

Massachusetts Student Privacy Alliance

STUDENT DATA PRIVACY SPECIAL TERMS AND CONDITIONS

This Student Data Privacy Special Terms and Conditions dated October 2, 2017 (hereinafter "Agreement") is by and between **Falmouth Public Schools ("FPS")** and **Hobsons, Inc. ("Contractor")**, a contractor performing institutional services and functions that will require student data to perform those services and functions.

1. Contractor and **FPS** have contracted for the Contractor to provide Naviance K-12 college and career readiness platform ("the Services"), which are institutional services and functions, to **FPS**. In the course of performing the Services, Contractor will obtain confidential student records and/or confidential student record information that contain personally identifiable student records, data and/or personally identifiable information and other non-public information, including but not limited to student data, meta data and user content ("Data Files"). **FPS** and Contractor acknowledge and agree that this Agreement is for the purpose of sharing Data Files between the parties in a manner consistent with the Family Educational Rights and Privacy Act of 1974 ("FERPA") and Massachusetts student record regulations, 603 C.M.R. 23.00 ("State Regulations"). The Data Files will be used by the Contractor and its employees to populate student data only for the purpose of delivering these Services. Contractor further acknowledges and agrees that all copies of such Data Files, including any modifications or additions to Data Files or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Data Files. The ability to access or maintain Data Files and/or any portion thereof under this Agreement shall not under any circumstance transfer from Contractor to any other party. Data Files do not include deidentified, aggregated information that does not allow for identification of any individual student per the standards set out in FERPA, provided that Contractor makes no attempt to reidentify any student.
2. Contractor acknowledges and agrees that it is providing institutional services or functions for **FPS** and that it is under direct control of **FPS** with respect to the use and maintenance of Data Files in connection with these Services. Contractor additionally acknowledges and agrees that at no point in time is the Contractor the owner of the Data Files. Ownership rights are maintained by **FPS** and **FPS** reserves the right to request deletion of the Data Files and/or all Data Files at any time for any reason whatsoever. Contractor further acknowledges and agrees that it shall adhere to the requirements set forth in both federal and state law regarding the use and re-disclosure of the Data Files or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information contained within the Data Files. Contractor also acknowledges and agrees that it shall not make any re-disclosure of any Data Files or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Data Files, without the express written consent of **FPS** unless required pursuant to applicable law, subpoena or other court processes. Additionally, Contractor agrees that except as otherwise described in clause (i) of Section 3 below, only authorized employees of the Contractor directly involved in delivering the Services shall have access to the Data Files or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Data Files and that it and its employees shall protect the confidentiality of the Data Files or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or

Massachusetts Student Privacy Alliance

personally identifiable information contained in the Data Files in such a way that parties other than officials of FPS and their authorized agents cannot identify any students.

3. Contractor also acknowledges and agrees to:
- (i) use Data Files shared under this Agreement for no purpose other than in connection with and through the provision of the Services provided under this Agreement with FPS. It is understood and agreed that the Services include features provided by Contractor's third party partners to FPS on Contractor's behalf. Contractor represents that such third parties receive only the minimally required information from Data Files to provide Services to FPS, are contractually obligated to comply with Contractor's privacy and security policies, as well as with all applicable federal and state laws, and may make no additional use of personally identifiable information from Data Files. Services also include features through which students may share personally identifiable information with higher education institutions. All such features may be turned on or off at the sole discretion of FPS.
 - (ii) use reasonable methods, including but not limited to, appropriate technical, physical and administrative safeguards, that reflects technology best practices and is consistent with industry standards, to protect the Data Files and/or any portion thereof from re-disclosure that is created, sent, received, stored, processed or transmitted in connection with the Services under this Agreement while the Data Files and/or any portion thereof contained therein is both at rest and in transit. Contractor further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
 - (iii) not share the Data Files and/or any portion thereof received under this Agreement except as described in clause (i) above and as necessary to provide the Services, with any other entity without prior written approval from FPS and the prior written approval of the parent/guardian of the student or eligible student.
 - (iv) not copy, reproduce or transmit the Data Files and/or any portion thereof, except as necessary to fulfill the Services.
 - (v) not re-disclose, transfer or sell the Data Files and/or any portion thereof.
 - (vi) not to use the Data Files and/or any portion thereof to market or otherwise advertise directly to students and/or their parents/guardians, provided that it is understood and agreed that making information regarding higher education institutions and scholarship opportunities is part of the Services for which FPS is engaging with Contractor and as such is not precluded herein
 - (vii) not to use the Data Files and/or any portion thereof to inform, influence or guide marketing or advertising efforts or to develop a profile of a student or group of students for any commercial or other purposes.
 - (viii) not to use the Data Files and/or any portion thereof contained therein for the development of commercial products or services.
 - (ix) not to mine the Data Files and/or any portion thereof for any purposes other than those agreed to by the parties. Contractor further acknowledges that data mining or scanning of user content for the purpose of advertising or marketing to students or their parents/guardians is expressly prohibited.
 - (x) notify the Director of Technology for FPS in writing within three (3) days of its determination that it has experienced a data breach, breach of security, privacy incident or unauthorized acquisition or use of any Data Files and/or any portion thereof contained therein. Contractor agrees that said notification shall include, to the extent feasible, the date or approximate dates of such incident and the nature thereof, the specific scope of said breach (i.e., what data was accessed, used, released or otherwise breached, including the names of individual students that were affected by said breach) and what actions or steps with respect

Massachusetts Student Privacy Alliance

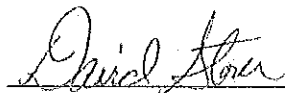
to the incident that Contractor plans to take or has taken in response to said breach. Additionally, Contractor agrees to adhere to all requirements in the Massachusetts Data Breach law and in federal law with respect to a data breach related to the Data Files, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach. Contractor further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Data Files or any portion thereof, including personally identifiable information.

- (xi) not provide any Data Files or any portion thereof to any party known by Contractor to be ineligible to receive student records and/or student record data and information protected by FERPA and State Regulations or prohibited from receiving the Data Files or any portion thereof and/or any personally identifiable information from any entity under 34 CFR 99.31(a)(6)(iii).
- (xii) maintain backup copies, backed up at least daily, of Data Files in case of Contractor system failure or any other unforeseen event resulting in loss of Data Files or any portion thereof.
- (xiii) .
- (xiv) upon receipt of a written request from FPS, begin the process of erasing and/or otherwise destroying any Data Files, be it digital, archival or physical form, including without limitation any copies of the Data Files or any portions thereof that may reside in system backups, temporary files or other storage media and or are otherwise still in Contractor's possession and/or in the possession of any subcontractors, or agents to which the Contractor may have transferred Data Files or any portion thereof, in a manner consistent with technology best practices and industry standards for secure data disposal methods such that Contractor and/or any of its subcontractors or agents are no longer in possession of any student work belonging to FPS and to ensure that the Data Files cannot be recovered and are securely destroyed FPS Contractor also will provide FPS with written certification, including an inventory of its Data Files destruction, and with written certification, FPS, within thirty (30) days of its receipt of FPS request for destruction of Data Files.
- (xv) in the event of the Contractor's cessation of operations, promptly return all Data Files to FPS in an organized, manageable manner and subsequently erasing and/or otherwise destroying any Data Files, be it digital, archival or physical form, including without limitation any copies of the Data Files or any portions thereof that may reside in system backups, temporary files or other storage media and or are otherwise still in Contractor's possession and/or in the possession of any subcontractors, or agents to which the Contractor may have transferred Data Files or any portion thereof, in a manner consistent with technology best practice and industry standards for secure data disposal methods such that Contractor and/or any of its subcontractors or agents are no longer in possession of any student work belonging to FPS and to ensure that the Data Files cannot be recovered and are securely destroyed. Contractor also will provide FPS with written certification, including an inventory of its Data Files destruction, and with written certification, including an inventory of all Data Files returned to FPS, within thirty (30) days of Contractor's cessation of operations.
- (xvi) not use, disclose, compile, transfer, sell the Data Files and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Data Files and/or any portion thereof other than as described in clause (i) above.
- (xvii) delete FPS Data Files that it collects or receives under this Agreement once the Services referenced in this are to be provided by Contractor to FPS and upon receipt of written confirmation from FPS to delete the Data Files.

Massachusetts Student Privacy Alliance

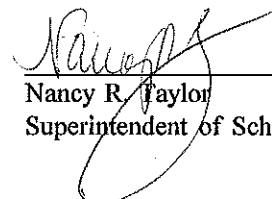
- (xviii) upon receipt of a litigation hold request from FPS, immediately implement a litigation hold and preserve all documents and data relevant identified by FPS and suspend deletion, overwriting, or any other possible destruction of documentation and data identified in, related to, arising out of and/or relevant to the litigation hold.
 - (xix) cooperate fully with FPS and any local, state, or federal agency with oversight authority/jurisdiction in connection with any investigation of the Contractor and/or delivery of Services to students and/or FPS, and shall provide relevant access to Contractor's facilities, staff, agents and FPS Data Files, FPS Data Files and delivery of Services to FPS.
 - (xx) not assign, subcontract or in any way transfer any interest in this Agreement without the prior written consent of FPS.
4. Contractor certifies under the penalties of perjury that it complies with all federal and state laws, regulations and rules as such laws may apply to the receipt, storing, maintenance or access to personal information, including without limitation, all standards for the protection of personal information of residents of Massachusetts and maintaining safeguards for personal information. Contractor hereby further certifies under penalties of perjury that it has a written comprehensive information security program that is in compliance with the provisions of 201 C.M.R. 17.00 et seq. Further, the Contractor hereby certifies under the penalties of perjury that it shall fully comply with the provisions of the federal Family Educational Rights Privacy Act, 20 U.S.C. §1232g and regulations promulgated thereunder and Massachusetts student records law and regulations, including without limitation, 603 C.M.R. 23.00 et seq., and to fully protect the confidentiality of any student data, meta data, user content or other non-public information and/or personally identifiable information provided to it or its representatives. Contractor further represents and warrants that it has reviewed and complied with all information security programs, plans, guidelines, standards and policies that apply to the work it will be performing, that it will communicate these provisions to and enforce them against its subcontractors and will implement and maintain any other reasonable and appropriate security procedures and practices necessary to protect personal information and/or student record information from unauthorized access, destruction, use, modification, disclosure or loss. Contractor also represents and warrants that if the Data Files or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information, is to be stored on a laptop or other mobile electronic device, that such electronic devices are encrypted. Furthermore, Contractor represents and warrants that it has in place a service that will allow it to wipe the hard drive on any stolen laptop or mobile electronic device remotely.

Hobsons, Inc./Naviance


Name

Dave Storer, Global Controller
Title

Falmouth Public Schools


Nancy R. Taylor
Superintendent of Schools