

**MASSACHUSETTS STUDENT DATA PRIVACY AGREEMENT  
VERSION (2018)**

**Milton Public Schools**

**and**

**Classcraft Studios, Inc.**

**October 1, 2019**

This Massachusetts Student Data Privacy Agreement (“DPA”) is entered into by and between the school district, Milton Public Schools (hereinafter referred to as “LEA”) and Classcraft Studios, Inc. (hereinafter referred to as “Provider”) on October 1, 2019. The Parties agree to the terms as stated herein.

## RECITALS

**WHEREAS**, the Provider has agreed or will agree to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) as described in Article I and Exhibit “A”; and

**WHEREAS**, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in Massachusetts the opportunity to accept and enjoy the benefits of the DPA for the Services described, without the need to negotiate terms in a separate DPA; and

**WHEREAS**, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 et. seq.; and

**WHEREAS**, the documents and data transferred from Massachusetts LEAs and created by the Provider’s Services are also subject to several Massachusetts student privacy laws, including Massachusetts student record regulations, 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

**WHEREAS**, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

## ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit “C”) transmitted to Provider from the LEA pursuant to Exhibit “A”, including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.
  
2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described in Exhibit “A”.

3. **Student Data to Be Provided.** In order to perform the Services described in this Article and Exhibit “A”, LEA shall provide the categories of data described in the Schedule of Data, attached hereto as Exhibit “B”.
4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit “C”. In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

## **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA , or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. The Provider will cooperate and provide Student Data within ten (10) days at the LEA’s request. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall cooperate and respond within ten (10) days to the LEA’s request for personally identifiable information in a pupil’s records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account.
4. **Third Party Request.** Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a

compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student Data 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 Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws.** LEA shall provide data for the purposes of the DPA in compliance with the FERPA, PPRA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H, and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all Massachusetts and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, , 603 C.M.R. 23.00 and Massachusetts General Law, Chapter 71, Sections 34D to 34H.
2. **Authorized Use.** Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data 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 Student Data, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.
  
4. **No Disclosure.** De-identified information, as defined in Exhibit “C”, may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). The Provider and LEA agree that the Provider cannot successfully de-identify information if there are fewer than twenty (20) students in the samples of a particular field or category of information collected, i.e., twenty students in a particular grade, twenty students of a particular race, or twenty students with a particular disability. Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA.
  
5. **Disposition of Data.** Provider shall dispose or delete all personally identifiable data obtained under the DPA when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA’s designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a “Request for Return or Deletion of Student Data” FORM, A Copy of which is attached hereto as Exhibit “D”). Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within three (3) calendar days of receipt of said request.
  
6. **Advertising Prohibition.** Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing or advertising efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to Client; or (d) use the

Student Data for the development of commercial products or services, other than as necessary to provide the Service to Client.

## ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit “F” hereto. These measures shall include, but are not limited to:
  - a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.
  - b. **Destruction of Data.** Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA’s designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.
  - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.
  - d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
  - e. **Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer (“SSL”), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the DPA in an environment using a firewall that is periodically updated according to industry standards.
  - f. **Security Coordinator.** Provider shall provide the name and contact information of Provider’s Security Coordinator for the Student Data received pursuant to the DPA.
  - g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the

terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

- h. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
  - i. Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider’s system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.
  - j. Audits.** Upon receipt of a request from the LEA, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof. The Provider will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide full access to the Provider’s facilities, staff, agents and LEA’s Student Data and all records pertaining to the Provider, LEA and delivery of Services to the Provider. Failure to cooperate shall be deemed a material breach of the Agreement.
- 2. Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within ten (10) days of the incident. Provider shall follow the following process:
- a.** The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described herein under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.
  - b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

    - i.** The name and contact information of the reporting LEA subject to this section.
    - ii.** A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
    - iii.** If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
    - iv.** Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
    - v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

- c. At LEA's discretion, the security breach notification may also include any of the following:
  - i. Information about what the agency has done to protect individuals whose information has been breached.
  - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d. Provider 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 Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- e. Provider 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 Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
- f. At the request and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

## ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years.
2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated.

The LEA may terminate this DPA and any service agreement or contract with the Provider if the Provider breaches any terms of this DPA.

3. **Effect of Termination Survival**. If the DPA is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b).
4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA, IDEA, COPPA, PPR, 603 CMR 28.00, 603 C.M.R. 23.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.



5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives below.

The designated representative for the Provider for this Agreement is:

Name	Lauren Young
Title	CFO
Address	#220 - 165 Wellington N, Sherbrooke, QC, J1H 5B9
Telephone Number	514-377-0289
Email	lauren@classcraft.com

The designated representative for the LEA for this Agreement is:

AJ Melanson, Educational Technology Director  
amelanson@miltonps.org, 617-696-4470 x 5586  
Milton Public Schools  
25 Gile Road, Milton, MA 02186

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
7. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF MASSACHUSETTS, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF NORFOLK COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way.
10. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Electronic Signature:** The parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with Massachusetts and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of my electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Each party will immediately request that their electronic signature be revoked in writing if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation at any time of their electronic signature for any other reason in writing.

If either party would like a paper copy of this Agreement, they may request a copy from the other party.

12. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

## **ARTICLE VII- GENERAL OFFER OF TERMS**

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit “E”), be bound by the terms of this to any other school district who signs the acceptance in said Exhibit.

*[Signature Page Follows]*

**IN WITNESS WHEREOF**, the parties have executed this Massachusetts Student Data Privacy Agreement as of the last day noted below.

**MILTON PUBLIC SCHOOLS**

*AJ Melanson*  
AJ Melanson (Sep 28, 2019)

Date: 09.28.19

Printed Name: AJ Melanson

Title: Educational Technology Director

**CLASSCRAFT STUDIOS, INC.**

*Lauren Young*

Date: 28 Sept 2019

Printed Name: Lauren Young

Title: CFO

**EXHIBIT "A"**

**DESCRIPTION OF SERVICES**

**Classcraft**, online, game-based approach to teaching.

**EXHIBIT “B”**

**SCHEDULE OF DATA**

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	✓
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	✓
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	✓
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	✓
	Student grade level	✓
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	✓
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	✓
Parent/Guardian Name	First and/or Last	✓

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	✓
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	✓
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last	Optional
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	✓
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc. Other student work data - Please specify:	✓
Transcript	Student course grades	

Category of Data	Elements	Check if used by your system
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if used by your system
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

## EXHIBIT “C”

### DEFINITIONS

**De-Identifiable Information (DII):** De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider’s specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual. Information cannot be de-identified if there are fewer than twenty (20) students in the samples of a particular field or category, i.e., twenty students in a particular grade or less than twenty students with a particular disability.

**NIST 800-63-3:** Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

**Personally Identifiable Information (PII):** The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes, without limitation, at least the following:

First Name	Home Address
Last Name	Subject
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	Date of Birth
Grade	Classes

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student’s Educational Record

Information in the Student’s Email



**Provider:** For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

**Pupil Generated Content:** The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

**Pupil Records:** Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

**School Official:** For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records. The definition of “school official” encompasses the definition of “authorized school personnel” under 603 CMR 23.02.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians, that is descriptive of the student including, but not limited to, information in the student’s educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Massachusetts and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services.

**Subscribing LEA:** An LEA that was not party to the original Services Agreement and who accepts the Provider’s General Offer of Privacy Terms.

**Subprocessor:** For the purposes of this Agreement, the term “Subprocessor” (sometimes referred to as the “Subcontractor”) means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

**Targeted Advertising:** Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time.

**Third Party:** The term “Third Party” means an entity that is not the provider or LEA.

**EXHIBIT "D"**

**DIRECTIVE FOR DISPOSITION OF DATA**

[Name or District or LEA] directs [Name of Company] to dispose of data obtained by Company pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

\_\_\_ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

\_\_\_ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

\_\_\_ Disposition shall be by destruction or deletion of data.

\_\_\_ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions.]

3. Timing of Disposition

Data shall be disposed of by the following date:

\_\_\_ As soon as commercially practicable

\_\_\_ By (Insert Date)

4. Signature

\_\_\_\_\_  
(Authorized Representative of LEA)

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Company

\_\_\_\_\_  
Date

**OPTIONAL: EXHIBIT "F"**  
**DATA SECURITY REQUIREMENTS**

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy?  Yes  No

If yes, please provide it.

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

\_\_\_ ISO 27001/27002

CIS Critical Security Controls

\_\_\_ NIST Framework for Improving Critical Infrastructure Security

\_\_\_ Other: \_\_\_\_\_

3. Does your organization store any customer data outside the United States?  Yes  No

4. Does your organization encrypt customer data both in transit and at rest?  Yes  No

5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: Stephane Guillemette

Contact information: stephane@classcraft.com

6. Please provide any additional information that you desire.

**Data is stored on AWS servers in the USA, but customer support is provided from Canada.**



## **Data Security Policy**

### **Updated: July 27, 2018**

---

## **Introduction**

**Classcraft Studios Inc** (“Classcraft”) produces online software for use by teachers, students, parents and school administrators. In addition to gathering and storing information from our users, Classcraft also gathers and stores information about suppliers, employees, business contacts and other people the organization has a relationship with or may need to contact.

This policy describes how this data must be collected, handled and stored to meet the company’s data security standards and to comply with legislative requirements. This policy applies to the head office of the Classcraft, all branch locations, all employees and all contractors and suppliers working on behalf the Classcraft.

## **Collection of Data**

Classcraft only collects personal information that relates directly to its programs or activities. Wherever possible that data is collected directly from the individual or entity that it is about, and the individual is advised that the data is being collected and for what purpose.

Classcraft only uses collected personal information for the purposes for which it is collected, unless the individual consents to other uses. Classcraft does not allow third parties (such as marketing agencies or research groups) to have access to collected personal information without the express written consent of the individual, unless that information is anonymized and no personal information is identifiable.

Classcraft has a policy that any individual may review all data stored in regards to them, within 30 days of any written request addressed to [wecare@classcraft.com](mailto:wecare@classcraft.com). In the case of individuals under the age of 18, Classcraft will provide access to this data to a parent or legal guardian.

# Data Protection Risks

This policy helps to protect Classcraft from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failure to inform and offer choice.** All individuals should be fully informed as to how the company uses data related to them, and should have the option to review and correct such data, or to have such data erased.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

## Responsibilities

Everyone who works for or with Classcraft has some responsibility for ensuring data is collected, stored and handled appropriately. Furthermore, each team member that handles personal data must ensure that it is handled and processed in line with this policy and the underlying data protection principles.

However, these people have key areas of responsibility:

- The **Board of Directors** is ultimately responsible for ensuring that Classcraft meets its legal obligations.
- The **Data Protection Officer, presently Shawn Young** is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule, but no less often than every 12 months.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Checking and approving any contract or agreements with third parties that may handle the company's sensitive data.
- The **Chief Technology Officer, presently Stephane Guillemette** is responsible for:
  - Ensuring all systems, services and equipment used for data storage meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Performing regular checks to ensure that staff members who have access to sensitive data are observing security procedures, such as passwords and security of portable hardware.

- Evaluating any third-party services the company is considering using to store or process data, such as cloud computing services.
- The **Chief Financial Officer, Lauren Young**, is responsible for:
  - Ensuring that all user licenses and terms of service, privacy policies, and other data protection statements are up to date and conform with legislation and Classcraft's privacy and data security objectives.
  - Dealing with requests from individuals to see the data Classcraft holds about them or their children under the age of 18 ("Subject Access Requests").
  - Ensuring the security of all gathered information related to employees, contractors and suppliers.
  - Checking and approving any contract or agreements with third parties that may handle the company's sensitive data.

## General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their front line managers.
- **Classcraft will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Passwords that give access to sensitive data should not be stored using the "autofill" abilities of browsers or other similar software. However, use of a secure password manager application is permitted.
- Personal data **should not be disclosed** to unauthorized people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, either by law or for its intended purpose, then it should be deleted and disposed of.
- Employees **should request help** from their line manager or the Data Protections Officer if they are unsure about any aspect of data protection.

# Strong Password Policy

Passwords should consist of at least 8 characters, including one symbol, one number and one change of case. The password must be hard to crack so if a word or proper name is used it must have at least two unconnected words or proper names.

User passwords must be changed frequently. When a staff person leaves our organization, all passwords used by that person are changed, so that they will no longer have access even if he/she visits our office. The person also returns any keys used to physically secure the offices.

# Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely should be directed to the Data Protection Officer or Senior Developer.

When data is **stored on paper**, it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a **locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorized people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed frequently and never shared between employees.
- Passwords that give access to sensitive data should not be stored using the “autofill” abilities of browsers or other similar software. However, use of a secure password manager software is permitted.
- If data is **stored on removable media** (like a DVD, USB key or external hard drive), these should be kept secure when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to **approved cloud computing services**.

- Servers containing personal data should be **situated in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with Classcraft's standard backup procedures.
- Personal data **should never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

## Data Use

Personal data is of no value Classcraft unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended (Screen saver with password).
- Personal data **should not be shared informally**. In particular it should never be sent by email, as this form of communication is not secure.
- Personal Data must be **encrypted before being transferred electronically**. Should you need to transfer personal data, please talk to the Senior Developer for instructions on how to send data securely.
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any personal data.

## Data Accuracy

It is the responsibility of all employees who work with personal data to take reasonable steps to ensure it is kept accurate and as up to date as possible:

- Data should be kept in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when you are in communication with them.
- Classcraft will make it **easy for data subjects to update the information** that Classcraft holds about them. For instance, via the user's profile page.
- Any customer or potential customer who has **unsubscribed or otherwise indicated they do not wish to be contacted** will have this information stored in their file and this



will be cross referenced before sending group emails and communications so that they will not be contacted.

## Automatic Deletion of Personal Information

Classcraft policy is to delete personal data of students and parents is cancelled as below:

- Behaviour data will be deleted 1 year after their account has become inactive
- Forum postings, assignments, and comments will be deleted one year after their account has become inactive
- Login information, email account (if stored), and avatars, pets, equipment and badges, and other game attributes will be deleted 3 years after the account has become inactive, as the student can reuse these elements in a later grade at the same school.
- Personal data of teachers and any data not already deleted that is related to the teacher's classes will be deleted 5 years after their account has become inactive.

## Subject Access Requests

All individuals who are the subject of personal data held by Classcraft are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a Subject Access Request.

Subject access requests from individuals should be made by email, addressed to [wecare@classcraft.com](mailto:wecare@classcraft.com). The relevant data will be provided to them within 30 days. The identity of the individual making a subject access request will be verified before release to them of any personal data.

## Disclosing Data for Other Reasons

Classcraft may receive requests to access personal data from government agencies, including law enforcement agencies. Under these circumstances, Classcraft will disclose the requested data without obtaining the consent of the data subject, once it has been determined that the

request is legitimate. Classcraft may seek assistance from the board and from the company's legal advisers should it deem such assistance necessary.

# Privacy Policy

Classcraft aims to ensure that individuals are aware that their data is being processed, and that they understand how the data is being used, and how to exercise their rights.

To these ends, Classcraft has a Privacy Policy setting out how data related to individuals is used by the company.

This Privacy Policy is available at <http://classcraft.com/privacy-policy/>.

## If a Breach Occurs

If our Data Protection Officer determines that personal data has been accessed without authorization, he/she will notify and work with the authorities to investigate the crime and to protect the victims' identities and other personal data. To the extent possible, and in adherence to the Classcraft Privacy Policy, the Data Protection Officer will also warn the victims of the theft so that they can take appropriate steps.