NORTH PROVIDENCE SCHOOL DEPARTMENT CONFIDENTIALITY OF INFORMATION POLICY	Approved: 8/25/2021

I. PURPOSE

This policy provides notice to staff, parents, and students of the District's expectations that confidential information shall not be inappropriately accessed, used, viewed, shared or disclosed by District staff unless authorized by written District protocol, procedure or otherwise authorized by senior administrators.

In the normal course of operating a school district, staff will unavoidably receive and handle, learn of or have access to, personal, private and/or confidential information about students, parents, co-workers, the District and/or other third parties.

Disclosure of such personal, private and/or confidential information is prohibited by federal and state law and regulation and District policy. To ensure the privacy rights as set out herein, the District will take steps, including disciplining staff for improperly disclosing information and/or failing to protect the privacy interests of our students, parents, employees, the District and/or other third parties, consistent with state and federal law and District policy.

II. SCOPE

This policy applies to all staff, who may have access to confidential information, including those that are both employees and residents of the Town of North Providence[1].

III. POLICY

DEFINITIONS

Confidential information

Unpublished financial information, personally identifiable information or any other type of information held or stored by the District. Confidential information also includes any information entitled to protection under any applicable federal or state law or regulation as confidential, any educational record[2] and/or any other

[1] ***Residency in the Town of North Providence does not in any way release a District employment from the confidentiality requirements as set by this District.***

[2] Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and

information the District designates as confidential and/or any data or information in the following categories:

- Application Technology Meta Data.
- Application Use Statistics.
- Assessment(s).
- Attendance.
- Communications.
- Conduct or behavioral data.
- Demographic data including but not limited to race, color, religion, ancestral origin, sex, sexual orientation, gender identity or expression, age, disability, marital status, citizenship, genetic information.
- Enrollment data including student school enrollment, student grade level, guidance counselor or educators or service providers, curriculum programs or requests or receipt of services, year of graduation.
- Parent/Guardian Contact Information including address, email, or phone numbers.
- Parent/Guardian or student ID identifications including any student or parent ID numbers (created to link parents to students); Parent/Guardian Name, First and/or Last.
- Special Indicators such as English language learner information.
- Schedule information including student or staff scheduled courses, services or activities.
- Teacher names.
- Income status.
- Medical alerts/ health data.
- Student data[3].

---

of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

[3] Student Data includes any data that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student disability information. Specialized education services (IEP or 504). Living situations (homeless/foster care). Student, parent, or staff contact information. Student Identifiers including Local (School district) ID number, State ID number, Provider/App assigned student ID number, Student app username, Student app passwords. Student Name First and/or Last. Student Program Membership or engagement in academic or extracurricular activities or transcript data. Student Survey Responses. Student work Student generated content; writing, pictures, etc. Student transportation information including student bus assignments, student pick up and/or drop off location or student bus card ID number.

- All other student, or parent or staff personal or employment information of any type not otherwise proscribed as public information by the Rhode Island State Access to Public Records Act or other state or federal law all as amended from time to time.

Senior Administrator

The Superintendent of Schools, the Assistant Superintendent of Schools, the Director of Student Services, the Director of Finance, the Director of Human Resources, a school principal, or any other individual with such authority as designated by the Superintendent or as otherwise specified in written District Policy or protocol.

Unauthorized Third Party

Any individual or entity employed or not employed by the District who does not have a legitimate educational interest in the confidential information.[4]

EMPLOYEE MAINTENANCE OF CONFIDENTIAL INFORMATION

- Never access or use any confidential information for any purpose without authorization from a supervisor.
- *Never disclose confidential information to another colleague, co-worker, staff member, student, parent, or any other Unauthorized Third Party without prior authorization of senior administrators*
- Never for benefit or profit from disclosure of confidential information.
- Never replicate confidential documents and files and/or store them on unsecure devices.
- Never access, keep, or use confidential information from or on a non-district designated device.
- Never disclose confidential information inconsistent with this policy or District protocol.
- Never obtain, access, keep, use, or view confidential information which you are not authorized to view or possess.
- Lock or secure confidential information at all times.
- Destroy confidential information when the information is no longer needed in compliance with District, Municipal, State and/or Federal record retention laws.
- Keep confidential documents inside your work environment.
- Take reasonable steps to ensure that confidential material is never left in plain view or otherwise unsecured.
- Ensure that any confidential information in a digital format is only viewed on secure District issued and authorized devices.
- Surrender all confidential documents and material to the District upon leave, resignation, termination or at any time upon the request of their supervisor.
- Take reasonable steps to ensure that you do not mistakenly disclose any confidential information to any unauthorized persons in or outside the District.
- Immediately report any inadvertent disclosures of confidential information to their direct supervisor as soon as possible.

[4] 34 CFR §99.31(a)(1).

- Immediately notify a Senior Administrator of any suspected inappropriate access, viewing, release or distribution of confidential information.
- Immediately report any discovered or known breach of this policy to a senior administrator.
- All staff shall comply with a clean desk protocol which requires:
    - Maintenance of a desk clean of any confidential information when such information is not being actively worked on and store and lock all confidential information.
- Use provided encryption on all confidential electronic information and safeguard databases as provided by the District.
- Execute a District adopted non-disclosure of confidential information agreement (NDA).
- Fully comply with all District confidential measures.
- When in doubt, always ask for authorization by senior administrators to allow access or release of confidential information.

DISTRICT CONFIDENTIALITY MEASURES

The District may take certain measures to ensure that confidential information is well protected. Such measures may include:

- Issuing protocol and procedures from time to time;
- Requiring appropriate professional development of particular or the entire staff;
- Requiring staff to execute an acknowledgement that staff members have read and understand this policy;
- Requiring that staff execute a District non-disclosure of confidential information agreement.

DISCIPLINARY CONSEQUENCES

The District has the expectation that this policy will be followed and will investigate every breach. An intentional violation of this policy or any other related policy is considered a serious infraction. Depending on the severity of the infraction, a staff member may face disciplinary action up to and including termination of the employment relationship without regard to corrective discipline and, possibly, other legal action. The District may also discipline for any unintentional breach of this policy depending on its frequency and/or seriousness.

This policy is binding on all staff, regardless of residency, even after separation of employment with the District.

Approved: 8/25/2021