UNITED
CHARTER HIGH SCHOOLS
Engaging Minds

United Charter High Schools - Data Security and Privacy Policy

The purpose of this document is to highlight key requirements followed by the United Charter High Schools (UCHS) around data privacy and data security. This policy will be posted on the UCHS's public website, provided to staff during onboarding and included in the annual data security and privacy training. Failure of UCHS staff members to follow this data privacy and data security policies may lead to disciplinary action including, but not limited to, termination and/or legal action. Please note this is not an exhaustive document as there are contractual, legal, and technology changes or exceptions that can affect this policy. Staff members affected by contractual, legal, technology changes or exceptions shall be informed and trained to maintain data security and privacy. This policy may be updated at any time to address changes in school practices, legal requirements, or changes to technology or services used by the school. Staff will be notified of data security and privacy policy updates/changes via electronic communication, print media, in person meetings, or during annual training. The updated/changed policy will also be posted to the UCHS's public website.

Definition of Terms

Data - 1) Factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation [1] 2) Pieces of information from which "understandable information" is derived[2].

Personally Identifiable Information (PII) - Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means[3].

Data Privacy - in this document refers to the relationship between the collection and dissemination of data which is considered personally indefinable information or considered confidential to UCHS.

Data Security - in this document refers to the processes, technology, and practices that are used to protect data.

Principle of Least Privilege - The principle that a security architecture should be designed

[1] "Data", Merriam-Webster Dictionary, Accessed June 9, 2020 https://merriam-webster.com/dictionary/data

[2] "Data - Glossary," CSRC (National Institute of Standards, December 2014), https://csrc.nist.gov/glossary/term/data.

[3] "PII - Glossary," CSRC (National Institute of Standards, July 2015), https://csrc.nist.gov/glossary/term/principle_of_least_privilege

so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function[4].

Third-Party vendor - (may also be referred to as contractor or consultant) Any person or entity that is not an employee of the school.

Confidential Data - Also called "Confidential Information". Any data, physical or electronic, that contains, but is not limited to, any information the school classifies as restricted or not meant for public release. Such data may include health data, sensitive organizational information, employment records, student information, or any other information required by law to be protected from unauthorized access or public dissemination. Includes but is not limited to data protected by federal, state, and local law.

Data Breach - Data that is physical or electronic media that has been accidentally or on purpose released or shared without authorization, accessed by unauthorized individuals or entities, or stolen.

Data Security and Data Privacy

1. UCHS will limit the collection of personally identifiable information to what is needed to carry out required tasks, services, or legal requirements.

2. Any collection or disclosure of students' personally identifiable information will only be done for the benefit of the student or UCHS through authorized secure sharing methods and with correct legal authorization.

3. UCHS shall not include student, teacher, or principal personally identifiable information in public-facing reports or documents unless proper legal authorization is received or such inclusion is required by law.

4. All UCHS employees must be familiar with school policies, laws, or regulations which apply to data they collect, access, or share.

5. All employees are required to report all data breaches, any unauthorized disclosure of data, or improper security practices to the respective school's Data Protection Officer including but not limited to:
    a. Improper sharing of user credentials
    b. Data breach of PII or confidential data
    c. Third-party vendor mishandling of data
    d. Unapproved applications or software use
    e. Improper physical or electronic confidential data storage

6. All employees are required to complete annual data security and privacy training

[4] "Principle of Least Privilege - Glossary," CSRC (National Institute of Standards, December 2016), https://csrc.nist.gov/glossary/term/principle_of_least_privilege

including but not limited to:

   a. Data security and privacy
   b. Security awareness
   c. School policies
   d. Breach reporting
   e. Laws and regulations

7. Employees are required to only use school-issued devices and accounts to store, access, or share school-owned data and services including but not limited to:
   a. Student data or files
   b. School owned documents
   c. Employee data or files
   d. School owned cloud Services

   The use of personal accounts including, but not limited to, Yahoo, Hotmail, AOL, Gmail, Dropbox, etc. is prohibited.

8. Employees are required to follow sharing and security practices as outlined in the UCHS Employee Handbook and the UCHS Charter Security Sign Off document.

Network and Data Storage

9. UCHS uses the National Institute of Standards and Technology(NIST) Cybersecurity framework 1.1 to create school security policies and procedures.

10. Data, where applicable, shall be maintained in accordance with federal, state, local laws, rules and regulations such as, but not limited to:
    a. Family Education Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
    b. New York State Education Law §2-d
    c. New York State Education Law §3012-c

11. Network infrastructure and Cloud services that work with or store student, teacher, or principal personal identifiable information must be configured to stop unauthorized user access and protect data in transit and at rest. Examples of steps taken to meet this standard may include but are not limited to:
    a. Following Principle of Least Privilege
    b. Restriction of network routes
    c. Network segmentation
    d. Restrictions on data sharing/access methods
    e. Encryption in transit and at rest
    f. Use of multifactor authentication
    g. Firewall traffic rules

12. Network infrastructure devices and servers must be configured to block

unauthorized external (internet) access to the internal network.

13. External third-party vendor's access to the school's internal network or systems must be authorized and follow the principle of least privilege to perform required work and must be terminated upon completion of work.

14. All printed documents/records containing student, teacher, or principal personal identifiable information must be kept in accordance with federal, state, and local laws.

Third-Party Vendors Data Access

The protection of PII and confidential data for school employees and students is very important for UCHS, however, there are times when sharing data with third-party vendors is necessary for services that benefit the school, student/s, or employees. When the school enters into contracts or written agreements with these third-party vendors the school will ensure the following:

- Third-party vendors' security policy and data privacy plan that complies with state, federal, and local data and security requirements;

- Third-party vendors' security policy and data privacy plan complies with the school's policies;

- Third-party vendors must follow federal, state, and local laws when sharing PII data; these laws include but not limited to:
    - Family Education Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
    - New York State Education Law §2-d
    - New York State Education Law §3012-c
    - New York Shield ACT
    - NYCDOE Chancellor's Regulation A-820

- Third-party vendors and their subcontractors may not sell nor disclose PII data for marketing, any commercial purpose, or use the data for any purpose outside the educational purposes of the contract or written agreement;

- Third-party vendors must notify the school of all data breaches. Should a third-party vendor/contractor notify the school of a data breach or unauthorized disclosure of PII or confidential data, the third-party vendor and school shall follow federal, state, and local legal requirements for notification of affected parties and authorities. This includes notifying the NYS Chief Privacy Officer within 10 calendar days, and affected parents.

Reporting a Breach or Unauthorized Disclosure of Data

Each school makes its best effort to protect data and privacy for students, employees, and guardians. Should anyone need to report a breach of data security or privacy they must do so by notifying the School's Data Protection Officer and the United Charter High School central office administrator. This notification must be in writing and sent by email to tkebatta15@unitedcharter.org. The email must contain the following information:

- Reporting individual/s name
- Contact information of the individual/s reporting incident
- Relationship of the reporter to the school:
    - Parent/Guardian
    - Student
    - School employee
    - Third-party vendor/contractor
    - Other
- Time and date of discovery
- Summary of the incident including
    - Details on what data/systems were breached
    - Information on how the breach was discovered
- Any information that can be provided to assist with the investigation such as but not limited to:
    - Pictures/Screenshots
    - Application name
    - website URL
    - Information affected

An investigation will be carried out with the reporter being notified of the results in accordance with federal, state, and local laws. Please note that the investigation may require withholding or delaying of information due to law enforcement actions, legal requirements, stopping further compromise. The school will only investigate breaches involving school data.