

**Nanuet Union Free School District
Vendor Agreement**

1. Notwithstanding any of the above, the parties agree that New York State Education Law sections 2-d, 101, 207 and 305 and its implementing regulations (Part 121) must be strictly adhered to by the software provider, its agents, officers, employees and third part contractors.
2. The software provider specifically incorporates into this agreement the District Bill of Privacy Rights attached to this agreement as Exhibit A and it agrees to fully abide by them. The additional information required for each agreement will also be included as an attached to the Bill of Rights.
3. In addition, the software provider agrees to the following as provided in 8 NYCRR 121:
 - a. To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;
 - b. To comply with the data security and privacy policy of the educational agency with whom it contracts, Education Law § 2-d, and 8 NYCRR 121;
 - c. To limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
 - d. To not use the personally identifiable information for any purpose not explicitly authorized in its contract;
 - e. To not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student: (i) except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or (ii) unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.
 - f. To maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
 - g. To use encryption to protect personally identifiable information in its custody while in motion or at rest; and
 - h. To not sell personally identifiable information 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.
 - (b) Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.
4. The software provider shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.

5. The software provider also acknowledges the accuracy of Appendix B to this agreement regarding its Data and Security Procedures.
6. The software provider must cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.

Vendor Agreement – This Section To Be Completed By Vendor

Bill of Rights Supplemental Information (to be filled out for each software/online package: The supplemental information must be developed by the educational agency and include the following information:

(1) List the exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

To provide the District with the functionality of the Classcraft software and applications.

(2) Explain 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 or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d); 6

Classcraft will ensure that a contract is in place between it and any subcontractor or other third party entity that receives Protected Data via the Classcraft platform. The contracts will specify that the Protected Data may only be used for limited and specified purposes that are consistent with the applicable state and federal laws, and that the recipient of the Protected Data will provide the same level of protection as agreed to under this MLSA. Classcraft will remain liable for the acts and omissions of its subcontractors and other third party entities who receive Protected Data.

(3) State the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed).

Contracts are either annual or multi-year. Upon expiration of the contract, data will be destroyed according to the procedures outlined in Privacy Policy (<https://www.classcraft.com/privacy-policy/>). Deletion of data will take place within a reasonable delay following a written request from the district to wecare@classcraft.com.

(4) State 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;

contacting the student's teacher, school or district and asking them to verify or modify the data.

(5) State 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 and data security and privacy risks mitigated; and

Data is stored on Amazon and Google servers located within the USA. Security measures are explained in our Data Security Policy, copy attached.

(6) Explain how the data will be protected using encryption while in motion and at rest.

Data is encrypted (military grade) both in transit and at rest.

Data Security and Privacy

(1) Outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;

Third-party contractor will perform periodic reviews of the relevant state, federal and local requirements and will adjust its policies within a reasonable time frame in order to ensure compliance.

(2) Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract;

Please see attached data security policy for this, as the answer is too long for this space.

(3) Demonstrate that it complies with the requirements of Section 121.3(c) of this Part (Bill of Rights);

Contractor undertakes to comply with the Nanuet Privacy Bill of Rights for Parents and Students. The Data Security Policy of the contractor details the practices in place to ensure compliance, including data security measures, oversight of subcontractors, procedures to challenge the accuracy of student data, data breach and notification, etc.

(4) Specify how officers or employees of the third-party contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

Officers and employees are trained on the confidentiality required by federal and state laws upon hiring and are required to sign a confidentiality agreement before commencing employment;

(5) Specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

Classcraft will ensure that a contract is in place between it and any subcontractor or other third party entity that receives Protected Data via the Classcraft platform. The contracts will specify that the Protected Data may only be used for limited and specified purposes that are consistent with the applicable state and federal laws, and that the recipient of the Protected Data will provide the same level of protection as agreed to under this MLSA. Classcraft will remain liable for the acts and omissions of its subcontractors and other third party entities who receive Protected Data.

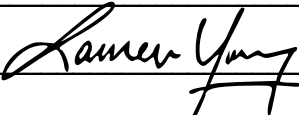
(6) Specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

Contractor will follow the data breach and notification procedure in the contractor's Data Security Policy as attached.

(7) Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

Data will be deleted upon request from the district. Data can be provided to the district in readable form should they request it upon termination of the contract.

Vendor: _____ Classcraft Studios Inc. _____

Signature: _____  _____

Date: _____ November 19, 2020 _____

Data Security Policy

Updated April 1, 2020

1. Purpose of This Policy

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 Classcraft, all branch locations, all employees and all contractors working on behalf of Classcraft.

2. Data Collected

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 fully informed about what data is being collected and for what purpose.

Classcraft only uses personal information for the purposes for which it is collected, unless the individual consents in writing to other uses. Classcraft does not allow third parties (such as marketing agencies) to have access to collected personal information.

Protected Data

Classcraft collects student, teacher and parent data for the use of its software. This data is considered Protected Data and will be exclusively used to provide services to these users and to educational agencies. Protected Data is not used for any other purpose than those explicitly authorized by the users (in the case of individual licenses) and the agencies (where a contract is entered into directly with an educational agency). Protected Data received by Classcraft or any of its subcontractors, assignees, or other authorized agents, is not sold, or released or used for any commercial or marketing purposes.

Research

Where it is not prohibited by agreement with educational agencies, Classcraft may use de-identified Protected Data for research purposes with the following goals:

- To improve the Classcraft product
- To study the effectiveness of the Classcraft product

3. Roles and Responsibilities

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

These people have key areas of responsibility:

- The **Chief Executive 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.
 - Ensuring data protection training for the people covered by this policy.

- The **Data Protection 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 Protected Data or other 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.
 - Handling data protection questions from staff and anyone else covered by this policy.

- The **Chief Financial Officer**, presently Lauren Young, is responsible for:
 - Ensuring that all Classcraft 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.
 - Handling requests from individuals to see the data Classcraft holds about them or their children under the age of 18 ("Subject Access Requests").
 - Handling any requests from schools and districts and other education agencies
 - Handling any requests from government, law enforcement agencies and other third parties
 - 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.

4. Policies

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Each user shall be provided with by a unique user ID so that individuals can be held accountable for their actions.
- Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.
- The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.
- 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 and to understand the various laws and agreements covering data security.
- Strong passwords must be used and they should never be shared. The Data Protection Officer will set requirements for password length, complexity and expiration. Employees should ensure the screens of their computers are always locked when left unattended (screen saver with password).
- Passwords that give access to sensitive data should not be stored using the “autofill” abilities of browsers or other similar software. Use of a company approved secure password manager application is required.
- Protected 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 Protection Officer if they are unsure about any aspect of data protection.
- Each user shall read and sign a Protected Data Security Agreement.

Network Access

- All employees and contractors shall be granted network access in accordance with business access control procedures and the least-privilege principle, and shall access data and systems only if there is a business need to do so and they have approval from higher management.

- Segregation of networks shall be implemented as recommended by the company's network security research. Network administrators shall group together information services, users and information systems as appropriate for the required segregation.
- De-identified data used for research purposes will be stored on separate servers
- Network routing controls shall be implemented to support the access control policy.
- Role-based access control (RBAC) will be used to secure access to all Protected Data.
- The Data Protection Officer will promptly remove all access privileges for terminated employees or subcontractors.

Technical Practices

The Data Protection Officer will implement reasonable technical and operational practices to protect against unauthorized access to Protected Data, including but not limited to the following:

- Ensure that all Protected Data is encrypted both at rest and in transit;
- Ensure that all Protected Data is only retained or deleted in accordance with the Classcraft Privacy Policy or any overriding agreements with educational agencies;
- Maintain an inventory of authorized devices;
- Maintain an inventory of authorized software;
- Maintain secure configurations for hardware and software on all mobile devices, workstations and servers;
- Perform periodic vulnerability assessments;
- Maintain a control system for use of administrative privileges;
- Maintain audit logs;
- Maintain email and web browser protections;
- Maintain malware defenses;
- Limit and control network ports, protocols and services;
- Maintain a data recovery protocol;
- Maintain secure configurations for network devices and boundary defenses;
- Control access to data based on the need to know;
- Maintain wireless access controls;
- Maintain account monitoring and control;
- Utilize application security software; and
- Maintain an incident response plan and an incident log.

Oversight of Subcontractors

Classcraft will ensure that a contract is in place between it and any subcontractor or other third party entity that receives Protected Data via the Classcraft platform. The contracts will specify that the Protected Data may only be used for limited and specified purposes that are consistent with the applicable state and federal laws, and that the recipient of the Protected Data will provide the same level of protection as may be required under agreements with educational agencies.

Compliance Review

The Data Protection Officer and the Chief Financial Officer will perform a review at least once per year of the data security and privacy policies and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of the user agreements with educational agencies. In the event Vendor's policy and practices are not in conformance, the Data Protection Officer will implement commercially reasonable efforts to ensure such compliance.

5. Access to Data for Other Reasons

Challenging Accuracy of Protected Data

Users have access to their personal information via their Classcraft user account, or by contacting their teacher or school's administration. Users may also request a copy of their personal information, or can make modifications to any incorrect information by sending a written request to support@classcraft.com. The user will then be contacted by a member of the Classcraft team for verification purposes. Users can also correct and update their personal information using the same procedures described above. In the case of individuals under the age of 18, Classcraft will provide access to this data to a parent or legal guardian.

Requests from Government and Law Enforcement

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. Where required by specific agreements with educational agencies, Classcraft will notify the relevant agencies of the request, unless prohibited to do so.

6. Data Breach and Notification

The Data Protection Officer shall be responsible for the monitoring of all systems to detect any data breach or unauthorized release of Protected Data and will promptly and thoroughly investigate any suspected breach or unauthorized release.

In the event of a breach or unauthorized release, he/she shall promptly convene an incident response team consisting of the Chief Executive Officer, the Data Protection Officer and the Chief Financial Officer, along with outside legal counsel if needed.

Upon discovery of a data breach or unauthorized release, the incident response team will take immediate action to:

- Ensure that the incident was fully investigated
- Take immediate actions to prevent a further breach or unauthorized release of Protected Data
- Determine what data was compromised
- Determine all affected parties
- Notify all affected parties

Notification of affected parties shall proceed in the following manner:

- Notification of affected education agencies with whom there is a data security agreement or by specific legislation will be done according to the terms of the related data security agreement or related legislation.
- Notification of users not covered by a data security agreement with an education agency or by specific legislation shall be made within the 7 days following the verification of the security breach.

Affected parties will receive a notification by email stating the following information:

- A list of the types of Protected Data that were or are reasonably believed to have been the subject of a breach
- 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
- 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
- A general description of the breach incident, if that information is possible to determine at the time the notice is provided
- Information about the steps that have been taken to protect individuals whose information has been breached

- Advice on steps that the person whose information has been breached may take to protect himself or herself.

7. Privacy Policy

Classcraft aims to ensure that individuals understand what data Classcraft is collecting related to them, how it is being used and how to exercise their rights with respect to such data.

To these ends, Classcraft has a Privacy Policy setting out how Classcraft handles user data.

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