# Custom Class Charter School

# Administrative Data Governance Plan and Student Data Privacy Policy

**Effective:** As listed below

---

## 1. Purpose

Custom Class Charter School (“Custom Class” or the “School”) has a moral and legal responsibility to protect student privacy and maintain secure student data systems. This Data Governance Plan describes how Custom Class manages student data across its lifecycle—**collection, use, storage, sharing, retention/expungement, and disposal**—and how the School responds to privacy or security incidents.

---

## 2. Scope and Applicability

This Plan applies to all Custom Class **employees, contractors, volunteers, and third-party service providers** who access, handle, store, or transmit student data or education records.

This Plan is used to:

- Control access to student data;
- Ensure disclosures are authorized and documented;
- Evaluate and approve vendors and digital tools that handle student data;
- Establish retention and expungement practices; and
- Provide a clear breach response and training expectations.

This Plan works in conjunction with:

- **Student Data Privacy and Security Policy** (board policy)
- **FERPA Policy / FERPA Administrative Procedures**
- **Student Data Collection Notice**
- **Metadata Dictionary** (data elements and systems)
- **IT Security Practices** maintained by the School’s IT provider

**PLACEHOLDER – LINKS/LOCATIONS FOR THE ABOVE DOCUMENTS**

---

# 3. Roles and Responsibilities

## 3.1 Student Data Manager (Privacy Manager)

The **Executive Director (or designee)** serves as the Student Data Manager and is responsible for student privacy and data governance, including:

1. Approving and managing sharing of student data outside the School;
2. Ensuring student data is not disclosed without proper legal authority or written consent, unless an exception applies;
3. Ensuring vendor tools are approved before use and governed by an appropriate data privacy agreement;
4. Maintaining a list of School roles or employees with access to student data (as required);
5. Ensuring annual privacy training occurs for staff with access to education records;
6. Publishing and updating the Student Data Collection Notice and this Plan as required;
7. Maintaining the School's Metadata Dictionary and providing it as required; and
8. Overseeing response and reporting for significant data breaches consistent with R277-487.

## 3.2 IT Security Manager

Custom Class's contracted IT provider or Executive Director when no contractor exists, serves as the IT Security Manager and is responsible for:

1. Securing School systems and endpoints used to access student data;
2. Supporting identity and access management (accounts, MFA, permissions);
3. Managing patches, monitoring, and security incident investigation support;
4. Supporting backup and recovery practices for School-managed systems; and
5. Reporting periodic security status and issues to School leadership.

## 3.3 Employees and Volunteers with Access

Any employee or volunteer with access to education records must:

1. Complete annual student data privacy training (employees must also sign annual acknowledgement);
2. Access student data only for legitimate educational interest/job duties;
3. Use strong passwords and MFA where required;
4. Never share accounts or passwords;

5. Keep student data in approved systems (not personal devices or personal cloud storage);
6. Use secure methods when transmitting data (approved systems, secure portals, encrypted email when necessary);
7. Protect printed records (locked storage; shred when disposing);
8. Avoid disclosure in public settings and use de-identification when appropriate; and
9. Immediately report suspected breaches or suspicious access.

### 3.4 Educators

Educators must also:

1. Use only School-approved instructional apps and platforms; and
2. Complete any state-required privacy/security training tied to licensure renewal where applicable.

### 3.5 Third-Party Contractors (Vendors)

Vendors that access or receive student data must:

1. Sign a School-approved data privacy agreement (e.g., DPA/Confidentiality Addendum);
2. Use student data only to provide contracted services;
3. Not sell student data;
4. Not use student data for targeted advertising;
5. Return or delete data upon request at contract end (unless legally required otherwise); and
6. Report security incidents involving School data promptly to the Student Data Manager.

### 3.6 Consequences for Non-Compliance

Non-compliance may result in removal of system access, corrective action, termination, contract termination, and/or referral to appropriate authorities where required.

---

## 4. Data Collection

### 4.1 Why We Collect Data

Custom Class collects student data to:

- Deliver educational services and supports;
- Comply with state and federal reporting requirements;
- Maintain accurate records for enrollment, funding, attendance, and services; and

- Support personalization and educational planning.

### 4.2 How We Collect Data

Student data is primarily collected through:

- Secure online application, lottery, and registration processes; and
- School systems used for enrollment, attendance, special education, and instruction.

### 4.3 What We Collect

Custom Class collects:

- **Necessary student data** required for enrollment, funding, services, and reporting; and
- **Optional student data** only when needed for program operations or with appropriate consent as required.

Custom Class does **not** collect student Social Security Numbers.

The School's Student Data Collection Notice lists the specific data elements collected and is posted publicly.

---

## 5. Data Use

Custom Class personnel may access and use student data only for legitimate educational interest and assigned duties. Student data may not be used for personal purposes or unrelated activities.

Outside parties may use student data only when:

- Authorized by law and approved by the Student Data Manager; and
- Governed by written agreements that restrict use and re-disclosure.

---

## 6. Data Storage and Protection

### 6.1 Approved Systems

Custom Class stores student data primarily in **Aspire SIS** and other School-approved systems.

### 6.2 Access Controls

Access is role-based and limited to those who need it. Where available, the School uses:

- MFA for sensitive systems
- Strong password standards
- Audit logs and account management processes

### 6.3 Prohibited Storage

Personally identifiable student data may not be stored on personal devices, personal cloud accounts, removable drives, or unsecured locations unless expressly authorized by the Student Data Manager.

### 6.4 Printed Records

Printed student records must be kept in locked storage with controlled access. Disposal must be via secure shredding or approved destruction methods.

---

## 7. Data Sharing

### 7.1 General Rule

Custom Class does not disclose personally identifiable student data outside the School without:

- Written consent, **or**
- A lawful exception under FERPA/PPRA/Utah law.

### 7.2 Common Authorized Disclosures (Examples)

Disclosures may occur, when lawful, to:

- Parents/guardians or eligible students;
- School officials with legitimate educational interest;
- Vendors performing a school function under contract and data agreement;
- Other schools for transfer/enrollment purposes;
- Appropriate parties in a health/safety emergency;
- Government authorities for audit, evaluation, or compliance;
- In response to subpoena/court order (handled through administration); and
- Directory information (only if the annual notice is provided and not opted out).

### 7.3 Vendor Approval Requirement

No staff member may adopt or use an app, platform, or vendor that receives student data unless it is approved and has an appropriate data privacy agreement in place.

### 7.4 Aggregate/De-Identified Data

Custom Class may share aggregate or de-identified data when it meets Utah requirements (e.g., minimum group sizes and de-identification techniques) and when approved by the Student Data Manager.

# 8. Record Retention and Expungement

### 8.1 Retention

Custom Class retains and disposes of student records consistent with:

- Utah Code § 63G (records requirements),
- Utah Code § 53E-9-306, and
- USBE Rule R277-487.

Unless Custom Class adopts an approved retention schedule, the School follows the Utah Division of Archives and Records Service (State Archives) education retention schedules.

### 8.2 Expungement

Custom Class may expunge student data that is not required to be retained when the administrative need has passed, consistent with Utah law and rule. The School may not expunge permanent records such as grades/transcripts/enrollment history/required assessment records.

Parents/eligible students may request expungement or amendment of records they believe are inaccurate, misleading, or privacy-violating. Requests must be made in writing to the Student Data Manager and will be handled using FERPA amendment procedures and timelines.

# 9. Data Breach Response

### 9.1 Definition

A data breach is unauthorized access, disclosure, or release of personally identifiable student data, whether managed directly by the School or by a vendor.

### 9.2 Reporting

Any employee, volunteer, vendor, parent, or student who suspects a breach must notify the Student Data Manager immediately.

### 9.3 Response Steps (Simplified)

Custom Class will:

1. Contain the incident (disable accounts, reset credentials, isolate affected systems);
2. Investigate scope and impacted data;
3. Preserve evidence and document actions taken;
4. Coordinate with IT provider and legal counsel as appropriate;
5. Notify parents/eligible students when required;
6. Notify USBE within required timelines if it constitutes a **significant data breach** under R277-487; and
7. Implement corrective actions to prevent recurrence.

---

## 10. Transparency

Custom Class posts or makes available, as required:

- Student Data Collection Notice
- This Data Governance Plan
- Metadata Dictionary (or summary)
- Relevant privacy policies and notices

Documents may also be requested at **info@customclass.org**.

---

## 11. Auditing and Review

Custom Class periodically reviews compliance with this Plan, including:

- Access reviews (who has access and why);
- Vendor list review and agreement verification; and
- Incident log review and corrective action tracking.

The School may use third-party experts to support audits when appropriate.

---

## 12. Training

Custom Class provides annual student data privacy training to employees with access to education records and provides IT security guidance as needed. Training completion is documented and retained.

---

### Certification

The undersigned officers and/or Board of Directors of Custom Class Charter School certify that this Administrative Data Governance Plan was duly adopted as of the date below.

Signature:

Matthew J. Middione – Board Chair

Signature:

Douglas Reed – Board Vice Chair

**Effective Date:** As listed above
**Revised Date:**

**References:** FERPA (20 U.S.C. § 1232g; 34 CFR Part 99), PPRA (20 U.S.C. § 1232h; 34 CFR Part 98), Utah Code Title 53E Chapter 9 (Student Data Privacy), USBE Rule R277-487