DIGITAL PROMISE AND DIGITAL PROMISE GLOBAL

PRIVACY POLICY FOR PERSONAL INFORMATION

MARCH 27, 2018

Effective Date: April 27, 2018

DIGITAL PROMISE PRIVACY POLICY FOR PERSONAL INFORMATION

INTRODUCTION

It is the policy of Digital Promise and Digital Promise Global (collectively, "Digital Promise") to comply with applicable laws and regulations protecting the privacy of personal information in the jurisdictions and the School districts in which Digital Promise operates. Digital Promise respects and protects personal information collected or maintained by or on behalf of Digital Promise, regardless of the form, format, location or use of the information.

This document (the "Policy") sets forth the standards Digital Promise applies with respect to protecting nonpublic personal information ("NPI"), as defined below. The Policy governs employees, temporary staff, contractors, and consultants of Digital Promise and its affiliates -- defined below as "Digital Promise Representatives" -- with respect to their access to and handling of NPI. The principal objectives of the Policy are to:

- Ensure the confidentiality and integrity of NPI;
- Protect against unauthorized access to or use of NPI;
- Prevent harm to individuals due to identity theft, fraud, or any other act that would violate an individual's right to privacy.

Each Digital Promise Representative has the obligation to play his or her role in protecting NPI, including NPI of fellow Digital Promise Representatives, in compliance with all applicable laws, regulations, this Policy and other Digital Promise policies and procedures, including, but not limited to, the Digital Promise Child Safeguarding Policy and Procedures ("DPCSPP") which can be found at http://digitalpromise.org/wp-content/uploads/2016/03/Safeguarding-Children-Policy.pdf.

DEFINITIONS

For purposes of this Policy, the following definitions apply:

"Digital Promise Representative" means any employee, temporary staff member, contractor or consultant working for Digital Promise.

"Nonpublic personal information" ("NPI") means:

> Information in any media or format, that identifies or may be used to identify an individual and that does not consist solely of information that is publicly available or derived from federal, state or local government records lawfully made available to the general public. NPI may include, but is not limited to: (1) an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: Social Security number, student identification number, driver's license number, voter registration number, other government-issued identification number, biometric

identifier, medical beneficiary number, financial account number, or credit card/debit card number, non-public e-mail address, and (2) health information together or in association with an identifier of an individual (such as an e-mail address, birth date, or any other identifying number or code).

NPI does not include anonymized data, such as aggregated data, to the extent that the aggregation is sufficient to prevent identification of an individual from that data either itself or in combination with publicly available data.

"Security Assessment Questionnaire" means the list of questions prepared by Digital Promise as a means to review and assess the quality of data protection maintained and implemented by a Third Party.

"Third Party" means any person, consultant, contractor, vendor, company, organization, public authority/agency, or other entity outside of Digital Promise that may have access to or contact with NPI, other than the individual to whom such NPI pertains.

"Sites" means Digital Promise's websites located at www.digitalpromise.org, www.digitalpromise.net, www.global.digitalpromise.org, Verizon.digitalpromise.org, microcredentials.digitalpromise.org, www.digitalpromise.net, and any of Digital Promise's other websites and their respective subdomains.

ADMINISTRATION AND IMPLEMENTATION

Privacy Officer

Digital Promise's Privacy Officer ("PO") has primary responsibility for the administration of this Policy. In fulfilling that responsibility, the PO shall consult, as appropriate, with legal counsel ("Legal"), the Information Officer ("IO"), Human Resources ("HR"), and others.

Review and Revision

The PO shall review this Policy periodically and ensure that it is updated and revised as appropriate. The PO, in consultation with Legal, shall monitor updates in applicable data privacy law to ensure that this Policy reflects Digital Promise's legal obligations with respect to NPI.

Training

The COO, with support of the PO, shall implement training to make Digital Promise Representatives aware of their obligations with respect to this Privacy Policy. Such training shall be provided to all current Digital Promise Representatives after the effective date of this Privacy Policy and, for new Digital Promise Representatives hired after the effective date, at the time of, and as a term and condition of, employment. The COO also shall implement "refresher" reminders or training annually, but also in the event of material revisions to this Policy or before Digital Promise Representatives engage in a new project involving NPI. All Digital Promise Representatives must be educated on the principles and procedures set forth in this Policy, as applied to the specific context in which they handle

NPI and the nature of that NPI. The training may be offered in conjunction with training required by the Digital Promise Information Security Policy.

POLICIES AND PROCEDURES

1. COLLECTION AND USE OF NPI

1.1. Permissible Uses of NPI

Digital Promise accesses, collects and uses NPI to effectively manage and develop its business and to comply with its legal obligations. For example, Digital Promise may access, collect, use and disclose (as stated in Section 2.1 below) NPI for legitimate business purposes such as, without limitation:

- Fulfilling requests and providing information, services and notices to persons or entities participating in Digital Promise programs or using Digital Promise services (*e.g.*, newsletters, updates, promotional materials, and email messages or mailings);

- Providing compensation and benefits to employees, including:

  - Managing payroll and tax information;

  - Evaluating employee flexible spending or medical leave requests;

  - Conducting background checks;

- Developing new services and offerings and maintaining and improving services and offerings;

- Improving marketing and promotional efforts;

- Operating its business in the normal course and managing its risks, including for auditing and security purposes;

- Updating and enhancing records;

- Creating aggregated, de-identified information for analytical, research, reporting, product development, or other appropriate purposes;

- Handling litigation and complying with government (regulatory, judicial, legislative) requests or orders;

- Preventing fraudulent transfers;

- Performing analyses to review the effectiveness of Digital Promise programs and operations;

- Resolving disputes, troubleshooting problems, and enforcing and investigating compliance with agreements with Digital Promise Representatives and persons or entities participating in Digital Promise programs or using Digital Promise services; and

- Otherwise protecting Digital Promise's rights or processes.

1.2. Authorized Users of NPI

Digital Promise Representatives may not use NPI for any purpose other than to perform their job functions, and then only if such use is required by the nature of their jobs.

1.3. Minimum Necessary Uses

Digital Promise uses only the type and minimum amount of NPI needed to accomplish the purposes for its legitimate uses of NPI. Digital Promise Representatives must collect or use only that minimum amount of NPI to perform their legitimate and authorized responsibilities.

1.4. Use for Marketing Purposes

Digital Promise does not use NPI for marketing purposes, including to promote, advertise, or suggest the benefits or quality of any product or service, without providing the individual to whom the NPI pertains the opportunity to opt out of such use in the future, or, where required by law, with the advance consent of the individual.

1.5. Uses for Text Messaging Purposes

Digital Promise may use NPI for text messaging to the extent permitted by law, including the federal Telephone Consumer Protection Act and similar state laws. Digital Promise may use third-party vendors to send text messages using an automatic telephone dialing system ("autodialer"), provided recipients of the messages (i) have expressly provided their consent to receive such messages and (ii) are offered the opportunity to opt out of receiving further text messages in the future.

1.6. Uses for Email Purposes

If an individual has provided Digital Promise with his or her email address to subscribe to its newsletter, Digital Promise may periodically send the individual emails that promote or otherwise contain commercial information relating to Digital Promise. An individual will have the ability to "opt out" of, and thus to stop receiving, further promotional or commercial emails. Even if an individual requests not to be contacted by Digital Promise, Digital Promise may use the individual's contact information to send crucial information about Digital Promise's Sites, including information about changes to its privacy policy or the terms of use.

1.7. Automatically Collected Usage Information

Digital Promise may, by using "cookies," pixel tags, Flash cookies, and other technologies, collect information relating to the way an individual uses and access Digital Promise Sites, such as what pages an individual visits, what type of browser an individual is using, his or her IP address, his or her location, the information for which an individual searches, the domain name of the website from which he or she came. Digital Promise may use the information it automatically collects to operate and improve its Sites. Digital Promise may share aggregated data concerning users with partners or potential partners and others interested in how Digital Promise Sites are used. When third parties help Digital Promise to collect data relating to an individual's use of Digital Promise Sites, they also may collect information automatically, using an individual's IP address, or through cookies, pixel tags, Flash cookies, and similar technologies. These third parties collect this data to help Digital Promise analyze usage of Digital Promise Sites and better manage content on the Sites by giving Digital Promise information about the usage and popularity of Digital Promise content and features. These third parties may collect information (which may be considered NPI) about an individual's online activities over time and across different websites when an individual uses our Sites. Collection, use, and sharing of information by these third parties are governed by the privacy policies of those third parties, not by this Privacy Policy. Digital Promise is not responsible for the privacy practices of any third parties. Digital Promise Sites do not currently respond to "do not track" signals or other mechanisms that provide an individual user with the ability to exercise choice regarding the collection of that user's NPI involving online activities over time and across third-party websites or online services.

1.8. Other Websites or Applications

Digital Promise's Sites may contain links to other websites or may allow an individual to use third-party services (such as payment processing services or social networking services). Digital Promise is not responsible for the privacy practices of any other websites or service providers.

1.9. Behavioral Research Involving Human Subjects

Digital Promise Representatives whose work involve behavioral research involving human subjects shall comply with applicable privacy laws, regulations and rules, including, but not limited to, the Federal Policy for the Protection of Human Subjects (commonly referred to as the "Common Rule"), to the extent applicable to their work, and shall obtain any consent from human subjects as may be required by an institutional review board.

1.10. Privacy of Children and Students

Digital Promise Representatives whose work involve access to information from children or students shall comply with privacy laws, regulations, rules to the extent applicable, including, but not limited to, the federal Family Educational Rights and Privacy Act ("FERPA"), the federal Protection of Pupil Rights Amendment, and the federal Children's Online Privacy Protection Act, as applicable.

Except as permitted by FERPA and other applicable law, Digital Promise shall not publish or otherwise disclose data containing NPI, or any other information, which identifies students, employees or officers of a school district or individual schools participating in a Digital Promise program by name without the written consent of such individuals, or in the case of a student under the age of 18, his or her parent or legal guardian.

2. DISCLOSURE OF AND ACCESS TO NPI

2.1. Permissible Purposes for Disclosures

Digital Promise limits its disclosures of NPI to those necessary to accomplish Digital Promise's legitimate business purposes, including without limitation, those purposes described under Section 1.1 of this Policy.

2.2. Disclosures within Digital Promise

Access to NPI maintained by Digital Promise is limited to those Digital Promise Representatives or Third Parties with a legitimate need to know such information. For example, those with access to NPI needed to conduct payroll functions may not need, and therefore should not have, access to student information.

2.3. Disclosures to Third Parties

2.3.1. Scope of Disclosure Generally

Digital Promise limits its disclosures of NPI to those Digital Promise Representatives and Third Parties necessary to accomplish Digital Promise's legitimate educational and business purposes. To the extent disclosures are made to a Third Party, Digital Promise Representatives must ensure that the NPI is disclosed only to those individuals employed by or acting on behalf of such a Third Party who have a specific need to view the NPI. Digital Promise will not sell student NPI.

2.3.2. Subcontractors/Vendors

NPI may be disclosed to a Digital Promise subcontractor (including any Third-Party vendor) only pursuant to a written agreement providing that the subcontractor agrees, prior to accessing any NPI, to protect the NPI. Digital Promise will share the names of these subcontractors/vendors with customers, or individuals from whom it collects NPI, upon request.

Absent an exception granted by the IO or PO, NPI may not be disclosed to a Third Party subcontractor prior to Digital Promise's receipt, review and approval of the subcontractor's completed Security Assessment Questionnaire.

2.3.3. Disclosures to Governmental and Regulatory Agencies or Authorities

NPI may be disclosed to law enforcement and other governmental or regulatory agencies and/or authorities, and to other third parties, when compelled to do so by any governmental

authorities or for the purpose of complying with applicable law, including in response to court orders and subpoenas.

2.3.4. Disclosure in Case of Threat of Injury, Interference or Fraud.

NPI may be disclosed in the event Digital Promise has reason to believe someone is causing or threatening to cause injury to or interfere with Digital Promise's rights, operations or property (including, but limited to, by enforcing and investigating an individual's compliance with Digital Promise agreements with the individual, including the terms of use, relating to any of the Digital Promise Sites), the rights or property of others, the operations of Digital Promise's Sites, Digital Promise's Sites' users, or anyone else that could be harmed by such activities; as well as to protect against fraud.

2.3.5. Transfers.

NPI may be disclosed in the event Digital Promise undergoes (or is in discussions regarding) an acquisition, merger, sale, reorganization, consolidation, termination, dissolution, winding up, liquidation, or sale of assets that results in a third party's acquisition of Digital Promise or its assets, and NPI may be among the transferred assets in such a transaction.

2.4. Access to One's Own NPI

Digital Promise endeavors to ensure that all NPI it maintains is accurate. When Digital Promise receives a request to revise or delete certain NPI, appropriate action is taken to evaluate and, if feasible and appropriate, grant the request.

Digital Promise will grant an individual's requests for correction/updating of his/her NPI absent questions regarding the veracity or source of the purportedly corrected/updated information. The PO will resolve any such questions and report to the individual the reason for any denial of the individual's request. An individual may submit a written request to access, correct/update, or delete his or her NPI by contacting Digital Promise at contact@digitalpromise.org.

Direct access by an individual to his or her NPI shall be provided for purposes of confirming the accuracy, integrity, and current validity of the information. Digital Promise will provide an individual with access to his/her NPI in a form and manner that protects the confidentiality of other NPI and does not impose undue cost upon Digital Promise. NPI is limited to the meaning of the term in the Definitions section of this Policy. This Section 2.4 is not intended to give a person the right to revise or delete other information gathered from the person, such as, but not limited to, the person's answers to a survey.

Individual access shall be granted in accordance with this Policy by approval of the COO of a written request from:

- A Digital Promise Representative on his or her own behalf;
- A Third-Party contractor, on behalf of its employees;

- An individual customer with whom Digital Promise has direct contact;
- A Digital Promise Representative on behalf of a consultant whose business relationship with Digital Promise the Representative manages; or
- An individual who has the right under applicable law to access his or her NPI.

Except to the extent prohibited by law, Digital Promise may keep a record of all information that is changed or deleted, and may determine what may be changed or deleted. For example, if Digital Promise is required to keep track of certain kinds of transactions, an individual may be prevented from changing or deleting information relevant for those transactions. Even if Digital Promise deletes or changes an individual's information from Digital Promise's 'live' database, it may still be stored on other databases (including those kept for archival purposes). Digital Promise is not responsible for changing or deleting information about an individual from the databases of any third parties.

3. RETENTION AND DISPOSAL OF NPI

3.1. Retention

Digital Promise retains NPI to accomplish the purposes for which it was collected or is needed to fulfill Digital Promise's legitimate business objectives, consistent with Digital Promise's general data retention policies and any specific document holds applicable to the information. In general, Digital Promise retains NPI for a five year period, unless a different retention period is specified in a grant agreement or other contract for certain NPI.

3.2. Disposal

If certain NPI is no longer permitted to be maintained by Digital Promise pursuant to applicable law, internal retention policies, or contractual agreements with Third Parties, each Digital Promise Representative must either destroy the NPI in an approved manner (as described below) or provide the NPI to his/her manager for its disposal or safe-keeping, consistent with applicable law and any contracts or agreements between Digital Promise and Third Parties. NPI that is subject to disposal in accordance with this policy must be disposed of using means that assure that it no longer be accessible and in compliance with the Digital Promise Information Security Policy.

3.2.1. Hard-Copy Documents

Any hard copy or printed material that displays or contains NPI must be destroyed in a manner that prevents reconstruction. The general approved method of destruction is shredding, but Digital Promise retention policies may require stronger methods of destruction at a more granular level for more sensitive data.

3.2.2. Electronic Documents

To dispose of electronic NPI, the NPI must be purged or destroyed consistent with reasonable industry practices for destruction of data, but Digital Promise retention policies may require stronger methods of destruction at a more granular level for more sensitive data.

4. SECURITY: SAFEGUARDING NPI

Digital Promise strives to protect NPI within its possession, with the nature and extent of protection depending on the nature of the NPI and applicable local laws and regulations.

Accordingly, Digital Promise maintains an Information Security Policy that include reasonable and appropriate administrative, technical and physical safeguards that are designed to: (a) ensure the security and confidentiality of NPI; (b) protect against any anticipated threats or hazards to the security, confidentiality and integrity of NPI; and (c) protect against unauthorized access, disclosure, alteration, or destruction of NPI that could result in the destruction, use, modification, or disclosure of the NPI or substantial harm or inconvenience to Digital Promise or an individual.

Each Digital Promise Representative is responsible for abiding by the Information Security Policy, including the Appendices, as applicable to the Digital Promise Representative and otherwise protecting the security of NPI, including by taking all reasonable measures to safeguard NPI within his or her possession.

5. POLICY VIOLATIONS

5.1. Obligations to Report

Each Digital Promise Representative has the responsibility to report any known or suspected violation of this Policy, including upon receipt of notice of such a violation from a Third Party. Such reports shall be made to the PO and to the IO as promptly as possible after discovery of a known or suspected violation. Digital Promise shall treat each such report with confidentiality to the extent permitted with respect to the reporting individual.

5.2. Content of Report

Reports of known or suspected violations should include all of the following to the full extent known:

- Names and locations of persons, databases, and systems involved with the incident;
- Nature and description of the incident, including the type and extent of NPI involved;
- Approximate date and time of the incident;

- Date and time that the person making the report initially learned of the incident, or otherwise Digital Promise's first time of knowledge; and

- Contact information for the person making the report and any other persons who were involved in identifying the incident.

5.3. Complaints By Individuals Regarding Privacy Protection

Complaints by individuals regarding respect for their data privacy rights should be referred to the PO. All such complaints shall be documented by the PO and shall be investigated to the extent necessary to determine whether and what remedial action may be warranted. Confidentiality will be maintained throughout the investigatory process to the extent consistent with adequate investigation and appropriate corrective action.

5.4. Responsive Action

Violations of this Policy by Digital Promise Representatives could result in disciplinary action up to and including termination of employment, termination of a work assignment or contract, as applicable, and/or legal action. When deemed appropriate, the CEO may report violations of this Policy to appropriate outside organizations, including law enforcement authorities.

6. QUESTIONS REGARDING THIS POLICY

Each Digital Promise Representative has the affirmative obligation to raise questions if he or she is in doubt about the scope, content, meaning, or application of any element of this Policy. Questions should be presented to the PO.

7. UPDATES TO POLICY

Digital Promise reserves the right, at its discretion, to change, modify, add, or remove portions of this Policy at any time.