

## Uncommon Schools Data Privacy & Security Policy

Uncommon Schools, Inc. (“Uncommon”) acknowledges the need to secure and protect Personally Identifiable Information (“PII”) aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or “NIST CSF”). Uncommon will establish policies and procedures which address the protection of PII of students and teachers under Education Law 2-d and Part 121 of the NY Commissioner of Education.

Every use and disclosure PII will benefit students and Uncommon (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

Uncommon will protect the confidentiality of student and teacher PII while stored or transferred using industry standard safeguards and best practices. Uncommon will monitor its data systems, develop incident response plans, limit access to PII to district employees and third-party contractors who need access to fulfill their contractual obligations, and destroy PII when it is no longer needed.

Uncommon also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA’s requirements, unless otherwise permitted by law or regulation, Uncommon will not release PII contained in student education records unless it has received a written consent from a parent or eligible student.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides privacy protections for students who are receiving special education and related services. Uncommon will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

Uncommon will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR 121.4).