules for how private sector organizations in British Columbia collect, use, and disclose personal information.

Where the College engages in interprovincial or international commercial activities, it may also be subject to the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 ("PIPEDA"). In such cases, the College will comply with both statutes.

This policy applies to all personal information collected, used, or disclosed by the College in the course of its commercial and educational activities, including the administration of student enrolment, academic records, student services, employment, and institutional operations.

This policy applies to all employees, faculty, staff, administrators, contractors, agents, and volunteers of the College who handle personal information on the College's behalf.

The College is accountable for how it handles personal information and for following the rules and procedures set out in this policy.

2. Definitions

"Personal Information" means information about an identifiable individual, as defined under PIPA. This includes, but is not limited to: name, address, telephone number, email address, date of birth, student number, Social Insurance Number, academic records, financial information, immigration documents, photographs, and employment records. Personal information does not include contact information used to reach an individual in a business capacity (business name, title, business address, business telephone number, or business email address), or work product information prepared or collected by an employee as part of their work responsibilities.

"Employee Personal Information" means personal information about an individual that is collected, used, or disclosed solely for the purposes reasonably required to establish, manage, or terminate an employment or volunteer relationship between the College and the individual. This includes, but is not limited to, personnel records, job applications, references, performance evaluations, payroll records, and letters of resignation or termination.

"Consent" means voluntary agreement to the collection, use, or disclosure of personal information for a specified purpose. Consent may be express, implied, or opt-out, depending on the sensitivity of the information and the reasonable expectations of the individual.

"Privacy Officer" means the individual designated by the College as responsible for

overseeing compliance with this policy and with PIPA.

"Privacy Breach" means any unauthorized access to, collection, use, disclosure, or disposal of personal information in contravention of PIPA.

3. Accountability

The College is responsible for all personal information under its control, including personal information transferred to third parties for processing on the College's behalf.

The College has designated a Privacy Officer who is responsible for:

- overseeing the College's compliance with this policy and with PIPA;
- receiving and responding to privacy inquiries, access requests, and complaints;
- ensuring that all employees, faculty, and contractors who handle personal information are appropriately trained on their privacy obligations;
- reviewing and updating this policy as required.

The Privacy Officer's contact information is set out in Section 18 of this policy and is available to any individual upon request.

4. Identifying Purposes and Limiting Collection

The College will identify the purposes for which personal information is collected at or before the time of collection. The College will collect only the personal information that is necessary to fulfill the identified purposes. Personal information will be collected by fair and lawful means. The College will not collect personal information indiscriminately and will not mislead or deceive individuals about the purposes for which information is being collected.

The College collects personal information for the following purposes, as applicable:

- processing applications for admission and enrolment;
- administering student records, academic programs, grades, and credentials;
- processing tuition, fees, and financial aid;
- meeting regulatory reporting obligations to the Private Training Institutions Regulatory Unit (PTIRU), StudentAid BC, Immigration, Refugees and Citizenship Canada (IRCC), and other governmental and regulatory bodies;
- administering study permits, letters of acceptance, and compliance reporting under the International Student Program;
- providing student services including academic advising, career services, and support referrals;
- managing employment, payroll, benefits, and human resources functions;
- maintaining institutional safety and security;
- communicating with students, alumni, and the College community;
- complying with applicable laws and regulations.

If the College identifies a new purpose for which it wishes to use personal information

already collected, it will obtain the individual's consent before using the information for that new purpose, unless the new use is permitted or required by law.

5. Consent

The College will obtain the informed consent of the individual for the collection, use, or disclosure of personal information, except where PIPA permits or requires collection, use, or disclosure without consent. The College will not require an individual to consent to the collection, use, or disclosure of personal information beyond what is necessary to provide a product or service.

Consent may take the following forms:

- Express consent: obtained through a clear, affirmative act such as signing a consent form or providing written or oral agreement.
- Implied consent: reasonably inferred from the individual's actions or inaction where the purpose of collection, use, or disclosure would be obvious to a reasonable person.
- Opt-out consent: where the individual is notified of the intended use and is given a clear opportunity to decline, and does not do so.

The type of consent required will depend on the sensitivity of the personal information and what a reasonable person would consider appropriate in the circumstances.

Withdrawal of Consent: An individual may withdraw consent at any time by providing written notice to the Privacy Officer. The College will inform the individual of the likely consequences of withdrawing consent (such as the College being unable to provide certain services that require the personal information). Withdrawal of consent does not have retroactive effect.

Employee Personal Information: In the case of employee personal information, PIPA permits the College to collect, use, or disclose employee personal information without consent if it is reasonable for the purposes of establishing, managing, or terminating an employment or volunteer relationship. However, the College will notify employees in advance of the collection, use, or disclosure, and the purposes for it, before collecting employee personal information without consent.

The College may also collect, use, or disclose personal information without consent where permitted or required by PIPA, including but not limited to:

- where necessary to comply with a subpoena, warrant, court order, or other legal requirement;
- where necessary to respond to an emergency that threatens an individual's life, health, or security;
- where the information is publicly available as defined by PIPA;
- where necessary for a legal proceeding or to collect a debt owed to the College;
- where disclosure is to a regulatory body (such as PTIRU or IRCC) as required or authorized by law.

6. Limiting Use and Disclosure

Personal information will be used or disclosed only for the purposes for which it was collected, unless the individual consents to another use, or the use or disclosure is permitted or required by law.

The College may disclose personal information without consent to third-party service providers who perform services on the College's behalf (such as IT service providers, payment processors, or student information system vendors), provided that the College ensures by contractual or other means that the service provider protects the personal information to a standard consistent with this policy and PIPA.

The College may disclose personal information to regulatory bodies including PTIRU, StudentAid BC, IRCC, and provincial or federal governmental bodies where required or authorized by law.

The College may also disclose personal information where authorized by PIPA or required by law, including in the event of a court order, subpoena, or search warrant.

Where any other circumstances arise in which the College discloses personal information, those circumstances will be identified and communicated to the individual.

6A. Students Funded Through StudentAid BC

Where a student applies for or receives funding through StudentAid BC, the College will disclose to StudentAid BC and, where applicable, the National Student Loans Service Centre, the information required to administer that funding. This includes the student's enrolment status, program and course load, program start and end dates, attendance or academic progress, withdrawal or dismissal and its effective date, tuition and fees charged, and any refund issued. Students are notified of this disclosure, and their consent is recorded in the Student Declaration of the Enrolment Contract.

6B. Online Learning and Monitoring

For programs and courses delivered by distance education, the College collects learning management system (LMS) activity data, including log-ins, time on task, submissions and assessment results. This data is used to track academic progress, attendance and completion, and to meet reporting obligations to PTIRU and StudentAid BC. Where live online sessions are held, students will be informed in advance if a session is to be recorded and of the purpose of the recording. Camera use during live sessions is for participation purposes only. Recordings, where made, will be retained and destroyed in accordance with Section 7.

7. Retention

Personal information will be retained only as long as necessary to fulfill the purposes

for which it was collected, or as required by law or regulatory obligation.

Minimum Retention: Where personal information has been used to make a decision that directly affects an individual (such as an admissions decision, a grading decision, a disciplinary decision, or an employment decision), the College will retain that personal information for at least one (1) year after the decision is made, as required by PIPA.

Student records for approved programs will be retained for at least eight (8) years for Class A programs, and at least three (3) years for Class B and Class C programs, after the date the student completes the program, the College receives a notice of withdrawal, or the College provides a notice of dismissal, in accordance with section 38 of the Private Training Regulation. Records kept electronically will be backed up at least monthly, stored securely in a non-proprietary format that can be copied, and made accessible to the Registrar on request. For Class A programs, the College will submit each archived student record (the signed enrolment contract, the transcript and any credential granted) to the Registrar within sixty (60) days after the end date of the enrolment contract, the receipt of a notice of withdrawal, or the provision of a notice of dismissal, in accordance with section 39 of the Regulation.

8. Accuracy

The College will take reasonable steps to ensure that personal information is accurate, complete, and up-to-date as is necessary for the purposes for which it is used, particularly where the personal information is likely to be used to make a decision that directly affects an individual or is to be disclosed to another organization.

Students, employees, and other individuals are encouraged to notify the College promptly of any changes to their personal information.

Corrections: An individual may request that the College correct any errors or omissions in their personal information that is under the College's control. If the College is satisfied that the request for correction is reasonable, the College will correct the information and send the corrected information to any organization to which the personal information was disclosed during the year before the date the correction was made.

If the College is not satisfied that the request for correction is reasonable, it will annotate the personal information, noting that the correction was requested but not made. The individual will be informed in writing of the College's decision and their right to request a review by the OIPC.

9. Safeguards

The College will protect personal information with security safeguards appropriate to the sensitivity of the information, to protect against unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks.

Security safeguards include:

- Physical safeguards: locked filing cabinets, restricted access to offices and server rooms, secure disposal of paper records.

- Technological safeguards: password-protected systems, encryption of sensitive data in transit and at rest, firewalls, access controls and role-based permissions, secure backup systems.
- Administrative safeguards: staff training on privacy obligations, confidentiality agreements for employees and contractors, limiting access to personal information on a need-to-know basis, regular audits of privacy and security practices.

The College will promptly investigate any suspected privacy breach and take appropriate remedial steps, in accordance with Section 14 of this policy.

10. Openness

The College will make information about its privacy policies and practices readily available to individuals. This includes:

- making this policy available on the College's website and upon request;
- providing the Privacy Officer's name or title and contact information upon request;
- providing a description of the types of personal information held by the College and the general purposes for which it is used;
- explaining how to make an access or correction request, or how to file a complaint.

11. Individual Access and Correction

Upon written request, an individual has the right to:

- be informed of the existence of personal information about them held by the College;
- access their personal information;
- be informed of the ways in which their personal information has been or is being used;
- be informed of the names of individuals and organizations to whom their personal information has been disclosed.

These rights are subject to the exceptions set out in PIPA.

Making a Request: An individual may request access to their personal information by submitting a written request to the Privacy Officer. The individual may be required to verify their identity before the College provides access to their personal information.

Response Timeline: The College will respond to the access request within thirty (30) business days of receiving the request, as required by PIPA. The College may extend this period by an additional thirty (30) business days where reasonably necessary, with written notice to the individual explaining the reason for the extension.

Fees: The College may charge a minimal fee for providing an individual with access to their personal information. If a fee is required, the College will provide the individual

with a written estimate in advance. The College may require payment of a deposit or the full fee before releasing the requested information.

The College may refuse an access or correction request in the circumstances set out in PIPA, including where:

- disclosure would reveal personal information about another individual;
- the information is protected by solicitor-client privilege;
- disclosure could reasonably be expected to threaten the safety or mental or physical health of another individual;
- the information was collected for an investigation or legal proceeding.

If the College refuses an access or correction request, it will provide the individual with written reasons and inform them of their right to request a review by the Office of the Information and Privacy Commissioner for British Columbia ("OIPC").

12. Complaints and Challenging Compliance

An individual who believes that the College has not complied with this policy or with PIPA may submit a complaint in writing or by contacting the Privacy Officer.

An individual may be required to verify their identity before the College discusses any complaint or request involving their personal information.

The Privacy Officer will:

- acknowledge receipt of the complaint within five (5) business days;
- investigate the complaint in a fair and thorough manner;
- provide the individual with a written response within thirty (30) business days, setting out the findings and any steps taken or to be taken to address the complaint.

If the individual is not satisfied with the College's response, they have the right to file a complaint with the Office of the Information and Privacy Commissioner for British Columbia (OIPC). Contact information for the OIPC is set out in Section 18 of this policy.

13. Employee and Contractor Obligations

All employees, faculty, contractors, and agents of the College who have access to personal information are required to:

- comply with this policy and with PIPA;
- collect, use, and disclose personal information only for authorized purposes and only to the extent necessary;
- safeguard personal information against unauthorized access, disclosure, or loss;
- report any suspected or actual privacy breach immediately to the Privacy Officer;
- complete privacy training as required by the College.

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

14. Privacy Breach Response

A privacy breach occurs when there is unauthorized access to, collection, use, disclosure, or disposal of personal information. The College will respond to all suspected or actual privacy breaches promptly and in accordance with this policy and applicable law.

In the event of a suspected or actual privacy breach, the College will:

- immediately contain the breach, to the extent possible, to prevent further unauthorized access or disclosure;
- notify the Privacy Officer, who will lead the breach investigation and response;
- conduct an assessment of the breach, including the cause, the scope of personal information involved, the number of affected individuals, and the risk of harm;
- where the breach creates a real risk of significant harm to affected individuals, notify those individuals as soon as practicable, providing: a description of the breach, the types of personal information involved, steps the College has taken to mitigate the harm, and recommended steps the individual can take to protect themselves;
- where appropriate, voluntarily report the breach to the OIPC (note: breach reporting to the OIPC is currently voluntary under PIPA for private organizations, but is strongly recommended by the OIPC and may become mandatory under future legislative amendments);
- where the College has obligations under PIPEDA (e.g., for interprovincial or international commercial activities), report any breach that creates a real risk of significant harm to the Office of the Privacy Commissioner of Canada, as required by PIPEDA;
- document all breaches in a breach log, regardless of whether they trigger notification obligations, including the facts of the breach, the assessment, and any remedial actions taken;
- take steps to prevent similar breaches from occurring in the future, including reviewing and updating safeguards, policies, and training as appropriate.

15. Cross-Border Transfers of Personal Information

Where the College transfers personal information to a service provider or other organization located outside British Columbia or outside Canada, the College will ensure by contractual or other means that the personal information receives a comparable level of protection.

The College may transfer personal information outside of British Columbia or Canada in the following circumstances:

- to comply with reporting obligations to federal bodies such as IRCC;
- where a student or applicant is located outside British Columbia or Canada and has consented to the transfer;
- where a third-party service provider (such as a cloud-based student information system) stores data outside British Columbia, subject to contractual protections;
- where required or authorized by law.

The College will inform individuals, upon request, of the jurisdictions in which their personal information may be stored or accessed.

16. Business Transactions

PIPA recognizes that personal information may need to be disclosed in the course of a prospective or completed business transaction such as a merger, acquisition, or sale of assets. In such circumstances, the College will:

- limit disclosure to information that is necessary for the purpose of the transaction;
- require the receiving party to agree to use and disclose the personal information solely for the purpose of the transaction;
- require the receiving party to protect the personal information with safeguards consistent with PIPA;
- if the transaction is completed, notify individuals that their personal information has been transferred and identify the receiving organization;
- if the transaction does not proceed, require the receiving party to return or destroy the personal information.

17. Related Legislation and Institutional Policies

Legislation:

- Personal Information Protection Act, S.B.C. 2003, c. 63 (PIPA)
- Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (PIPEDA)
- Immigration and Refugee Protection Act, S.C. 2001, c. 27
- Private Training Act, S.B.C. 2015, c. 5

Multihexa College Policies:

- Sexual Misconduct Policy
- Respectful and Fair Treatment of Students Policy
- Dispute Resolution Policy
- Student Dismissal Policy
- Information Technology Acceptable Use Policy

18. Contact Information

Privacy Officer — Multihexa College

Name	Swati Yadav
Title	Campus Manager
Email	swati.yadav@multihexa.ca
Phone	604-677-3866
Address	305-333, Terminal Avenue, Vancouver, BC V6A 4C1

Office of the Information and Privacy Commissioner for British Columbia (OIPC)

Phone	250-387-5629
Toll-Free	1-800-663-7867
Website	www.oipc.bc.ca
Address	PO Box 9038, Stn Prov Govt, Victoria, BC V8W 9A4

19. Review

This policy will be reviewed at least once every three (3) years, or sooner if required by changes to PIPA, PIPEDA, or other applicable legislation. The Privacy Officer is responsible for initiating the review and recommending amendments to the Director.

20. Non-Compliance

Non-compliance with PIPA can result in fines of up to $10,000 for individuals and $100,000 for organizations. The College takes its obligations under PIPA seriously and expects full compliance from all employees, faculty, contractors, and agents.