Data Privacy & Security Policy

I. Purpose

This policy addresses Bold Charter School's responsibility to adopt appropriate administrative, technical and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its data, data systems and information technology resources.

II. Policy Statement

It is the responsibility of Bold Charter School:

(1) to comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information;
(2) to maintain a comprehensive Data Privacy and Security Program designed to satisfy its statutory and regulatory obligations, enable and assure core services, and fully support the school's mission;
(3) to protect personally identifiable information, and sensitive and confidential information from unauthorized use or disclosure;
(4) to address the adherence of its vendors with federal, state and SED requirements in its vendor agreements; and
(5) to communicate its required data security and privacy responsibilities to its users, and train its users to share a measure of responsibility for protecting SED's data and data systems.

III. Standard

Bold Charter School will utilize the National Institute of Standards and Technology's Cybersecurity Framework v 1.1 (NIST CSF or Framework) as the standard for its Data Privacy and Security Program.

IV. Scope

The policy applies to Bold employees, interns, volunteers, and consultants, and third-parties who receive or have access to Bold's data and/or data systems ("Users").

This policy encompasses all systems, automated and manual, including systems managed or hosted by third parties on behalf of Bold and it addresses all information, regardless of the form or format, which is created or used in support of the activities of Bold.

This policy shall be published on the Bold website and notice of its existence shall be provided to all Users.

V. Compliance

Deputy Commissioners of Education are responsible for the compliance of their programs and offices with this policy, related policies, and their applicable standards, guidelines and procedures. Instances of non-compliance will be addressed on a case-by-case basis. All cases will be documented, and program offices will be directed to adopt corrective practices, as applicable.

VI. Oversight

Bold's Chief Privacy Officer shall annually report to the Board of Trustees on data privacy and security activities, the number and disposition of reported breaches, if any, and a summary of any complaints submitted pursuant to Education Law §2-d.

VII. Data Privacy

(1) Laws such as the Family Educational Rights Privacy Act (FERPA), NYS Education Law §2-d and other state or federal laws establish baseline parameters for what is permissible when sharing student PII.

(2) Data protected by law must only be used in accordance with law and regulation and Bold policies to ensure it is protected from unauthorized use and/or disclosure.

(3) Bold has established a Data Governance Team to manage its use of data protected by law. The Chief Privacy officer and the Data Governance Team will, together with program offices,

determine whether a proposed use of personally identifiable information would benefit students and educational agencies, and to ensure that personally identifiable information is not included in public reports or other public documents, or otherwise publicly disclosed;

(4) No student data shall be shared with third parties without a written agreement that complies with state and federal laws and regulations. No student data will be provided to third parties unless it is permitted by state and federal laws and regulations. Third-party contracts must include provisions required by state and federal laws and regulation.

(5) The identity of all individuals requesting personally identifiable information, even where they claim to be a parent or eligible student or the data subject, must be authenticated in accordance with Bold procedures.

(6) It is Bold's policy to provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes. Therefore, Bold shall ensure that its contracts require that the confidentiality of student data or teacher or principal APPR data be maintained in accordance with federal and state law and this policy.

(7) Contracts with third parties that will receive or have access to personally identifiable information must include a Data Privacy and Security Plan that outlines how the contractor will ensure the confidentiality of data is maintained in accordance with state and federal laws and regulations and this policy.

VIII. Incident Response and Notification

The Department will respond to data privacy and security incidents in accordance with its **Incident Response Policy.** The incident response process will determine if there is a breach. All breaches must be reported to the Chief Privacy Officer. For purposes of this policy, a breach means the unauthorized acquisition, access, use, or disclosure of student, teacher or principal PII as defined by Education law §2-d, or any Bold sensitive or confidential data or a data system that stores that data, by or to a person not authorized to acquire, access, use, or receive the data.

Bold will comply with legal requirements that pertain to the notification of individuals affected by a breach or unauthorized disclosure of personally identifiable information.

IX. Acceptable Use Policy, User Account Password Policy and other Related Department Policies

(1) Users must comply with **NYSED's Information Security Policy**, which outlines the responsibilities of all users of SED information systems to maintain the security of the systems and to safeguard the confidentiality of SED information.
(2) Users must comply with the **Acceptable Use of IT Resources Policy** in using Department resources. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with SED's mission and business functions.
(3) Users must comply with the **User Account Password Policy**.
(4) All remote connections must be made through managed points-of-entry in accordance with the **Data Privacy and Security Guidelines for Remote Work and Telecommuting Policy**.

X. Training

SED Users must annually complete SED's information privacy and security training.