

CEREBRAL PALSY OF WESTCHESTER

<u>DIVISION:</u> Information Tech, Corporate Compliance	<u>PROGRAMS:</u> School, Pre School	<u>RESPONSIBLE FOR INTERPRETATION:</u> Data Protection Officer Program Directors	<u>EFFECTIVE:</u> 02/11/2021	<u>PAGE:</u> <u>1</u> of 3
---	--	--	--	--------------------------------------

Data Privacy and Security

Adapted from the NYSED Data Privacy and Security Policy dated 10/01/2020.

I. PURPOSE:

This policy addresses Cerebral Palsy of Westchester's (CPW'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 CPW:

- (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 Department's mission.
- (3) to protect data* 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 CPW's data and data systems.

III. SCOPE:

The policy applies to CPW employees, interns, volunteers, and consultants, and third parties who receive or have access to CPW'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 CPW, and it addresses all information, regardless of the form or format, which is created or used in support of the activities of CPW.

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

IV. COMPLIANCE:

School and Pre-School Directors 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 reviewed by the Compliance & Privacy Coordinator, and addressed on a case-by-case basis. All cases will be documented, and program offices will be directed to adopt corrective practices, as applicable.

V. OVERSIGHT:

CPW's Compliance & Privacy Coordinator shall report to the Board of Directors at least annually 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, which addresses the

CEREBRAL PALSY OF WESTCHESTER

protection of student's data.

2 of 3

VI: 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 applicable laws, regulations, and SED and CPW policies, to ensure it is protected from unauthorized use and/or disclosure.
- (3) CPW has appointed a Data Protection Officer to manage its use of data protected by law. The Compliance & Privacy Coordinator and the Data Protection Officer, will, together with Program Directors, 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 SED and CPW procedures.
- (6) It is CPW'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, CPW shall ensure that its contracts require that the confidentiality of student data be maintained in accordance with federal and state law and this policy.
- (7) Contracts with third parties who 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.

VII: INCIDENT RESPONSE AND NOTIFICATION:

CPW will respond to data privacy and security incidents in accordance with its Investigation of Compliance Issues Policy and the NY SHIELD Act.

The incident response process will determine if there is a breach. All breaches must be reported to the Compliance & Privacy Coordinator. For purposes of this policy, a breach means the unauthorized acquisition, access, use, or disclosure of student, teacher or principal data as defined by Education law §2-d, or any CPW 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.

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

VII: Electronic Service and Internet Use Policy and Other Related CPW Policies:

- (1) Users must comply with the Electronic Service and Internet Use Policy, Laptop Agreement, Password Policy, Cell Phone Use Agreement, and the Email Encryption Policy, which outline the responsibilities of all users of CPW information systems to maintain the security of the systems and

CEREBRAL PALSY OF WESTCHESTER

to safeguard the confidentiality of CPW information.

- (2) Users must comply with the Electronic Service and Internet Use Policy, File Access Request Form, Data Restoration Request Policy, User Access and Security Review Policy & Financial Systems Users Access and Security Policy in using CPW 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 CPW's mission and business functions.
- (3) Users must comply with the Electronic Service and Internet Use Policy, Laptop Agreement, Password Policy, and Cell Phone Use Agreement.
- (4) All remote connections must be made through managed points-of-entry in accordance with the Remote Access Agreement and Laptop Agreement.

IX: TRAINING

Employees must annually complete CPW's Corporate Compliance Training, as well as the Cyber Security training. Initial Orientation provides IT security, passwords, email, files security (electronic and physical) and cell phone use training.

*Data: Personally identifiable information (PII or PHI), and sensitive and confidential information.

APPROVED BY:

Sinda Kudz

DATE:

2/11/21

PAGE:

3 of 3