

# DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

Morris Central School District Bill of Rights for Data Security and Privacy  
and  
Supplemental Information about a Master Agreement between  
Morris Central School District and the University of Oregon

## 1. **Purpose**

(a) Morris Central School District (hereinafter "District") and the University of Oregon (hereinafter "Vendor") are parties to a contract or other written agreement pursuant to which Vendor will receive student data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District for purposes of providing the easyCBM software-as-a service to the District (the "Master Agreement").

(b) This Exhibit supplements the easyCBM User Agreement & Privacy Policy ("Master Agreement") to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Master Agreement between Morris Central School District and the University of Oregon that the District is required by Section 2-d to post on its website.

(c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the Services that are the subject of the Master Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

## 2. **Definitions**

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

(b) "Protected Data" means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Master Agreement.

(c) "NIST Cyber security Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cyber security (Version 1.1).

## 3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

---

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d). The District will provide Vendor with a copy of its policy on data security and privacy upon request.

#### 4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Agreement, Vendor has the easyCBM Teacher Deluxe Security & Compliance White Paper in place to describe the confidentiality, privacy and security measures for the Protected Data it receives from the District.

Vendor's Plan for protecting the District's Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Master Agreement are as follows:

(a) Vendor will implement all state, and federal, data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement.

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between Morris Central School District and the University of Oregon." Vendor's obligations described within this section include, but are not limited to:

- (i) its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law and the Master Agreement shall apply to the subcontractor, and
- (ii) its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.

(d) Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees who will have access to Protected Data, prior to their receiving access.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and has developed and implemented plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

#### 5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to the District by contacting Greg Thom directly by email at [gthom@morriscsd.org](mailto:gthom@morriscsd.org) or by calling (607) 263-6100

---

(c) Vendor will cooperate with the District and provide as much information as possible directly to Morris Central School District or his/her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform Morris Central School District or his/her designee.

## 6. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

- (i) the parent or eligible student has provided prior written consent; or
- (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the District soon as reasonably possible, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) To use encryption technology to protect Protected Data in its custody while in motion or at rest.

(f) To adopt technologies, safeguards and practices that align with the NIST Cyber security Framework.

(g) To comply with New York Education Law, Section 2-d and Part 121.

(h) To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(i) To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights

for Data Security and Privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

(j) To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

## **Bill of Rights for Data Security and Privacy**

### **Morris Central School District**

#### **PARENT'S BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

The District, in compliance with Education Law §2-d, provides the following:

#### **DEFINITIONS:**

As used in this policy, the following terms are defined:

**Student Data** means personally identifiable information from the student records of a District student.

**Third Party Contractor** means any person or entity, other than a District, that receives Student Data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of an educational partnership organization that receives Student Data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization, other than a District.

1. Student Data will be sold or released for any commercial purpose;
  2. Parents have the right to inspect and review the complete contents of their child's education records. Procedures for reviewing student records can be found in the Board Policy entitled (insert title of FERPA policy);
  3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of Student Data are maintained at standards for a public university providing similar services and best practices. The safeguards include, but are not limited to, encryption, firewalls, and password protection. As required by Education Law §2-d(5), alignment with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cyber security Version 1.1 (NIST Cyber security Framework or NIST CSF) is adopted as the standard for data security and privacy;
  4. New York state maintains a complete list of all Student Data collected by the State and the data is available for public review at <http://www.p12.nysed.gov/irs/sirs/NYSEDDataElements2018.xlsx> or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234;
  5. Parents have the right to have complaints about possible breaches of Student Data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaint may also be submitted using the form available at the following website <http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure>.
-

6. The District has also established the following procedures for parents to file complaints with the District about breaches or unauthorized releases of Student Data:
  - a. All complaints must be submitted to the District's Data Protection Officer in writing.
  - b. Upon receipt of a complaint, the District will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.
  - c. Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;
  - d. Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation the District shall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;
  - e. The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1.
7. This policy will be regularly updated with supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives Student Data. The supplemental information must be developed by the District and include the following information:
  - a. the exclusive purposes for which the Student Data will be used by the third-party contractor, as defined in the contract;
  - b. how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the Student Data, if any, will abide by all applicable data protection and security requirements, including, but not limited to, those outline in applicable State and federal laws and regulations (e.g., FERPA; Education Law §2-d);
  - c. the duration of the contract, including the contract's expiration date and a description of what will happen to the Student Data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the District, and whether, when and how the data will be destroyed?);
  - d. if and how a parent, student eligible student, teacher or Principal may challenge the accuracy of the Student Data that is collected;
  - e. where the Student Data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed.

This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third party contractor where the third party contractor receives Student Data.

---

## Supplemental Information about a Master Agreement between

### Morris Central School District and the University of Oregon

Morris Central School District has entered into a Master Agreement with the University of Oregon, which governs the availability to the District of the following products or services:

The software-as-a-service entitled: easyCBM

Pursuant to the Master Agreement(which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students that is protected by Section 2-d of the New York Education Law (“Protected Data”).

**Exclusive Purposes for which Protected Data will be Used:** The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the functionality of the Services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.

**Oversight of Subcontractors:** In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Master Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Vendor under the Master Agreement and applicable state and federal law and regulations.

#### **Duration of Agreement and Protected Data Upon Termination or Expiration:**

- The Master Agreement commences when the District begins using the Services and expires when the district stops using the Services.
- Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Vendor will, as soon as reasonably possible, securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by the District, Vendor will assist the District in exporting all Protected Data previously received back to the District for its own use, prior to deletion, in such formats as may be requested by the District.
- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

**Challenging Accuracy of Protected Data:** Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

**Data Storage and Security Protections:** Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cyber security Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

---

**Encryption of Protected Data:** Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.

**Agreement and Signature**

By signing below, you agree:

- To comply with the terms contained in the Supplemental Information Master Agreement
- To comply with the terms of Morris Central Schools Parents' Bill of Rights for Data Privacy and Security (applicable to Third-Party Contractors subject to New York Education Law § 2-d only)

**BY THE VENDOR:**

**University of Oregon**

**easyCBM**

**Name**

**Product Name**

**Orca Merwin**

*Orca Merwin*

**3/13/22**

**Name (Print)**

**Signature**

**Date**

**Data Privacy Rider for All Contracts Involving Protected Data Pursuant to New York State Education Law §2-C and §2-D**

Morris Central School District and the Vendor agree as follows:

1. Definitions:
  - a. Protected Information means personally identifiable information of students from student education records as defined by FERPA, under New York Education Law §3012-c and §3012-d;
  - b. Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);
2. Confidentiality of all Protected Information shall be maintained in accordance with State and Federal;
3. The Parties agree that the Morris Central School District Parents’ Bill of Rights for Data Security and Privacy are incorporated as part of this agreement, and the Vendor shall comply with its terms;
4. The Vendor agrees to comply with New York State Education Law §2-d and its implementing regulations;
5. The Vendor agrees that any officers or employees of the Vendor, and its assignees who have access to Protected Information, have received or will receive training on Federal and State law governing confidentiality of such information prior to receiving access;
6. The Vendor shall:
  - a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
  - b. not use the Protected Information for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes;
  - c. except for authorized representatives of the Vendor to the extent they are carrying out the contract or written agreement, not disclose any personally identifiable information to any other party;
    - i. without the prior written consent of the parent or eligible student; or
    - ii. unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information as soon as reasonably possible, unless providing notice of the disclosure is expressly prohibited by statute or court order;
  - d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
  - e. use encryption technology to protect data while in motion or in its custody from unauthorized;
  - f. adopt technology, safeguards and practices that align with the NIST Cyber Security Framework;

**Agreement and Signature**

By signing below, you agree to the Terms and Conditions in this Rider:

University of Oregon

easyCBM

\_\_\_\_\_  
**Name**

\_\_\_\_\_  
**Product Name**

**Orca Merwin**

*Orca Merwin*

\_\_\_\_\_  
**Name (Print)**

\_\_\_\_\_  
**Signature**

3/13/22

\_\_\_\_\_  
**Date**