EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **<u>Purpose</u>**

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **<u>Definitions</u>**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy.. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

- In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA:

  PFG will utilize PFG' s Data Governance Policy K-12 and Data Retention and Deletion Policy K-12. This governance structure is in place to foster sound policy, clarity of controls and consistent, processes. PFG recognizes its responsibility to protect the privacy and ensure security for all users. PFG has adopted this Data Governance Policy to comply with all applicable laws and regulations (see

Addendum 1) to protect against unauthorized access.

PFG will provide an annual training program for all employees and consultants who are directly or peripherally involved in design, production, development, monetization and operations of the products and employees and consultants involved in the collection, use, storage, disclosure or any other handling of data including PII.

PFG evaluates all 3rd parties that we work with to ensure compliance.(See Addendum 1).

PFG will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement and utilizing PFG Data Breach Policy K-12 (see Addendum 1),

- Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

- For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

- Vendor [*check one*] ____X__will _____will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

- Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

- Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. <u>Notification of Breach and Unauthorized Release</u>

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR: PASSPORT FOR GOOD

DocuSigned by:

270CB4A3171F4D4...

Signature

Peter Farman

Printed Name

Authorized Representative

Title

5/31/2023

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND PASSPORT FOR GOOD

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Passport For Good] which governs the availability to Participating Educational Agencies of the following Product(s):

Passport For Good Web Application

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: PFG will provide annual training program for all employees and consultants who are directly or peripherally involved in design, production, development, monetization and operations of the products and employees and consultant involved in the collection, use, storage disclosure or any other handling of data including PII.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2023 and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a

Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

ADDENDUM 1 DATA & SECURITY

Data Governance Policy K-12

Data Retention and Deletion Policy K-12

Data Breach Policy K-12

2 items below struck as part of iKeepSafe notification re:

Addendum to MSLA Executed 10/27/2021

GIVING - TREE ASSOCIATES, LLC
T/A PASSPORT FOR GOOD ("PFG")
333 Broadway - 4th Floor
Troy, New York 12180
(518) 203-6710 (T)
General E-Mail: info@passportforgood.com
Website: www.passportforgood.com

Data Governance Policy K-12

Policy Title	**Data Governance Policy K-12**
Policy Owner	**Chief Privacy Officer**
Policy Approver(s)	**Data Governance Committee**
Storage Location	**Google Drive Corporate Policies shared folder.**
Effective Date	**09/01/2019**
Revision Date	**10/27/2021 & 3/23/2-23**

Purpose

Data governance is an organizational approach to management that is formalized as a set of policies and procedures that encompass the full life cycle of Data, including, PII; from acquisition, to use, to disposal. These rules and policies establish decision rights, as well as the controls that ensure security, accountability, and trustworthiness. Governance is not active day-to-day oversight, but rather a strong foundation for a viable management system. Any governance structure is in place to foster sound policy, clarity of controls, and consistent processes.

PFG recognizes its responsibility to protect the privacy and ensure security for all users.

PFG has adopted this Data Governance Policy to comply with all applicable laws, rules and regulations.

Scope & Definitions

This policy applies to all employees and consultants of PFG. In accordance with PFG's policy and procedures, this policy will be reviewed and adjusted on an annual basis or more frequently, as needed. This policy is designed to ensure only authorized disclosure of Data, including, PII as well as establishing best practices around governance. Where PFG uses contractors such as third-party service providers they will be notified of this policy.

See the Definitions section of the policies for certain definitional terms used in this policy.

Data Access Policy

1. PFG restricts access to Data, including, PII to only those who need to know the information in order to process the Data, including, PII for the intended service or provide customer assistance and any such access will be limited to the Data, including, PII necessary for the performance of the operation.

2. PFG will conduct background checks on all PFG employees and consultants who will have access to Data, including, PII as part of the hiring process.

3. Access to Data, including, PII may be revoked by PFG for any reason, including, termination.

4. PFG identifies access to Data, including, PII based on roles and need for access.

5. PFG will protect its Data, including, through security measures.

Role	Data	Purpose
Product Development	All	For development and customer support
Customer Support	All	For customer support and development
Onboarding and Engagement	All	For onboarding and customer support
Business Development	All	For business development, customer support and engagement
Data Owner	All	For development and control

Data Usage Policy

1. PFG has instituted policies to make sure Data, including, PII are not misused or abused and are used in accordance with all applicable regulations, rules and laws. Data Owners manage Data, including, PII according to this policy and all other applicable policies and practices implemented by PFG.

2. PFG employees and consultants are only allowed to access Data, including, PII for the required performance of their job function/role and not for any inappropriate purposes.

De-Identification Method

1. PFG may use Data, including, PII in a de-identified or aggregate format. The methods employed to de-identify Data, including, PII are technically reliable and consistent with industry best practices.

2. Data, including, PII is anonymized in the quality assurance and development environments by running a task to de-identify the Data, including, PII.

3. The de-identification task replaces all first and last names with another random name (list is from online public source of names), emails and usernames are changed to as '{userId}@p4g.fake' and phone numbers are blanked out, except for a small list of explicitly declared white list users (PFG employee personal accounts for testing).

Third Party Service Providers

1. PFG evaluates third party service providers to ensure they are capable of complying with our policies and practices, including, those related to the collection, use, transfer, deletion, confidentiality, security and integrity of Data, including, PII.

2. Third party service provider will only have access to Data, including, PII that is necessary for the service they provide to PFG.

Training

1. PFG will provide an annual training program for all employees and consultants who are directly or peripherally involved in design, production, development, monetization and operations of the products and employees and consultants involved in the collection, use, storage, disclosure or any other handling of Data, including, PII.

2. PFG will provide training to any employees and consultants who have access to Data on the federal and state laws governing confidentiality prior to receiving access to such Data, including, PII.

Security, Security Audit and Remediation

1. PFG uses and maintains reasonable security procedures and practices, taking in to account available technologies to safeguard and protect the Data, including, PII from unauthorized access, destruction, use, modification, or disclosure and ensure the confidentiality of Data, including, PII collected from and about students.

2. PFG stores all Data, including, PII with Microsoft Azure and relies upon the security audits conducted by Microsoft Azure. PFG reviews the security audits conducted by Microsoft Azure on a regular basis or as needed.

3. PFG periodically reviews its practices to protect against unauthorized access.

4. PII is encrypted at rest and in motion.

5. All accounts are protected by a password. All passwords are stored and transferred securely using encryption and salt hashing.

6. PFG has remediation plans to address identified security issues as they arise.

Data Integrity

PFG ensures that its storage for data, including, PII is accurate and kept up-to-date through the means of auditing, review processes, and the implementation of security controls (e.g. integrity monitoring).

Business Continuity Plan ("BCP") & Disaster Recovery Plan ("DRP")

To ensure that essential business function will continue to operate during and after a disaster, PFG has a BCP and DRP.

The objective of the BCP is to coordinate recovery of critical business functions in managing and supporting the business recovery in the event of a facilities disruption or disaster. **A disaster is defined as any event that renders a business facility inoperable or unusable so that it interferes with the organization's ability to deliver essential business services.**

The priorities in a disaster situation are to:

1. Ensure the safety of employees.
2. Mitigate threats or limit the damage that threats can cause.

3. Have advanced preparations to ensure that critical business functions can continue.

The BCP is dependent upon the ability of the third-party service providers that PFG uses for its services and website to provide uptime and system availability. The third-party service providers used for PFG's services and website does geographically redundant backup of PFG's database allowing PFG to access a backup very quickly if necessary.

PFG would be able to recover from any disaster by relying upon access to all data through the third-party service provider.

To ensure that PFG will be able to recover specific business applications after a disaster, PFG has a DRP.

1. PFG uses a third-party service provider for PFG services and website.

2. If a disaster occurs, PFG will notify users via the home page of its web site and through other available communication channels.

3. Response times will be dependent upon the third-party service provider's ability to recover from the disaster.

4. If necessary, PFG can restore the database.

5. PFG can redeploy our services to the instances, if necessary and test and monitor for stability.

6. PFG's has back up of the object code, source code and documentation at secured location.

Exceptions

Any exceptions to the Data Governance Policy K-12 are highly discouraged, but in the event, there is a legitimate business need, it must be approved by the PFG Chief Privacy Officer and the exception will be documented. All exceptions will be reviewed quarterly and will be prohibited after no longer necessary.

Governing Laws and Regulations

Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively (FERPA)
NYS Education Law section 2-d, 101, 207 and 305 – Part 121
Children's Online Privacy Protection Act (COPPA)

Non-Compliance

Violations of this policy will be treated in accordance with PFG's policies. PFG may face significant fines if non-compliant with regulations. Individuals subject to this policy will be subject to sanctions for non-compliance that may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable PFG policies.
2. Termination of employment or contract.
3. Legal action according to applicable laws and contractual agreements.

Relevant Policies, Procedures, Standards, and Processes

- Data Breach Policy K-12
- Data Retention and Deletion Policy K-12
- Data Table K-12
- Third Party Service Providers K-12
- Assurance of Compliance Requirements – COPPA

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Aimee Dowd	04/15/2019
2.0	Draft Reviewed by Product Team and CEO	Lynne Lapham	04/26/2019
2.1	Final Draft Submitted to IKS	Lynne Lapham	04/30/2019
2.2	Edited Final Draft Submitted to IKS	Lynne Lapham	05/31/2019
2.3	Final	Lynne Lapham	09/01/19
2.4	Revision	Chief Privacy Officer & Dir Business Admin	10/27/2021
2.5	Revision	Chief Privacy Officer & Dir Business Admin	3/23/2023

GIVING - TREE ASSOCIATES, LLC
T/A PASSPORT FOR GOOD ("PFG")
400 Broadway #959
Troy, New York 12180
(518) 203-6710 (T)
General E-Mail: info@passportforgood.com
Website: www.passportforgood.com

Data Retention and Deletion Policy K-12

Policy Title	**Data Retention and Deletion Policy K-12**
Policy Owner	**Chief Privacy Officer**
Policy Approver(s)	**Data Governance Committee**
Storage Location	**Google Drive Corporate Policies shared folder.**
Effective Date	**09/01/2019**
Revision Date	**10/27/2021 & 3/23/2023**

Purpose

This policy is designed to outline certain retention and deletion requirements for Data, including, PII, in alignment with laws, rules and regulations for student users in grades K-12. Retention of certain Data, including, PII, may be required by laws, rules or regulations permitted for designated purposes.

Scope and Definitions

This policy is written for all Data Owners, privacy officer(s) and any others who manage the use of Data, including, PII, within PFG.

See the Definitions section of the policies for certain definitional terms used in this policy.

Policy Statements

PFG only collects minimal Data, including, PII, from students in order to register and use PFG.

Data Retention

PFG stores a student users' Data, including, PII, for as long as the account is active, and it is necessary to provide the PFG services to the student user and thereafter, unless, otherwise specified herein.

Some Data, including, PII, may be kept after an account is inactive, including, for an Educational Entity's legal compliance reasons (e.g., maintenance of "education records" under FERPA or "student user records" under various state student privacy laws.)

Deletion

1. Upon Request – Data, Including, PII

Data, including, PII, may be deleted at any time as follows. Upon receipt of a request by a verified student user or the parent of the verified student user, of a request to delete the Data, including, PII, in writing, PFG will delete the Data, including, PII. The student user's Data, including, PII, will be deleted as soon as reasonably possible after receipt of a such request.

2. Upon Request – Account

An account may be deleted at any time as follows. Upon receipt of a request by a verified student user or the parent of the verified student user, of a request to delete the account, in writing PFG will delete the account. The student user's account will be deleted as soon as reasonably possible after receipt of a such request.

3. Inactive Accounts/Data, Including, PII

PFG deems an account and Data, including, PII, inactive if a student user or a parent of the student user does not log into their account for a period of 7 years.

4. Requested by a Parent/Eligible Student

All requests regarding a student user's Data, including, PII, are to be first addressed to the Educational Entity that the student user is associated with and has an account with PFG and otherwise addressed in accordance with PFG's K-12 Privacy Policy. If requests regarding a student user's Data, including, PII, are not addressed by the Educational Entity, such parent may as a second level of support, contact PFG, as follows:

PFG Chief Privacy Officer
400 Broadway #959 Troy,
New York 12180 Phone:
(518) 203-6710
E-Mail: cpo@passportforgood.com

5. Archival Storage

When deleting an account, the student user's username and password and any device specific information, location information and IP address will be deleted.

6. Specific Student Information

Copies of Data, including, PII may remain in a cached or archived form on PFG's systems or the system of PFG's third party service providers after deletion of the Data, including, PII.

Data Table

PFG has established a Data Table K-12 to document all Data, including, PII, processed, considering any reasons why Data, including, PII, must be retained. For each data type, the Data Table K-12 also documents the following:

a. Identification;
b. Data Owner;
c. Processing (transfer and share);
d. Classification;
e. Retention times, and:
f. Disposition upon deletion.

Anonymization

When the Data, including, PII, meets the end of the retention period or a request is made to delete the Data, including, PII, it may be erased or sufficiently anonymized. Anonymization may include practices such as the following:

a. Deleting specific element(s) or unique identifier(s) that would otherwise identify the subject.
b. Separating personal Data from non-identifying Data (e.g. separating order number from name/address).
c. Aggregating personal Data of enough individuals so that specific Data cannot be attributed to a subject.

Backups

Backups will be executed in accordance with the backup schedule of Microsoft Azure which is deployed by PFG in support of the Site and the PFG App.

Auditing/Review

PFG ensures that Data, including, PII stored is accurate and kept up-to-date through the means of auditing, review processes, and the implementation of security controls (e.g. integrity monitoring).

Storage

Data, including, PII, may be stored if it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

In the event of prolonged storage, PFG must document the purpose as PFG must implement and maintain technical and organizational measures to protect said Data, including, PII. Technical measures may include anonymization, encryption, and other controls.

Retention Upon Termination of Contract with an Educational Entity

Given PFG's intended business purpose to offer individual's a lifetime tool to collect their Data, including, PII, in PFG's platform, PFG cannot delete individual student user Data, including, PII, upon termination of a contract between an Educational Entity and PFG.

As part of the contract between PFG and an Educational Entity, the Educational Entity acknowledges that upon termination of that relationship, for any reason, PFG will continue to maintain the Data, including, PII, of the individual student users as detailed in the Data Table K-12, the Privacy Statement and if applicable, the K-12 Privacy Policy.

Upon termination of the contract between PFG and an Educational Entity, PFG will terminate any access to the Data, including, PII, by the Educational Entity, including, access by administrators, faculty and its personnel.

Upon termination of a contract between PFG and an Educational Entity, student users will only be allowed access to add new Data, including, PII, if the student user becomes associated with another Educational Entity that PFG has a contract with, or is registered with PFG as an Individual User in accordance with the requirements of PFG and the Terms.

Exceptions

Any exceptions to the Data Retention and Deletion Policy K-12 are highly discouraged, but in the event, there is a legitimate business need, it must be approved by the PFG Chief Privacy Officer and the exception will be documented. All exceptions will be reviewed quarterly and will be prohibited after no longer necessary.

Governing Laws and Regulations

Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively (FERPA)

Children's Online Privacy Protection Act (COPPA)

NYS Education Law section 2-d, 101, 207 and 305 – Part 121

Non-Compliance

Violations of this policy will be treated in accordance with PFG's policies. PFG may face significant fines if non-compliant with regulations. Individuals subject to this policy will be subject to sanctions for non-compliance that may include, but are not limited to, one or more of the following:

4. Disciplinary action according to applicable PFG policies.
5. Termination of employment or contract.
6. Legal action according to applicable laws and contractual agreements.

Relevant Policies, Procedures, Standards, and Processes

- Data Table K-12
- Data Governance Policy K-12

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Aimee Dowd	04/05/2019
2.0	Draft Reviewed by Product Team and CEO	Lynne Lapham	04/26/2019
2.1	Final Draft Submitted to IKS	Lynne Lapham	04/29/2019
2.2	Edited Final Draft Submitted to IKS	Lynne Lapham	05/31/2019
2.3	Final	Lynne Lapham	09/01/19
2.3	Final	Lynne Lapham	09/01/19
2.3	Final	Lynne Lapham	09/01/19
2.4	Revised	Chief Privacy Officer & Dir Business Admin	10/27/2021
2.5	Revised	Chief Privacy Officer & Dir Business Admin	3/23/2022

PASSPORT FOR GOOD®

GIVING - TREE ASSOCIATES, LLC
T/A PASSPORT FOR GOOD ("PFG")
400 Broadway #959
Troy, New York 12180
(518) 203-6710 (T)
General E-Mail: info@passportforgood.com
Website: www.passportforgood.com

Data Breach Policy K-12

Policy Title	**Data Breach Policy K-12**
Policy Owner	**Chief Privacy Officer**
Policy Approver(s)	**Data Governance Committee**
Storage Location	**Google Drive Corporate Policies shared folder.**
Effective Date	**09/01/2019**
Revised Date	**10/27/2021 & 3/23/2023**

Purpose

This policy is designed to outline the PFG's Data Breach Policy K-12.

Scope and Definitions

This policy is applicable to all Data Users. The policy applies to all Data, including, PII, processed by PFG. Where PFG uses contractors such as third-party service providers they will be notified of this policy.

See the Definitions section of the policies for certain definitional terms used in this policy.

Duty to Report Breach

Data Users shall report every discovery or report of a Breach to the Privacy Officer without unreasonable delay.

Notification of Breach

In the event of a Breach, PFG will to provide notice to affected parties, as soon as reasonably possible after confirmation of the Breach and the ability to ascertain the information required to fulfill the notice requirements.

PFG may notify a student user affected by the Breach in conjunction with the Educational Entity if the student is associated with the Educational Entity.

The notice of a Breach will include the following information:

a. The date the Breach was discovered;
b. The date of the Breach, estimated date of the Breach or the date range within the Breach occurred or a best estimate;
c. The information that was subject to the Breach;
d. A general description of what occurred including how the Breach occurred and the number of affected individuals, based on available information;
e. The name of the contact person at PFG;
f. Whether the notification was delayed because of law enforcement;
g. What steps PFG has taken to respond to and mitigate the situation, prevent it from happening again, and advice to the impacted individuals on how they can best protect themselves; and
h. Contact information for representatives who can assist individuals, parents or eligible students with additional questions.

PFG will comply with all applicable laws, rules and regulations regarding notice of a Breach.

Documentation

PFG will document all responsive actions taken in connection with any incident involving a Breach.

Post-Incident Review

PFG will conduct post-incident review of events and actions taken. Upon completion of the post-incident review PFG will determine if any business practices or policies relating to the protection of Data, including, PII need to be revised or edited.

Exceptions

Any exceptions to the Data Breach Policy K-12 are highly discouraged, but in the event, there is a legitimate business need, it must be approved by Chief Privacy Officer and the exception will be documented. All exceptions will be reviewed quarterly and will be prohibited after no longer necessary.

Governing Laws and Regulations

Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively (FERPA)

Children’s Online Privacy Protection Act (COPPA)

NYS Education Law section 2-d, 101, 207 and 305 – Part 121

Non-Compliance

Violations of this policy will be treated in accordance with PFG's policies. PFG may face significant fines if non-compliant with regulations. Individuals subject to this policy will be subject to sanctions for non-compliance that may include, but are not limited to, one or more of the following:

7. Disciplinary action according to applicable PFG policies.
8. Termination of employment or contract.
9. Legal action according to applicable laws and contractual agreements.

Relevant Policies, Procedures, Standards, and Processes

- Data Governance Policy K-12
- Data Retention and Deletion Policy K-12

Revision History

Version	Change	Author	Date of Change
1.0	Initial Draft	Aimee Dowd	04/09/19
2.0	Draft Reviewed by Product Team and CEO	Lynne Lapham	04/26/19
2.1	Final Draft Submitted to IKS	Lynne Lapham	04/30/19
2.2	Edited Final Draft Submitted to IKS	Lynne Lapham	05/31/19
2.3	Final	Lynne Lapham	09/01/19
2.4	Revised	Chief Privacy Officer & Dir Business Admin	10/27/2021
2.5	Revised	Chief Privacy Officer & Dir Business Officer	3/23/2023

F2023

iKeepSafe

ADDENDUM 2 Sample Training Plan – format different than 2020 format because couldn't track change 2020 layout

SAMPLE TRAINING AGENDA See attached for an example training plan and agenda. See attached Addendum 2.

Frequently Used P4G Terms

Institution= School District
Group = Clubs, Sports, Class of 202x
Section= Sub group or Season
Users –Student User or Admin User
Admins –Institution Admin/Club Advisor
Supervisor-External Community Service Leader
Institution Event -Every student who is a member of your institution can see this event.
Group Event–Only members within a group can see this.
Section Event–Only members in a section can see this.
Personal Event -An event that is not associated with a school.
Purpose Areas –26 Purpose Categories according to the National Volunteer Survey

STUDENT USER

MY DASHBOARD(Top right under your name)

Your Hours -3 Types of Hours: Community Service, Participation and Career Development. (Black numbers are hours that have been stamped. Orange numbers are hours that are currently pending.) You can click on the yellow button "View Passport" in the top of this bar to access your Passport directly AND you can click on the green button "Add Hours" which brings you to your calendar.

Hours in Progress –Status, Submission Status

Your Goals –For any group that has a goal set, it shows you how far you are towards that goal.

Recent & Upcoming Events –List of all recent and upcoming events for clubs that you are a member of AND allows you to sign-up to an event and Add Hours to an event in the past. If you click on the name of any event, it gives you more details for that event. (Note: This does NOT show personal events to allow you to Add Hours too. If you want to Add Hours for Personal Events from the dashboard, you need to go back up to "Your Hours" and click on green button title "Add Hours" which brings you to your calendar. You then click on the date that you want to add your personal event).

Add Hours: Click on the button that says "Add Hours" to the right of a past event. If you are a member of other groups that allows double dipping, then you can submit these hours to additional clubs. Once you click "Continue", then you can fill in the details regarding your hours.

Sign-Up: If there is an event in the future that allows sign up, then you will see a green button to the right of an event. You click on "Sign up" green button and it allows you to sign up and even upload a permission slip if that is required. **ACTION ITEM: Add Hours** to a past Event AND **Sign-Up** to an Event (10/31)

Your Active Groups –List of all of the groups that you are a member of. You can click on "Join More Groups" if you want to see list of additional groups to join. **ACTION ITEM:** Be able to **Join More Groups**

NOTES:

____

____

____

____

____

____

____

____

____

____

STUDENT USER *(Cont'd)*

MY PASSPORT(Top right under your name or "View My Passport" in Yellow when looking at your Dashboard)

On left, it allows you to upload a personal profile picture. On top, it shows you your total # of hours per each of the 3 Hour Types (Community Service, Participation and Career Development)

My Entries –Shows the most recent Entries (Pending or Stamped) "View All" shows all entries. (Once you click on "View All", be sure to sort at the top by Date to show most recent at the top.)

Journal –Shows the most recent Events you created. "View All' shows all Ratings and Reflections. You can also click on "Export" to be emailed a comprehensive listing of all of your events.

Action Item: Export your own **Journal**

My Top 4 Stamps –Out of the 27 Cause Stamps, it shows here your top 4 stamps.

My Affiliations –If you participated in an event that was affiliated with any of our affiliations, then that stamp would show here.

Export Button under Profile Picture –You can export your passport that simply creates a PDF document that lists the Total # of Hours for all 3 hour types. Lists Top Cause Area, List # of Hours for additional Cause Areas and Lists My Affiliations. Student user will receive an email from No-reply with the PDF as an attachment. (Note: This PDF does not include any of your ratings, reflections or list of all entries.)

Action Item: Export a copy of **Your Passport**

NOTES:

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

HELP BUTTON –Bottom right hand corner … yellow round ? button

Start a conversation (Left)Start a support ticket (Right)Knowledge Base Articles (Below - Read all articles.)

STUDENT USER *(Cont'd)*

MY CALENDAR(Top Right under your name)

Shows a calendar view of all of the events that are on the calendar for only groups that you are a member of. Depending on the color of the event (key is at the bottom of the calendar), it allows you to **Sign-Up** to an event by clicking on that event, it also allows you to **Add Hours** to an event in the past by clicking on that event AND it gives you more details for that event. Depending on if the event is in the Past, Present or the Future results in what activity is available to you. (For example you cannot Add Hours to something in the future that hasn't happened yet)

Sync Calendar: In the top right corner, there is a yellow button titled "Options". If you click on that you will see 2 options.. "Add Hours" and "Sync Calendar".

Add Hours for a Group/Institution Event -Click on Event Name and then click on "Add Hours". It will then ask you to choose "Which groups would you like to submit this experience too". (If other groups that you are a member of, allows Double Dipping, then you can submit your hours to multiple groups). Click "Continue" to add the # of hours that you participating in.

Action Item: Be able to **Add Hours** to a Past Group/Institution Event. (Blood Drive 10/16)

Add Hours for a Personal Event -Click on an empty portion on the day that you participated in your event. It will then ask you to choose "Which groups would you like to submit this experience too". (If other groups that you are a member of, allows Double Dipping, then you can submit your hours to multiple groups). Click "Continue" to add the # of hours that you participating in along with additional details about your personal event.

Action Item: Create a Personal Event.

Adding Experience Details –Input Title, Date/Time, Hour Type, Purpose, Rating and Location. Input external supervisor who can approve your hours, provide a reflection and upload a picture (if desired)

IF YOU RECEIVE AN ERROR MESSAGE: An appropriate response can be… "Sometimes our programmers are releasing code and it effects our demo site. This is usually resolved within a few minutes, but in the meantime I'm going to try another approach."

NOTES:

____
____
____
____
____
____
____
____
____
____
____
____
____
____
____

ADMIN USER

(Top right corner, Great Ridge School District –Administrator OR Click on Large Green Button center of screen)
Introduce the Sidebar along left side Introduce the 3 hour types for entire Institution at top Show a list of all groups with # of members and hour type totals for each
Blue Sidebar Institution Dashboard, **Statistics,** Goals, Communication, Admins, Events, Groups, Settings, Export **Action Item:** Show and be able to talk about the **Statistics** page.
Groups (Under Institution Name)
My Brothers Keeper – Dashboard shows the 3 Hour Types at the top. Under "Active Sections", click on the right, the yellow square button with the icon of a pen on the button. On the bottom of the next page, you can create a **Goal** by clicking "Add Goal". Fill out the information on the following screen and click on "Create". **Action Item:** Create **a goal** for a section.
If you Go To Sections, Click on Active Section Name (2019-2020) 3 Hour Types for this Group
Pending Unstamped Submissions –These are student submissions that have yet to be stamped by the Admin**Events**-Add Event is Under Yellow "Options" box in top right corner. **Action Item:**Add an event for MBK
Members –A complete list of members who have joined your group.
Create Event –Fill out details for new group event.
Record Attendance –This will allow you to take attendance on the day of the event but not before.
Event Sign-Up and **Permission Slip** Type of HoursSupervisor InformationLocation
Then go back to the calendar and click on a "Sign-Up" Event to show how to sign-up. 10/31
Also, click on a past event **"Special Meeting on Mentor Program"** to show how to take attendance.
Action Item: Take Attendance for an event both as an admin taking attendance and using a **QR Code**
NOTES:

____

____

____

____

____

____

____

____

____

____

____

COMPETENCIES LIST

1)**Add Hours** to a past Group/Institution Event

2)**Sign-Up** to an Event

3)Be able to **Join More Groups**

4)Export your own **Journal**

5)Export a copy of **Your Passport**

6)Show and be able to talk about the **Statistics** page.

7)Create **a goal** for a section.

8)**Add an Event** for My Brothers Keeper Group

9)**Take Attendance** for an event both as an admin taking attendance and using a QR Code

10)Start a **Customer Support Ticket** using the HELP button