

Privacy Impact Assessment – FlyWire

April 2023

PART 1: GENERAL INFORMATION

PIA file number: PIA_2022-23_FlyWire

Initiative title:	FlyWire https://www.flywire.com/
Organization:	FlyWire Payments Corp.
Branch or unit:	FlyWire Canada Inc.
Your name and title:	Dale Burgos, Executive Director – Communications, Privacy
Your work phone:	250-741-5273
Your email:	DirectorCommunications@sd68.bc.ca
Initiative Lead name and title:	Rob Hutchins District Principal of International Student Education
Initiative Lead phone:	250-751-0197
Initiative Lead email:	Rob.Hutchins@sd68.bc.ca
Privacy Officer:	Dale Burgos
Privacy Officer phone:	See above
Privacy Officer email:	See above

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Related PIAs, if any:
N/A

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

Nanaimo Ladysmith Public Schools' International Student Education Program intends to use FlyWire for the purpose of global wire transferring of funds from the student's family and/or agent to the district. Another more popular provider was used in the past but was challenging to use.

Flywire's global payment network makes the payment process seamless for businesses, organizations, and payers worldwide. The company has established a robust payment infrastructure based on their network of payment partners. Through these global, regional, and local banking relationships, Flywire offers convenient payment options and securely processes transactions from over 240 countries and territories, in more than 140 currencies. Payment



partners include Mastercard, Visa, Venmo, PayPal, American Express and many more.

<https://www.flywire.com/platform/global-payment-network>

Flywire allows users of the Platform to pay bills they receive from businesses, from educational institutions, and from hospitals and associated healthcare facilities, for which they serve as payment agents (each payment recipient, a "Designated Entity"). They may work with local banks, locally licensed payment entities, foreign exchange providers, credit card processors, credit card schemes (such as Visa and MasterCard), and other third-party service providers (each, a "Service Provider") to receive and/or settle payments to a Designated Entity's bank account.

To access certain Platform features, users may be required to register for a user account. When registering for a user account, users may be required to provide the company with some information, such as your email address or other contact information. Users agree to provide us only with accurate information, and they agree to keep such information accurate and up-to-date at all times. If users register, they will be asked to provide a password. They are solely responsible for maintaining the confidentiality of their user account and password, and they accept responsibility for all activities that occur under your access credentials. Users agree to keep their access credentials confidential and secure.

VENDOR:

Flywire Payments Corporation 141 Tremont Street, 10th Floor
Boston, Massachusetts 02111 U.S.A. support@flywire.com.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

This PIA addresses the use of Flywire by students/parents to pay Cross Border and Domestic Applications, Tuitions, etc., through the Flywire Payment Solution and have an Outgoing Payment option for paying Agent Commissions, Homestay families, Etc.

3. What are the data or information elements involved in your initiative?

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix.

Using Flywire, Students and Payer will potentially have the following information collected:

- Payer Name
- Payer Email
- Relationship to student
- Payment Information (Credit Card, Billing Address, etc)
- Student Identity Info

<https://www.flywire.com/legal/privacy-policy>

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Yes

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

4. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FOIPPA authority	Other legal authority
Step 1: Payer Goes to the NLPS Flywire Portal to process payment	NO	N/A	
Step 2: Payer indicates their banking country	Data Collection	26.d.ii	
Step 3: Payer inputs billing information	Data Collection	26.d.ii	

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FOIPPA authority	Other legal authority
Step 4: Payer inputs student information	Data Collection	26.c	
Step 5: Flywire processes payment info	Data Use	33.p	

5. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

Your information will be collected in accordance with B.C.'s Freedom of Information and Protection of Privacy Act (FIPPA) section 26(d)(ii). The personal information collected will be used solely for the purpose of processing payment. If you have any questions, please contact:

Executive Director of Communications, Privacy and Community Engagement

DirectorCommunications@sd68.bc.ca

250-741-5273

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

6. Is any personal information stored outside of Canada?

Yes

7. Does your initiative involve sensitive personal information?

Yes

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

8. Is the sensitive personal information stored by a service provider?

Yes

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
FlyWire	AWS	United States/Ireland

9. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

Data Transfer:

To facilitate global operations, FlyWire transfers and store information in the U.S and allow access to that information by employees from other countries in which Flywire operates. These countries may not have the equivalent privacy laws as those of the EU or UK. When FlyWire shares information about users within and among its corporate affiliates they make use of standard contractual data protection clauses, which have been approved by the European Commission.

FlyWire commits to cooperate with EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) and comply with the advice given by such authorities with regard to human resources data transferred from the EU and Switzerland in the context of the employment relationship.

FlyWire maintains reasonable safeguards combining administrative, technical, and physical measures to provide protection to the personal information users provide against accidental, unlawful or unauthorized destruction, loss, alteration, access, interference, modification, disclosure or misuse.

FlyWire uses data hosting service providers in the US and Ireland to host the information we collect and we use technical controls to secure that data

FlyWire uses Transport Layer Security (TLS) encryption on its website when transmitting information and use other commercially reasonable efforts to protect your information.

FlyWire continues to assess new technology for protection of information and upgrade their information security systems where appropriate.

10. Does the contract you rely on include privacy-related terms?

Yes

15. What controls are in place to prevent unauthorized access to sensitive personal information?

FlyWire makes sure that its employees know and adhere to our security policies. FlyWire requires periodic training on its security policies for all personnel, no matter their department. Personnel who work directly with customers receive extra training on emerging risks, such as identity theft.

All Flywire resources agree when joining the Company to a form of confidentiality/non-disclosure agreement or specific confidentiality undertaking in their agreements of employment. Flywire resources must understand and comply fully with these terms upon commencing work at Flywire, and keep information confidential that comes into their possession or control in connection with employment with Flywire. This includes internal Flywire information, as well as information relating to clients and third parties, and applies at any time during and after employment.

- All Data is end-to-end encrypted withing SOC 2 compliance.
- All data is secured behind a firewall.
- 3rd Party Security Audits are done regularly.
- Data can only be access remotely using secure authentication.

16. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive	Level of privacy risk (low, medium, high, considering	Risk response (this may include contractual mitigations, technical controls, and/or procedural	Is there any outstanding risk? If yes, please describe.

		personal information (low, medium, high)	the impact and likelihood)	and policy barriers)	
Billing Information Leak	High - Financial	Low	High	Flywire will respond to data leaks within their privacy framework. We will be informed and we will discuss next steps.	
US Federal Government Access rights	Low- Privacy	Low	Low	If we are informed, we will inform the user.	

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

17. Does your initiative involve digital tools, databases or information systems?

Yes

17.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

No

18. What technical and physical security do you have in place to protect personal information?

All data is Encrypted. Data is stored and handled using the SOC 2 compliance framework. Flywire undergoes an annual SOC II and PCI DSS review to help ensure that Flywire handles customer data securely and in compliance with all applicable laws, including, but not limited to, GDPR, PIPEDA, FERPA, GLBA and other data protection laws. Data is stored behind a Firewall, and Data is only available to employees with special permissions.

AWS Securities:

REDUNDANCY

Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AVAILABILITY

AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

CAPACITY PLANNING

AWS continuously monitors service usage to deploy infrastructure to support our availability commitments and requirements. AWS maintains a capacity planning model that assesses our infrastructure usage and demands at least monthly. This model supports planning of future demands and includes considerations such as information processing, telecommunications, and audit log storage.

EMPLOYEE DATA CENTER ACCESS

AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

DATA CENTER ACCESS REVIEW

Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.



DATA CENTER ACCESS LOGS

Physical access to AWS data centers is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis.

DATA CENTER ACCESS MONITORING

We monitor our data centers using our global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

CCTV

Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

DATA CENTER ENTRY POINTS

Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

INTRUSION DETECTION

Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to

server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 AWS Security Operations Centers for immediate logging, analysis, and response.

MEDIA DESTRUCTION

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

ONGOING DATA CENTER RISK MANAGEMENT

The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

THIRD-PARTY SECURITY ATTESTATION

Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to

obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.

<https://www.flywire.com/es/legal/sub-processors>

19. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	
We only allow employees in certain roles access to information	Yes
Employees that need standing or recurring access to personal information must be approved by executive lead	Yes
We use audit logs to see who accesses a file and when	No
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

20. How will you make sure that the personal information is accurate and complete?

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

Data is inputted by the user (payer) at time of collection. Data is updated by user (payer) at this time.

21. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

21.1 Do you have a process in place to correct personal information?

Yes

21.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Yes

21.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

Yes

22. Does your initiative use personal information to make decisions that directly affect an individual?

No

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

23. Does your initiative involve an information sharing agreement?

No

24. Will your initiative result in a personal information bank?

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

Yes

Describe the type of information in the bank
https://www.sd68.bc.ca/information-and-privacy/
Name of main organization involved
School District No. 68 (Nanaimo-Ladysmith)
Any other ministries, agencies, public bodies or organizations involved
N/A
Business contact title and phone number for person responsible for managing the PIB
Executive Director of Communications, Privacy & Community Engagement – 250-741-5273

PART 8: SIGNATURES

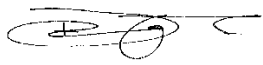
You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Nanaimo Ladysmith Public Schools' International Student Education Program intends to use FlyWire for the purpose of global wire transferring of funds from the student's family to the district.

Privacy Office Signatures


This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative and Head of public body designate	Dale Burgos		April 19, 2023

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Program/Department Manager	Rob Hutchins		
Contact Responsible for Systems Maintenance and/or Security	See Privacy Officer		

Role	Name	Electronic signature	Date signed
Only required if they have been involved in the PIA			