

**Exhibit D****PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

- (1) A student's personally identifiable information cannot be sold or released for any commercial purposes.
- (2) Parents have the right to inspect and review the complete contents of their child's education record.
- (3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
- (4) A complete list of all student data elements collected by the State is available for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.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 the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be directed to the Chief Privacy Officer via email at: [CPO@mail.nysed.gov](mailto:CPO@mail.nysed.gov).

  
\_\_\_\_\_  
Signature

General Counsel  
\_\_\_\_\_  
Title

February 11, 2020  
\_\_\_\_\_  
Date

iboss, Inc.  
\_\_\_\_\_  
Company

## APPENDIX

### Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Erie 1 BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to “student data” and/or “teacher or principal data,” as those terms are defined by law.

Each contract the BOCES enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include the following information:

- (1) the exclusive purposes for which the student data or teacher or principal data will be used;
- (2) how the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
- (3) when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
- (4) if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
- (5) where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

**Exhibit E****Vendor Use of Student Data**

The exclusive purposes for which Vendor is being provided access to the shared Student Data is as follows:

Vendor will process Customer Personal Data solely for purposes of providing the Services described in this Agreement and any applicable statement of work. For purposes of this Agreement, the term "Customer Personal Data" means Personal Data (as that term is defined in the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR")), the extent of which is determined and controlled by Erie 1 in its sole discretion, such as names, email addresses, IP addresses, web browsing data, including websites visited; location data (any data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a public electronic communications service); and browsing, search, and other network activity of authorized users of Customer's network."

By default, Vendor's secure cloud gateway cybersecurity platform processes Customer Personal Data. However, Vendor does not ordinarily access or review Customer Personal Data because it is protected within segregated, containerized reporting databases that isolate this information. Additionally, critical information, such as passwords, is encrypted during transit and at rest, preventing direct access to the underlying information. By default, Customer Personal Data is only accessible to the customers' administrator(s) and other authorized users who were designated by the administrator(s). In some cases, however, Erie 1 may elect to provide Vendor administrative access to the Customer Personal Data, typically to enable Vendor to provide customer support to Erie 1.