Adopted: June 16, 2020

Laconia School District: Information Governance Plan

1. Generally:

1.1 *Scope*: This Plan governs all aspects of the handling (*e.g.*, creation, receipt, acquisition, storage, maintenance, access, use, disclosure, transmission, transportation, disposal, and destruction) of Protected Information that either belongs to the District or is within its possession, custody or control. This Plan applies to all Information Systems and Electronic Devices owned or managed by the District. This Plan also applies to all Employees, Volunteers, and Contractors of the District who have access to or possession, custody or control of Protected Information. This Plan does not apply to Students or Family Members, unless and to the extent such Student or Family Member is an Employee, Volunteer, or Contractor as set forth above, provided that Protected Information includes information about Students and Family Members. Only an Information Security Officer may authorize a deviation from this Plan, and only to the extent that such a deviation is necessary or appropriate and permitted by Applicable Law.

1.2 *Protected Information*: This Plan covers Protected Information, which consists of Protected Personal Information (PPI), Protected Health Information, and other information that the District designates as Protected Information. While those terms are defined below in the Definitions of this Plan, they generally include certain information identifiable to Students, Family Members, and Employees, such as contact information (e.g., address, email, phone, etc.), passwords, social security numbers, governmental identification, date and place of birth, health information, genetic and biometric information, credit cards, insurance information, financial account information, personnel information, and certain other information that identifies or is identifiable to a Student, Family Member, or Employee.

Responsibilities of Employees and Volunteers

2.1 *Minimum Access*: Employees and Volunteers may handle Protected Information only if and to the extent doing so is necessary or appropriate for them to perform their duties for the District and permitted by this Plan. In doing so, Employees and Volunteers will handle only the minimum amount of Protected Information necessary or appropriate for them to perform those duties, and will not permit any other Person to handle Protected Information if or to the extent that Person is not authorized to do so under this Plan.

2.2 *Disclosure of Protected Information*: Employees and Volunteers may disclose Protected Information only to the following Persons and only under the following circumstances: (a) other Employees, Volunteers, and Contractors if necessary or appropriate for them to perform their duties for the District and permitted by this Plan; and (b) the Person about whom the Protected Information pertains and any other Person who that Person authorizes the District to disclose such Protected Information to, but only Protected Information related to that Person or the authorized representation of that Person. A Security Officer may disclose Protected Information, and authorize the disclosure of Protected Information, to other Persons to the extent necessary or appropriate and permitted by Applicable Law.

2.3 *Awareness and Training*: Employees and Volunteers will (a) acquire and maintain an awareness about the types of Protected Information they are authorized to handle and their authority and responsibility with respect to it, and (b) participate in the training provided to them by the District to safeguard Protected Information.

2.4 *Use of Electronic Devices and Accounts*: Employees and Volunteers may handle

Protected Information only using Information Systems and Electronic Devices covered by this Plan. Employees and Volunteers may not handle Protected Information using a personal Electronic Device, unless that personal Electronic Device is specifically covered by this Plan. Employees and Volunteers may not handle Protected Information using a personal online or electronic account, including any personal email, webmail, social media, or cloud storage account, unless expressly authorized to do so by a Security Officer.

2.5 *Use of Applications*: Employees and Volunteers may handle Protected Information using software, programs, and other applications (including online applications) only if and to the extent the District provides such applications to Employees and Volunteers to do so, or a Security Officer expressly authorizes the use of such application to do so.

2.6 *Transmission of Protected Information*: Employees and Volunteers may transmit Protected Information beyond the District's email domain or firewall by email, file transfer protocol, or other means of digital, analog, or electronic transmission only if the entire transmission or the Protected Information in the transmission is Encrypted.

2.7 *Transportation of Protected Information*: Employees and Volunteers may transport Protected Information outside of the District's facilities only (a) if in electronic format, the Electronic Device used for the transportation, or the Protected Information being transported, is Encrypted and (b) if in hard copy format, the Protected Information is transported in a container and manner appropriate to the nature and scope of the Protected Information being transported.

2.8 *Storage of Protected Information*: Employees and Volunteers will store Protected Information in electronic format only on Information Systems and Electronic Devices covered by this Plan. Employees will store Protected Information in electronic format on the District's Information Systems and Electronic Devices only in the file, database, or other application designated or appropriate for such Protected Information. Employees will store Protected Information in hard copy format only in a filing drawer or cabinet, or filing or storage room, at the District's facilities that is secured during non-working hours and whenever the Protected Information is not being supervised by an Employee or Volunteer authorized to access such Protected Information. If an Employee receives Protected Information in electronic format on an Electronic Device and the Electronic Device or the Protected Information on it are not Encrypted, either (a) the Electronic Device will be stored in a filing drawer or cabinet or filing or storage room that is secured during non-working hours and whenever the Protected Information is not being supervised by an Employee or Volunteer authorized to access such Protected Information, or (b) the Protected Information will be transferred either to a District Information
System or to an Electronic Device that is Encrypted, and the original unencrypted Electronic Device is returned to the Person from whom the District received it or destroyed in compliance with this Plan.

2.9 *Printing of Protected Information*: Employees and Volunteers may print or otherwise generate Protected Information in hard copy format only if and to the extent (a) doing so is necessary or appropriate for them to perform their duties for the District, and (b) the hard copy information generated is stored, maintained, disposed of, destroyed, and otherwise handled in accordance with this Plan.

2.10 *Laptops and External Drives*: Employees and Volunteers may handle Protected Information on a Laptop or External Drive only if (a) a Strong Password or Biometric is required to access the Laptop or External Drive or the Protected Information on it, (b) the entire Laptop or External Drive, or the Protected Information on it, is Encrypted, and (c) the Laptop or External Drive is owned by the District; provided that (d) Volunteers who are members of the school board may handle Protected Information on a Laptop or External Drive that is not owned by the District as long as they comply with sub-paragraphs (a) and (b) of this paragraph.

2.11 *Tablets and Smartphones*: Employees and Volunteers may handle Protected Information on a Tablet or Smartphone only if (a) a Strong Password or Biometric is required to access the Tablet or Smartphone or the Protected Information on it, and (b) the entire Tablet or Smartphone or the Protected Information on it is Encrypted.

2.12 *Remote Access*: Employees and Volunteers may handle Protected Information maintained on the District's Information Systems using an Electronic Device that is outside of the District's firewall only if they do so (a) through a dual authentication system maintained by the District, and (b) the transmission is Encrypted.

2.13 *Usernames, Passwords and Security Codes*: Employees and Volunteers may not use the username, password, or security code of any other Person to access any District security system, facility, Information System, or Electronic Device, unless expressly authorized to do so by a Security Officer. Employees may not permit any other Person to use their username, password, or security code to access any District security system, facility, Information System or Electronic Device, unless expressly authorized to do so by a Security Officer.

2.14 *Destruction and Disposal*: Employees and Volunteers will dispose of Protected Information in hard copy format only pursuant to paragraph 5.4. Employees and Volunteers will dispose of and destroy Protected Information in electronic format, and Information Systems and Electronic Devices that contain Protected Information, only pursuant to paragraph 4.15.

2.15 *Breaches*: Employees and Volunteers will not engage in any conduct that they know, or suspect may cause an actual or potential Breach. Employees and Volunteers will inform a Security Officer if they have reason to believe that an actual or potential Breach has occurred, will occur, or may occur, and will inform a or Security Officer of any circumstance or Person that they believe presents or may present a threat or risk to the security of Protected Information. Employees and Volunteers will cooperate with all investigations and other measures to address an actual or potential Breach of Protected Information.

2.16 *Questions and Concerns*: Employees and Volunteers will inform a Security Officer of any questions or concerns they have about Protected Information, this Plan, or Applicable Law.

2.17 *Cooperation and Participation*: Employees and Volunteers will cooperate with all practices, procedures, policies, programs, systems, and other measures under this Plan or implemented by the District to safeguard Protected Information.

2.18 *Discipline*: Employees and Volunteers will be subject to discipline, including termination, for failing or refusing to comply with this Plan, Applicable Law, or any related request or instruction made by the District or a Security Officer.

Administrative Safeguards

3.1 *General Duties*: Information Security Officer(s) have the authority and responsibility to (a) interpret, implement, and enforce this Plan, (b) develop additional policies about Protected Information, (c) develop, implement, and enforce new and additional security practices, and (d) generally ensure the District's compliance with this Plan and Applicable Law.

3.2 *Periodic Reassessment*: The District will conduct, or retain qualified Contractors to conduct, periodic internal and external vulnerability scanning and risk assessments to determine what Protected Information the District has, whether to modify or expand the scope of Protected Information, whether the District is subject to any new, additional, or reoccurring risks to Protected Information, whether the District should implement any new or additional measures to mitigate such risks and, if so, the measures that the District should implement. Based on that reassessment, the District will take steps to implement the measures that the District determines it should implement,

and to modify and amend this Plan if necessary or appropriate. The District will maintain records memorializing the assessments performed by the District and any other matters related to this Plan.

3.3 *Training*: Following the adoption of this Plan and periodically thereafter, the District will train Employees and Volunteers about their authority and responsibility under this Plan and Applicable Law. During the orientation of new Employees and Volunteers, the District will train them concerning their authority and responsibility under this Plan and Applicable Law. The Security Officers will maintain records of such trainings.

3.4 *Employees and Volunteers*: Before hiring or promoting a Person to be an Employee with access to Protected Information or permitting a Volunteer to have access to Protected Information, a Security Officer or Employee designated by a Security Officer will obtain background information or reports (as necessary or appropriate to the type or level of access that Person will have to Protected Information), including (to the extent necessary or appropriate) information about criminal, driver, and credit history (if applicable).

3.5 C*ontractors*: Before the District retains any Person to be a Contractor, the Information Security Officer, Superintendent and/or Assistant Superintendent will determine the extent to which the District must conduct due diligence with respect to such Person given the nature and scope of the Person's anticipated handling of Protected Information, and will direct such due diligence. Before providing Protected Information to any Contractor, a Security Officer will ensure that, if possible, the District enters into an appropriate confidentiality and information security agreement with the Contractor.

3.6 *Incident Response*: The District will create and maintain an incident response plan that includes at least the following: in the event of an actual or potential Breach, a Security Officer will initiate and direct a process to (a) determine if a Breach has occurred and, if so, the nature and extent of Protected Information affected, (b) notify the District's counsel and insurance carriers and cooperate with counsel and the carriers concerning the incident, (c) identify the individuals affected by the incident and Persons that the District should notify about the Breach, (d) determine the steps that the District should take in response to the incident, and initiate and supervise such activities; (e) determine if the District should implement measures to mitigate any risk to Protected Information related to the incident or any other risk discovered during the process and, if so, implement such measures, (f) determine if the District should take any disciplinary or other action related to the incident and, if so, take such action, (g) determine if the District should modify this Plan or provide additional training about Protected Information and, if so, modify this Plan and provide such training, (h) determine if the District should take any other action related to the incident and, if so, take such action, and (i) prepare and retain records memorializing the process and outcome.

3.7 *Record Retention*: The District will retain all records, logs, and other documents that are required, necessary, or appropriate to be retained under this Plan or Applicable Law for at least six years after creation of the record.

3.8 *Insurance*: The District will maintain commercially reasonable insurance providing coverage for a Breach of Protected Information.

Technical Safeguards

4.1 *Access Control*: The District will implement technological measures that (a) limit access to the District's Information Systems and Electronic Devices that contain Protected Information to only Employees and Volunteers who need access to such Protected Information to perform their duties for the District, and (b) to the extent feasible, limit access of Employees and Volunteers to only the Protected Information that they need to perform their duties for the District. The District will periodically review the access that Employees and Volunteers have to Protected Information and modify such access to the extent necessary or appropriate to do so. The District will

investigate and, if reasonable, implement network access control technological to limit access to the District's Information Systems that contain Protected Information to only Electronic Devices, Tablets, and Smartphones that are either owned by the District or registered with the District's Information Systems.

4.2 *System and Device Configuration*: The District will control the operating systems, settings, executable applications, security applications, and other configuration of all Information Systems and Electronic Devices owned or managed by the District. Only certain Security Officers, and Employees designated by a Security Officer, may have ability to alter such operating systems, settings, executable applications, security applications, and other configurations. The District will disable or restrict systems, applications, functions, services, and ports on all District Information Systems and Electronic Devices that are not necessary or appropriate for Employees or Volunteers to perform their duties for the District.

4.3 *Laptops and External Drives*: The District will provide Laptops and External Drives to Employees and Volunteers (other than members of the school board) who need to have Protected Information on a Laptop or External Drive to perform their duties for the District. The District will ensure that all Employees and Volunteers use either a Strong Passwords or Biometric to access such Laptops and Electronic Devices, and that such Laptops and External Drives, or the Protected Information on them, are Encrypted. The District will investigate and, if reasonable, implement technology that permits the District to remotely locate and manage the District Laptops.

4.4 *Tablets and Smartphones*: The District will implement mobile device management technology that maintains Protected Information in an Encrypted format on Tablets and Smartphones that are not owned by the District.

4.5 *Applications*: The District will investigate and, if reasonably, implement technological controls that restrict or prevent Employees and Volunteers from using software, programs, or other applications (including online applications) to handle Protected Information, unless the District has reviewed the application and provides it to Employees and Volunteers to do so, or a Security Officer has reviewed and approved the application for such use.

4.6 *Usernames and Passwords*: The District will implement technology that requires Employees and Volunteers to have a unique username and either a Strong Password or Biometric to access the District's Information Systems and Electronic Devices. Passwords or Biometrics will be changed if may have been or known to have been compromised in any manner, and that such Strong Passwords are different from the previous ten used by the Employee/Volunteer. The District will ensure that the District's Information Systems and Electronic Devices have software implemented that requires the use of the Strong Password or Biometric to access the device if it has been inactive for 30 minutes or longer. Promptly after an Employee or Volunteer ceases to be employed by or perform services for the District, the District will revoke that Employee's and Volunteer's usernames, passwords, and Biometrics. The District will revoke the usernames, passwords, and Biometrics for any Employee or Volunteer as soon as the District becomes aware that the Employee or Volunteer presents any threat to Protected Information. The District will require Employees and Volunteers to have passwords or Biometrics to access Tablets and Smartphones that contain Protected Information.

4.7 *Remote Access*: The District will implement a virtual private network with dual authentication and Encrypted transmission that permits Employees and Volunteers to access Protected Information using an Electronic Device that is outside the District's firewall. To the extent feasible, the District will configure all District Laptops to automatically connect to that virtual private network whenever they are outside the District's firewall.

4.8 *Inventory*: The District will maintain an inventory of all District Information Systems and Electronic Devices that contain or may contain Protected Information, and all software, programs, and other applications that Employees or Volunteers use or may use to handle Protected Information. Before issuing any Electronic Device to an Employee or Volunteer, the District will ensure that all Protected Information on the Electronic Device is removed

from it in accordance with National Institute of Standards and Technology Special Publication 800-88, if the removal of Protected Electronic Information is appropriate.

4.9 *Information Systems*: The District will ensure that all servers and other network equipment that support the District's Information Systems and contain Protected Information are maintained either (a) in a limited access secure room with appropriate environmental and disaster controls in a facility owned or controlled by the District, or (b) offsite with a Contractor. The Security Officers will ensure that the District conducts appropriate due diligence and obtains an appropriate confidentiality and information security agreement with such Contractors.

4.10 *Updating*: Only Security Officers, and Employees designated by a Security Officer may maintain and update Information Systems and Electronic owned or managed by the District, and applications on such Information Systems and Electronic Devices. To the extent feasible, the District will use the automatic updating functionality of commercially available software. If not feasible, the Security Officers will ensure that, no less than once every month, or more frequently if necessary or appropriate under the circumstances, the District will manually update software on the District's Information Systems and Electronic Devices.

4.11 *Protective Systems*: The District will implement and maintain up-to-date, commercially reasonable systems to safeguard Protected Information, including a firewall, intrusion and threat detection and prevention software, and anti-virus, anti-malware, and antispyware software on the District's Information Systems and Electronic Devices. The District will implement and maintain software and systems that detect multiple failed attempts to log-on to the District's Information Systems and Electronic Devices, and disable the account being used to attempt to log-on.

4.12 *Logs*: The District will implement and maintain up-to-date, commercially reasonable software and systems that log activities on the District's Information Systems and Electronic Devices. The District will investigate and, if reasonable, implement a security information event management system to aggregate and monitor security information and logs, and automatically alert the District in the event of a threat to Protected Information.

4.13 *Administrators and Software Installation*: Employees and Volunteers generally will not be administrators of any District Information System or Electronic Device. Only certain Security Officers, and Employees designated by a Security Officer, may be an administrator. Any Security Officer or Employee who is an administrator will also have a different username and password for non-administrator activities and will use the administrator credentials only to perform administrator activities. Administrator usernames and passwords will be given to a designated Security Offices and, if stored electronically, Encrypted. Employees and Volunteers, including administrators, may not download executable software to the District's Information Systems or Electronic Devices without prior express approval of the designated Security Officer.

4.14 *Transmission of Protected Information*: The District will implement and maintain technology that enables the transmission of Protected Information in electronic format, including by email and by file transfer protocol, in an Encrypted format.

4.15 *Transportation of Protected Information*: The District will implement and maintain technology that enables the transportation of Protected Information on Electronic Devices, including Laptops and External Drives, in an Encrypted format.

4.16 *Destruction of Protected Information*: If the District destroys electronic Protected Information, or Information Systems or Electronic Devices containing electronic Protected Information, it will do so pursuant to National Institute of Standards and Technology Special Publication 800-88. The Security Officers will ensure that, if the District retains a Contractor to do so, the District contractually requires the provider to do so in compliance with National Institute of Standards and Technology Special Publication 800-88.

4.17 *Disaster*: The District will create and maintain back-ups of electronic Protected Information, will be able to restore and use electronic Protected Information within a reasonable time after a disaster affecting the District's Information Systems, and will be able to continue critical business operations involving electronic Protected Information during and after an emergency or mass failure of the District's Information Systems.

Physical Safeguards

5.1 *Facility Security*: Access to the District's physical facilities that contain Protected Information will be limited to Employees, Volunteers, and other Persons with authority to access such Protected Information. During non-working hours, the District's physical facilities that contain Protected Information will be protected by physical security measures that are appropriate to the Protected Information within the facilities. Promptly when Employees and Volunteers cease to be employed by or perform services for the District, the District will recover all access codes, cards, and keys from such Employees and Volunteers.

5.2 *Storage*: The District will provide lockable or otherwise secure filing drawers or cabinets or filing or storage rooms for the storage of Protected Information in hard copy format at the District's facilities. All Protected Information in hard copy format will be stored and locked in such filing drawers or cabinets or filing or storage rooms during non-working hours and whenever the Protected Information is not being supervised by an Employee or Volunteer authorized to access such Protected Information. Any Protected Information in hard copy format stored at an off-site facility will be stored only in appropriately secure facilities of a Contractor. The Security Officers will ensure that the District conducts appropriate due diligence and obtains an appropriate confidentiality and information security agreement with such Contractors.

5.3 *Transportation of Protected Information*: The District will transport Protected Information in hard copy format only in a secure container or other method of transportation appropriate to the nature and scope of the Protected Information transported.

5.4 *Disposal and Destruction of Protected Information*: The District will provide Employees and Volunteers with receptacles for the disposal of Protected Information in hard copy format. The District will retain a Contractor to destroy Protected Information in hard copy format and contractually require the Contractor to do so in a manner that renders it essentially unreadable and indecipherable, such as by cross-shredding, incinerating, or pulverizing.

Definitions

The following definitions apply to this Plan. If a term used in this Plan is not specifically defined here, the definitions in Applicable Law may be used to interpret this Plan.

Applicable Law: "Applicable Law" means (a) New Hampshire Revised Statutes Annotated Section 189, Paragraphs 65, VII and VII-a and 66, V; (b) New Hampshire Revised Statutes Annotated Chapter 359-C, Paragraph19 *et seq.*, and (c) all other local, state, federal, and international laws and regulations applicable to Protected Information.

Biometric: "Biometric" means any method by which a Person can be uniquely identified using one or more distinguishing biological trait, including fingerprint, facial geometry, hand geometry, earlobe geometry, retina or iris pattern, and voice wave.

Breach: "Breach" means the handling of Protected Information without authorization, beyond the scope of authorization, or in a manner or to an extent that compromises Protected Information or violates Applicable Law. A Breach does not include the handling of Protected
Information that is Encrypted, as long as the decryption key also has not been compromised. A Breach also does not include (a) the unintended or good faith handling of Protected Information by an Employee, Volunteer, or Contractor related to fulfilling their duties for the District or (b) the disclosure of Protected Information by an Employee, Volunteer, or Contractor to another Employee, Volunteer, or Contractor, as long as the Protected Information is not otherwise further handled without authorization, beyond the scope of authorization, or in a manner or to an extent that compromises the Protected Information or violates Applicable Law.

Contractor: "Contractor" means any Person, not an Employee or Volunteer, who performs or assists in performing a function or activity for the District involving the handling of Protected Information or involving any other function or activity for the District regulated by Applicable Law.

"District" means New Hampshire School Administrative Unit 30, known as the Laconia School District, all schools operated by the District, and all other educational, vocational, business, and other operations of the District.

Electronic Device: "Electronic Device" means any digital, analog, or electronic machine, device, system, account or service used to create, receive, acquire, store, maintain, access, use, disclose, transmit, transport, analyze, or manipulate computerized or electronic data, including servers, routers, networks, hubs, switches, desktop computers, Laptops, Tablets, handheld computers, Smartphones, cellphones, electronic readers, music players, internal and External Drives, USB drives, digital cameras and video recorders, photo and video storage media, compact discs, digital video discs, other data storage media, digital telephone and voicemail systems, photocopiers, calculators, cloud storage, social media, micro-blogs, and blogs.

Employee: "Employee" means a Person employed by the District, but not a Contractor or Volunteer.

Encrypted: "Encrypted" means to transform data through use of an algorithmic process into a form where there is a low probability of assigning meaning to the data without the use of a confidential process, key, security code, access code, or password; provided that this term shall not include data acquired in combination with, or accessed or acquired using, the process, key, security code, access code, or password that permits access to the data, or data acquired where the process, key, security code, access code, or password has been Breached.

External Drive: "External Drive" means a digital, analog, or electronic machine or device external to a computer used to handle computerized or electronic data, including external hard drives, USB drives, photo and video storage media, compact discs, and digital video discs.

Family Member: "Family Member" means the spouse, guardian, biological or adoptive parent or grandparent, step-parent, step-grandparent, sibling, child, or grandchild of a Student.

Information Security Officer: The "Information Security Officer(s)" is designated by the District's Superintendent. The District has the discretion to designate, at any time and for any reason, a different or an additional Employee to serve as the Information Security Officer(s), or to assist the Information Security Officer.

Information Systems: "Information Systems" means a system of Electronic Devices used to handle electronic data, or online cloud storage or computing services to handle such data.

Laptop: "Laptop" means a computer designed to be transported from place-to-place by the user or that the user routinely transports from place-to-place, other than Tablets, Smartphones, and External Drives.

Person: "Person" means any individual or entity, including a sole proprietorship, partnership, corporation, limited liability company, limited liability partnership, professional association, professional corporation, S corporation, and any other entity whatsoever.

Plan: "Plan" means this Information Security Plan, and all predecessors, successors, additions, modifications, amendments, addenda, and appendices to this Plan.

Protected Health Information: "Protected Health Information" means (a) any information related to any physical or mental health or condition of an individual, the provision of health care to the individual, or the payment for health care for an individual, where (b) that information specifically identifies the individual, or there is a reasonable basis to believe that the information can be used to identify the individual.

Protected Information: "Protected Information" means Protected Health Information, Protected Personal Information, and any other information that the District or a Security Officer designates as Protected Information.

Protected Personal Information (PPI): "Protected Personal Information" means:

(a) with respect to a Student or Family Member, the (i) name or address of the Student or Family Member, (ii) any information that identifies the Student or Family Member, including date of birth, place of birth, social security number, email account or address, social media account or address, other electronic or online account or address, telephone or cellphone number, credit card account or number, insurance account or number, or financial services account or number, or (iii) any other information that, alone or in combination with other information, is linked to or linkable to a specific Student or Family Member that would allow a reasonable person in the school community to identify that Person with reasonable certainty;

(b) with respect to an Employee, the Employee's (i) social security number, (ii) date of birth, (iii) residential address, email account or address, or telephone or cellphone number, (iii) personnel information, including performance evaluations, (iv) any other information that, alone or in combination with other information, is linked to or linkable to a specific Employee that would allow a reasonable person in the school community to identify the Employee with reasonable certainty, and (v) any other information about an Employee that is requested by a Person knows or may know the identity of such Employee; and (c)with respect to all individuals, (i) the last name of an individual, together with that individual's first name or the first initial of the first name, in combination with (ii) any of the following for that individual (A) social security number, (B) governmental identification, including driver's license, non-drivers identification, passport, military identification, Medicaid or Medicare identification, etc., (C) bank, credit, debit, insurance, investment, or other financial account number, with or without any username, password, personal identification number, or other code necessary to access or control such account, (D) password, personal identification number, or other code used to access or control any bank, credit, debit, insurance, investment, or other financial account, (E) genetic and Biometric information, and (F) global positioning information; provided that this term does not include any information that is generally publicly available, including from any local, state or federal governmental record, as long as such information did not become generally publicly available through the violation of a Person's obligation to maintain the confidentiality of that information, including pursuant to this Plan, Applicable Law, or an applicable contract. (Also referred to as Personally Identifiable Information PII)

Security Officers: "Security Officer(s)" are District designees, appointed by the Information Security Officer, that may act on their behalf.

Smartphone: "Smartphone" means a handheld digital, analog, or electronic device used to handle electronic data, including iPhones, Droid phones, Google phones, Blackberries and other cellular phones, other than Laptops, External Drives, and Tablets.

Strong Password: "Strong Password" means either (a) a string of not less than 8 characters consisting of a combination of at least one upper case letter, one lower case letter, and either one number or symbol, or (b) a phrase of not less than four distinct and unrelated words consisting of not less than five characters per word.

Student: "Student" means either a Person who is a current or prospective enrollee in a school or other educational or vocational program or operation of the District.

Tablet: "Tablet" means a portable digital, analog, or electronic device used to handle electronic data, including iPads, Droid tablets, Google tablets, and electronic readers, other than Laptops, External Drives, and Smartphones.

Volunteer: "Volunteer" means any Person that performs services for or on behalf of the District without compensation, including, but not limited to, parents and family members of students and members of the school board.