DATA PRIVACY AGREEMENT

FABIUS-POMPEY CENTRAL SCHOOL DISTRICT
and
EDCLUB, INC

This Data Privacy Agreement ("DPA") is by and between the [Fabius-Pompey Central School District] ("EA"), an Educational Agency, and EdClub, Inc, a Maryland corporation ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to market products or services to students.
3. **Disclose**: To permit access to, or the release, transfer, or other communication of Personally Identifiable Information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.

12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

   In order for Contractor to provide certain services ("Services") to the EA pursuant to Contractor's standard Terms of Service and Privacy Policy (collectively, the "Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations. Contractor's current standard Terms of Service and Privacy Policy can be found using the following links: https://www.edclub.com/terms and https://www.edclub.com/privacy. EA hereby acknowledges that it has reviewed and approved Contractor's current standard Terms of Service and Privacy Policy prior to signing this DPA.

2. **Authorized Use.**

   Contractor has no property rights or claims of ownership to PII, and Contractor must not use PII for any purposes other than to provide the Services set forth in the Service Agreement and/or as otherwise permitted by applicable law. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. **Data Security and Privacy Plan**.
   Contractor shall adopt and maintain reasonable administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies as communicated to Contractor in writing. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan (entitled Information Security and Acceptable Use Policy) is attached to this DPA as Exhibit C. EA hereby acknowledges that it has reviewed and approved Contractor's said Data Security and Privacy Plan prior to signing this DPA.

4. **EA's Data Security and Privacy Policy**
   State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies as communicated to Contractor in writing.

5. **Right of Review and Audit.**
   Upon request by the EA and to the extent required by law, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, to the extent required by law, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at EA's sole cost and expense, and provide the audit report to the EA. Any such audits: (i) shall not occur more frequently than once per calendar year; and (ii) shall be limited in scope to data received by Contractor from EA (expressly excluding the data of Contractor's other customers). Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit pursuant to the foregoing.

6. **Contractor's Employees and Subcontractors**.
   (a) Contractor shall only disclose PII to Contractor's employees, agents and Subcontractors who need to know the PII in order to provide or assist with the Services. Contractor shall ensure that all such employees, agents and Subcontractors comply with the terms of this DPA.
   (b) Contractor must ensure that each Subcontractor performing functions pursuant to the Service Agreement where the Subcontractor will receive or have access to PII is contractually bound by a written agreement that, at a minimum, includes confidentiality and data security obligations materially similar to those found in this DPA.

(c) If at any point a Subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such Subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such Subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the Subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

(d) Contractor shall take full responsibility for the acts and omissions of its employees and Subcontractors.

(e) Except as provided herein and/or in the Service Agreement, Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training, materials and/or information (written or oral) on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its Subcontractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA, or required or permitted by law. Upon written request by the EA, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a reasonable format agreed to by the Parties to the EA.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall, upon written request by the EA, ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable,

read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) Upon written request by the EA, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that Contractor and/or its Subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data. Notwithstanding anything in this DPA to the contrary, any de-identified data may be used and/or retained by Contractor for any purposes allowed by law.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII (specifically excluding de-identified data) for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office.

(b) Notifications required under this paragraph must be provided to the EA at the following address:
Name: Karissa Graham
Title: DPO
Address: 1211 Mill St, Fabius, NY 13063
Email: kgraham@fabiuspompey.org

13. **Cooperation with Investigations.**
Contractor agrees that it will reasonably cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is solely attributable to Contractor or its Subcontractors.

14. **Notification to Individuals.**
Where a Breach of PII occurs that is solely attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. **Termination**.
The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.
Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. **Bill of Rights for Data Privacy and Security**.
As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**
In the event of a conflict between and among the terms and conditions of this DPA (including all Exhibits attached hereto and incorporated herein) and the Service Agreement, the terms and conditions of the Service Agreement shall govern and prevail.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

3. Section Headings.

The section and other headings contained in this DPA are for reference purposes only and shall not affect the meaning or interpretation of this DPA.

4. Venue.

ANY CAUSE OF ACTION RELATING TO OR ARISING OUT OF THIS DPA SHALL ONLY BE BROUGHT IN A COURT LOCATED IN MARYLAND (THE "MARYLAND VENUE"). THE PARTIES HEREBY CONSENT TO THE EXERCISE OF PERSONAL JURISDICTION BY THE MARYLAND VENUE (TO THE EXPRESS EXCLUSION OF ALL OTHER JURISDICTIONS).

5. Modifications to Form; Drafting.

The Parties hereby acknowledge that the format of this DPA is based on the New York State Model Data Privacy Agreement for Educational Agencies (the "NY Form"), **but that the contents of this DPA materially differ from the contents of the NY Form**. The Parties further acknowledge that they have carefully reviewed this DPA prior to signing. The Parties agree that no presumptions or interpretations against the drafting party shall apply.

6. Minimum Legal Requirements

Notwithstanding anything contained in this Agreement or any EA policies to the contrary, to the extent any obligations of Contractor contained in this Agreement and/or any EA policies extend beyond the minimum requirements for third party contractors under applicable law, Contractor shall only be required to comply with such obligations if the EA purchases at least $5,000 worth of Contractor products for a given academic year. For purposes of giving effect to the foregoing, any provisions in this Agreement and/or any EA policies that extend beyond the minimum requirements for third party contractors under applicable law shall be inapplicable to Contractor.

EDUCATIONAL AGENCY	CONTRACTOR
BY: Name & Title: Karissa K. Graham, DPO Signature: Karissa K Graham	BY: Mohsen Attarpour
Karissa Graham	Mohsen Attarpour
DPO	Authorized Person for EdClub, Inc
Date: 4/29/24	Date: 5/3/2024

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: [Karissa Graham, 1211 Mill St, Fabius, NY 13063 (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	Mohsen Attarpour
[Printed Name]	Mohsen Attarpour
[Title]	Authorized Person for EdClub, Inc
Date:	5/3/2024

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	*EdClub, Inc*
Description of the purpose(s) for which Contractor will receive/access PII	*Providing a subscription to EdClub products as licensed. EdClub products include web-based education tools to teach users skills such as touch typing, digital citizenship, spelling and vocabulary (among others).*
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date: 4/29/24_____ Contract End Date: No end date unless specified by one of the parties involved
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☒ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: *Data will be stored on servers located within the United States of America. Contractor will store and process data in accordance with commercial best practices, including implementing appropriate safeguards.*
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	Mohsen Attarpour
[Printed Name]	Mohsen Attarpour
[Title]	Authorized Person for EdClub, Inc
Date:	5/3/2024

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

[Exhibit C is contained on the following page(s) – See attached]

EDCLUB, INC.
INFORMATION SECURITY AND ACCEPTABLE USE POLICY

1. Overview

All EdClub Information Systems that Employees use to carry out their job functions are the property of EdClub. Information Systems are to be used for business purposes in serving the interests of the company and our clients in the course of normal business operations.

Effective security is a team effort requiring the participation and support of every Employee who handles information and/or Information Systems. Every Employee is responsible for knowing, and conducting their activities in accordance with, this policy.

2. Purpose

The purpose of this policy is to establish rules governing the acceptable use of EdClub's Information Systems. These rules are designed to protect EdClub, its clients, and its Employees. Failure to adhere to this policy will expose EdClub, its clients, and its Employees to risks, including potential cybersecurity attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to all EdClub Employees and Information Systems. All EdClub Employees are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with EdClub policies and standards, as well as and local laws and regulations. Exceptions to this policy are documented in Section 5.2.

4. Policy

4.1 General Use and Ownership

4.1.1 EdClub Confidential Information stored on Information Systems remains the sole property of EdClub. Employees must ensure that Confidential Information is protected in accordance with the *Data Protection Standard.*

4.1.2 Employees have a responsibility to promptly report the theft, loss, or unauthorized access to or disclosure of EdClub proprietary information.

4.1.3 Employees may access, use, or share EdClub Confidential Information only to the extent it is authorized and necessary to fulfill their assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Information Systems. If there is any uncertainty, Employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized Employees may monitor equipment, systems, and network traffic at any time, in accordance with the *Audit Policy*.

4.1.6 EdClub reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.1.7 Employees must protect all Confidential Information, including by not sharing, posting, publishing, commenting on, or otherwise disclosing Confidential Information unless they are explicitly authorized to do so.

4.2 Security and Proprietary Information

4.2.1 Employees must use extreme caution when opening email attachments, which may contain malware. Even emails that appear to be sent by coworkers may be malicious. Upon receipt of an email that looks out of the ordinary or suspicious, Employees shall check with the sender before opening any attachments.

4.2.2 Employees must be alert for potential phishing attacks. Phishing is a type of attack usually carried out through malicious emails, in which the sender pretends to be a credible source and requests sensitive information. Attackers can set up web sites under their control that look and feel like legitimate web sites. Phishing emails often have an immediate call to action that ask the recipient to "update your account information" or "login to confirm ownership of your account." Employees who suspect a phishing attack shall refrain from clicking on any links or opening any attachments, close the email, and report the situation to their supervisor immediately.

4.2.3 Employees shall not import any files that were created outside of EdClub's Information Systems into its Information Systems until those files are first scanned for viruses by an anti-virus program. Similarly, Employees shall not attach devices, including USB keys, to Information Systems unless they have prior approval.

4.2.4 All electronic devices that connect to Information Systems shall comply with the *Minimum Access Policy*.

4.2.5 System-level and user-level passwords shall comply with the *Password Policy*. Employees are prohibited from providing access to another individual, either deliberately or through failure to secure access.

4.2.6 All Information Systems shall be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Employees shall lock the screen or log off when the device is unattended.

4.2.7 Public communications by Employees that use an EdClub email address shall contain a disclaimer stating that the opinions expressed are strictly the Employees' own and not necessarily those of EdClub, unless posting is in the course of business duties.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of performing their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Any exemption from these restrictions must be approved by EdClub in writing before the conduct occurs.

Under no circumstances may an EdClub Employee engage in any activity that is illegal under local, state, federal, or international law while using Information Systems or Confidential Information.

The examples below are not exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

(a) Violations of the rights of any person or company protected by copyright, trade secret, patent, intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by EdClub. Employees shall not download software without the approval of a supervisor.

(b) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources; or copyrighted music.

(c) Accessing Information Systems for any purpose other than conducting EdClub business.

(d) Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws. Employees must consult a supervisor before exporting regulated materials.

(e) Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

(f) Revealing account passwords to non-Employees or allowing account access by others, including family and other household members.

(g) Using Information Systems to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the Employee's local jurisdiction. Please see the *EdClub Employee Handbook* for additional information related to EdClub's policy against unlawful harassment.

(h) Making fraudulent offers of products, items, or services originating from any EdClub account.

(i) Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these activities are in the scope of normal job duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

(j) Port scanning or security scanning, unless prior written notification to EdClub has been made or these activities are part of the Employee's job function.

(k) Executing any form of network monitoring that will intercept data not intended for the Employee's host, unless this activity is a part of the Employee's normal job function.

(l) Circumventing user authentication or security of any host, network, or account.

(m) Introducing honeypots, honeynets, or similar technology on Information Systems.

(n) Using any program, script, or command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via Information Systems.

(o) Providing information about, or lists of, EdClub Employees or customers to third parties outside EdClub.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, Employees must realize they represent the company.

The following activities are strictly prohibited, without exception:

(a) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material, to individuals who did not specifically request such material (email spam).

(b) Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages. Employees may not send harassing, intimidating, offensive, abusive, threatening, menacing, or hostile content to anyone by any means.

(c) Unauthorized use, or forging, of email header information.

3.1 Impersonating anyone else, whether inside or outside the company.

(d) Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.

4.3.3 Social Media and Blogging

(a) Employees are prohibited from using or accessing Social Media or blogging at work for non-EdClub-related reasons. Employees are not prohibited from using social media or blogging outside of work, but any posts, messages, videos, or pictures provided outside of work shall not be related to EdClub, its business practices, intellectual property, trade secrets, trademarks, logos, or other associated information.

(b) Use of Social Media or blogging for EdClub-related reasons, whether using EdClub's property and systems or personal computer systems, is subject to the terms and restrictions set forth in this policy. All EdClub-related online dialogue shall be conducted in a professional and responsible manner. Such dialogue shall not otherwise violate EdClub's policies or be detrimental to EdClub's best interests. Employees shall not engage in any dialogue that may harm or tarnish the image, reputation and/or goodwill of EdClub and/or any of its Employees. Use of Social Media or blogging from EdClub's systems is also subject to monitoring.

(c) EdClub's *Data Protection Standard* also applies to social media and blogging. As such, Employees are prohibited from revealing any Confidential Information when engaged in Social Media or blogging.

(d) When using Social Media or blogging, Employees are prohibited from making any discriminatory, disparaging, defamatory, or harassing comments or otherwise engaging in any conduct prohibited by EdClub's policy against unlawful harassment. Please see the *EdClub Employee Handbook* for more information.

(e) Employees may not attribute personal statements, opinions, or beliefs to EdClub when using Social Media or engaged in blogging. Unless authorized to speak on behalf of the company via Social Media, Employees shall never claim to speak on behalf of EdClub or express an official company position in such communications. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee shall not, expressly or implicitly, represent that he or she is representing EdClub's viewpoint. Employees assume any and all risks associated with blogging.

(f) Employees will be held accountable for the information they share online. Any information shared, published, posted, or otherwise disclosed on the Internet should not adversely affect EdClub's image, reputation or good will. Employees are personally responsible for what they share, even if they attempt to modify or delete it. Should EdClub or its clients, agents or assigns suffer any adverse consequences based upon an Employee's violation of this Policy, EdClub reserves the right to hold that Employee fully accountable for its losses.

5. Policy Compliance

5.1 Compliance Measurement

EdClub will verify compliance with this policy through various methods, including but not limited to, business tool reports and internal and external audits. Employees learning of any misuse of Information Systems or violations of this policy must notify management immediately.

5.2 Exceptions

Nothing in this Information Security and Acceptable Use Policy is intended to limit, restrict, inhibit, or interfere in any way with an employee's right to discuss with others and/or post any workplace concerns including wages, hours, terms, and conditions of employment.

Any exception to the policy must be approved in writing by EdClub in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

"Confidential Information" shall mean important or valuable business information that is not available to the public or personal information. Confidential information includes: Personal Information; customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; Employee information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

"Data Breach" shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

"EdClub" or "company" shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

"Employees" shall mean EdClub's employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

"Information Systems" shall mean EdClub's network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub's business purposes or that EdClub permits to access EdClub's Information Systems, such as Employees' personal mobile phones to the extent that Employees use such personal devices for EdClub's business purposes.

"Personal Information" shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

"Social Media" shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub's internal networking tools.

EDCLUB, INC.
DATA PROTECTION STANDARD

1. Overview

EdClub creates, receives, uses, and stores various data, including trade secrets and data about customers. It is the responsibility of every Employee to collect, protect, use, and disclose data only in accordance with this Data Protection Standard ("Policy").

2. Purpose

This Policy establishes EdClub's rules regarding data protection for Confidential Information.

3. Scope

This Policy applies to Employees and others who may have access to EdClub's Information Systems.

4. Policy

4.1 Confidentiality of Confidential Information

4.1.1 EdClub invests substantial resources in creating and using various types of data. Improper use or disclosure of data could create legal risk for the Company and result in loss of a competitive advantage. All Confidential Information shall be protected against misuse, Data Breach, and improper or inadvertent disclosure, as described below.

4.1.2 These rules apply regardless of whether Confidential Information is stored electronically, on paper, or in any other medium.

4.1.3 Employees shall not use Confidential Information for private or commercial purposes, disclose it to unauthorized persons, or use or disclose it in any other unauthorized way. Supervisors shall inform their Employees at the start of the employment relationship about the obligation to protect Confidential Information. This obligation shall remain in force even after employment has ended. Confidential Information shall not be distributed, repurposed, or shared without authorization. For example, Confidential Information should not appear in URLs, error messages, or other public-facing data.

4.1.4 Personal Information shall only be collected to the extent that it is required for the specific purpose of which the data subject has been given notice. Any Personal Information that is not necessary for that purpose shall not be collected.

4.1.5 Confidential Information shall not be kept longer than is necessary for a legitimate business purpose. Such information shall be destroyed or erased from EdClub's systems when it is no longer required.

4.1.6 Private keys shall be kept confidential and protected, whether in transit or at rest. Keys shall be randomly chosen, and will allow for retrieval of information for administrative or forensic use.

4.2 Data Security

4.2.1 All Employees shall implement appropriate measures designed to ensure the confidentiality, security, and availability of Confidential Information.

4.2.2 Confidential Information shall be encrypted when in transit and at rest consistent with current best practices, such as the most recent National Institute for Standards and Technology ("NIST") guidelines.

4.2.3 Information Systems shall run operating systems and firmware currently supported by their developers. Operating systems shall be configured according to current best information security practices. Operating systems and firmware shall be kept current with the latest viable patches.

4.2.4 Devices capable of doing so shall have installed anti-virus software that shall be configured to run scheduled scans and to obtain the latest definitions as they become available. Anti-virus software shall be approved by management before use.

4.2.5 Upon termination of employment, Employees shall return all EdClub devices to EdClub, including mobile devices, laptops, USB keys, and physical media containing Confidential Information. As soon as possible after receiving devices back from Employees, and in any event before permitting another Employee to use the device, EdClub shall erase, destroy, and render unreadable all Confidential Information on the devices in its entirety in a manner that prevents its physical reconstruction through the use of commonly available file restoration utilities.

4.2.6 Employees shall participate in ongoing information security training approved by management.

4.2.7 Consistent with reasonable best practices, Employees shall implement a comprehensive secure development lifecycle system, including policies, training, audits, testing, emergency updates, proactive management, design reviews, code reviews, a change management process, and regular updates to the secure development lifecycle system itself.

4.2.8 Passwords shall be stored using a non-reversible, iterative, salted, one-way cryptographic hash.

5. Compliance

5.1 Compliance Measurement

EdClub will verify compliance with this Policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, and internal and external audits.

5.2 Exceptions

EdClub must approve any exceptions to the Policy in advance.

5.3 Non-Compliance

An Employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

"Confidential Information" shall mean important or valuable business information that is not available to the public or personal information. Confidential information includes: Personal Information; customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; Employee information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

"Data Breach" shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

"EdClub" or "company" shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

"Employees" shall mean EdClub's employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

"Information Systems" shall mean EdClub's network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub's business purposes or that EdClub permits to access EdClub's Information Systems, such as Employees' personal mobile phones to the extent that Employees use such personal devices for EdClub's business purposes.

"Personal Information" shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

"Social Media" shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub's internal networking tools.

EDCLUB, INC.
MINIMUM ACCESS POLICY

1. Overview

All devices connected to Information Systems shall comply with this Minimum Access Policy (the "policy"). Compliance with these requirements is further mandated by the *EdClub Information Security and Acceptable Use Policy*.

2. Purpose

The purpose of this policy is to maintain an adequate level of security to protect the confidentiality, availability, and integrity of Confidential Information and Information Systems. This policy defines the rules necessary to achieve this protection and to ensure the secure and reliable operation of Information Systems.

3. Scope

This policy applies to all devices connected to Information Systems, all Employees, and all personnel affiliated with third parties (collectively, "Users") who have access to Information Systems. A written exception is required for any configuration that does not comply with this policy.

4. Policy

4.1 Minimum Access

4.1.1 Users shall be granted access to Information Systems and Confidential Information on a need-to-know basis. Users shall only receive access to the minimum applications and privileges required for performing their job duties.

4.1.2 Users are prohibited from gaining unauthorized access to any Information Systems or in any way damaging, altering, or disrupting the operation of these systems.

4.1.3 Information System access shall not be granted to any User without appropriate permissions.

4.2 Privileged Accounts

4.2.1 Privileged accounts used by administrators and other personnel with special permissions shall not be used for non-administrator activities. Network services shall run under accounts assigned the minimum necessary privileges.

4.3 Terminating User Access

4.3.1 Any changes in User duties or employment status shall be reported to appropriate managers. The affected User's access shall be immediately revoked if the User has been terminated. User access shall be appropriately modified if the User's work responsibilities have changed.

4.4 Use of Authentication

4.4.1 Information Systems shall require authentication by means of passphrases or other secure authentication mechanisms. Authentication requirements shall be appropriate to the type of data involved and transportation medium. EdClub shall use a third-party provider that is a recognized and trusted authority in the industry to generate any certificates used for authentication.

4.4.2 All network-based authentication shall be strongly encrypted. Traffic for one-time password authentication systems may be exempted from this encryption requirement. Users shall transmit Confidential Information only over TLS or via other secure methods, and shall use only SSL and similar technologies with appropriate safeguards in place.

4.4.3 Information Systems that are left unattended for more than 20 minutes shall be configured to log out automatically and require a User to re-authenticate. Information Systems that do not support an auto-log off function shall be secured with physical access restrictions.

4.4.4 Devices such as printers do not require authentication if the explicit purpose of the device is to provide unauthenticated access. Any devices that do not require authentication shall be physically secure and reasonable efforts shall be made to ensure that such devices are not readily accessible to unauthorized individuals.

4.5 Software Testing and Patch Updates

4.5.1 Devices connected to the EdClub network shall only run software for which timely security patches are available. All available security patches shall be applied according to a regular schedule that is appropriate for the confidentiality level of the affected data.

4.5.2 Confidential Information shall not be used in the development or testing of any products unless EdClub explicitly approves such use in writing beforehand and specific additional safeguards to protect such information are implemented.

4.6 Anti-Malware and Firewall Software

4.6.1 Anti-malware software shall be updated and running on Information Systems for which anti-malware software is available. Information Systems shall be scanned regularly for malware.

4.6.2 Host-based firewall software shall be running and configured to block all inbound traffic that is not explicitly required for the intended use of the Information System.

4.7 Information System Access Control Systems

4.7.1 All Information Systems used for EdClub business, regardless of where such systems are located, shall use an access control system approved by EdClub. In most cases this will involve password-enabled lock screens with an automatic log-off feature. Information Systems that are unlocked or unsecured shall not be left unattended for prolonged periods.

4.7.2 When a User leaves an Information System unattended, that User shall properly log out of all applications and networks. Users will be held responsible for all actions taken using devices or login credentials that are assigned to them.

4.7.3 Accounts will be locked after multiple failed login attempts. Affected Users shall be required to provide additional proof of identity to obtain access.

4.8 Confidential Information Access

4.8.1 Access to Confidential Information will be logged and audited in a manner that allows the following information to be deduced:

(a) Access time

(b) User account

(c) Method of access

(d) Privileged commands (which shall be traceable to specific User accounts)

4.8.2 All inbound access to EdClub's systems containing Confidential Information shall be logged. Audit results shall be securely stored and made available to the Data Breach Response Team in the event of any data breach.

4.8.3 Remote access to EdClub systems shall conform to this policy and shall comply with all applicable statutory requirements related to accessing and storing Confidential Information.

5. Policy Compliance

5.1 Compliance Measurement

EdClub will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, and internal and external audits.

5.2 Exceptions

Any exception to the policy must be approved by EdClub in advance.

5.3 Non-Compliance

A User found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

"Confidential Information" shall mean important or valuable business information that is not available to the public or personal information. Confidential information includes: Personal Information, customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; Employee information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

"Data Breach" shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

"EdClub" or "company" shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

"Employees" shall mean EdClub's employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

"Information Systems" shall mean EdClub's network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub's business purposes or that EdClub permits to access EdClub's Information Systems, such as Employees' personal mobile phones to the extent that Employees use such personal devices for EdClub's business purposes.

"Personal Information" shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

"Social Media" shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub's internal networking tools.

EDCLUB, INC.
PASSWORD CONSTRUCTION AND PROTECTION POLICY

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access to and/or exploitation of Information Systems and Confidential Information. All Employees and third parties with access to EdClub systems shall take the appropriate steps, outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

3. Scope

This policy applies to Employees and all personnel affiliated with third parties (collectively, "Users") that have accounts that permit access to Information Systems. This policy applies to all passwords, including but not limited to user-level accounts, system-level accounts, web accounts, email accounts, screen saver protection, voicemail, and local router logins.

4. Policy

4.1 Password Creation

4.1.1 Users shall use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their personal accounts or vice versa.

4.1.2 User accounts that have system-level privileges shall be protected by a unique password that is different from the passwords for all other accounts maintained by that User to access system-level privileges.

4.2 Password Construction

4.2.1 Password Length

Longer passwords are more secure. All passwords on EdClub systems shall be at least 10 characters long. However, a password length of at least 14 characters is recommended.

4.2.2 Password Content

We highly encourage the use of passphrases (passwords made up of multiple words). Examples include “It’s time for vacation” or “block-curious-sunny-leaves.” These passphrases are easy to remember, easy to type, and improve account security.

Your password must include at least one special character or number. We encourage you to place these characters towards the middle of the password. Placing special characters or numbers only at the end of a password greatly reduces their effectiveness in thwarting security threats.

4.2.3 Unacceptable passwords

EdClub passwords shall not display any of the following characteristics:

(a) Personal information, such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

(b) Sports or pop culture references.

(c) Obvious character substitutions, such as substituting 3 for “e” or $ for “s.”

(d) Number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

(e) Variations of “Welcome123” “Password123” or “Changeme123.”

4.3 Password Protection

4.3.1 Passwords shall not be shared with anyone, including coworkers. All passwords shall be treated as Confidential Information.

4.3.2 Passwords shall not be inserted into email messages, shared via other types of electronic communication, or revealed over the phone to anyone.

4.3.3 Passwords may only be stored in “password managers” that are authorized by the organization.

4.3.4 Users may not use the "Remember Password" feature of web browsers or other applications.

4.3.5 Any User suspecting that his or her password may have been compromised shall report the incident to management and change the password.

4.4 Password Change

4.4.1 Passwords should only be changed when there is reason to believe a password has been compromised.

4.4.2 Password cracking or guessing may be performed on a periodic or random basis by EdClub. If a password is guessed or cracked during one of these scans, the User will

be required to change it to be in compliance with the Password Construction Guidelines.

4.5 Application Development

Application developers shall ensure that their programs contain the following security precautions:

4.5.1 Applications support authentication of individual Users, not groups.

4.5.2 Applications do not store passwords in clear text or in any easily reversible form.

4.5.3 Applications do not transmit passwords in clear text over the network.

4.5.4 Applications provide for some sort of role management, such that one User can take over the functions of another without having to know the other's password.

4.6 Multi-Factor Authentication

4.6.1 Multi-factor authentication is required for accounts with access to the Personal Information that EdClub processes on behalf of its clients, and highly encouraged for other work-related accounts and personal accounts also.

5. Policy Compliance

5.1 Compliance Measurement

EdClub will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, and internal and external audits.

5.2 Exceptions

Any exception to the policy must be approved by EdClub in advance.

5.3 Non-Compliance

A User found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

"Confidential Information" shall mean important or valuable business information that is not available to the public or personal information. Confidential information includes: Personal Information; customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; Employee information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

"Data Breach" shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

"EdClub" or "company" shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

"Employees" shall mean EdClub's employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

"Information Systems" shall mean EdClub's network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub's business purposes or that EdClub permits to access EdClub's Information Systems, such as Employees' personal mobile phones to the extent that Employees use such personal devices for EdClub's business purposes.

"Personal Information" shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

"Social Media" shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub's internal networking tools.

EDCLUB, INC.
AUDIT POLICY

1. Overview

For security and network maintenance purposes, authorized Employees may monitor equipment, systems, and network traffic at any time. EdClub shall audit networks and systems in accordance with this Audit Policy ("Policy").

2. Purpose

This Policy establishes EdClub's rules regarding Audits. Audits are meant to verify that security controls are operating properly, a formal data protection system is in place, and all Employees are aware of and use that data protection system.

3. Scope

This Policy applies to all EdClub Employees and Information Systems.

4. Content of Audit

Audits shall occur at least once per year. Audits shall evaluate whether each element of EdClub's information security policies is operating as intended. Audits may also address, but are not limited to, the following questions:

4.1 Data Origin and Storage

4.1.1 From whom is the Confidential Information collected? Confidential Information obtained from residents of certain jurisdictions may be subject to specialized regulatory regimes, such as the GDPR in the European Union or the CCPA in California.

4.1.2 Where is the Confidential Information stored? Is it held on the premises or in third-party data centers?

4.1.3 What information about EdClub's data privacy and security practices has been disclosed to the source of the Confidential Information?

4.1.4 Have the purposes of the data collection been disclosed to the source of the Confidential Information?

4.2 Minimum Necessary Data

4.2.1 Has it been verified that the purposes of data collection could not be achieved effectively with less Confidential Information?

4.2.2 Is the Confidential Information being collected adequate to serve the stated purpose(s)?

4.3 Accuracy of Data

4.3.1 Have steps been taken to ensure the accuracy of the Confidential Information?

4.3.2 Is there a system of rolling reviews of Confidential Information to keep it up to date?

4.4 Data Retention

4.4.1 Is Confidential Information kept long enough to comply with relevant laws and regulations that define minimum data retention periods?

4.4.2 Is Confidential Information retained for longer than the minimum required retention period? If yes, is there a justification for doing so?

4.5 Appropriate Security Measures

4.5.1 Is the level of security adopted appropriate to the risks represented by the nature of the Confidential Information to be protected? Consideration should be given to the security of Confidential Information and the measures taken to guard against theft, computer viruses, or accidental disclosure.

4.5.2 Are Employees who handle Confidential Information aware of their responsibilities and obligations regarding that data?

4.5.3 Where consultants/contractors have access to Confidential Information, is there a data protection agreement in place that sets out the consultant's or contractor's data security obligations?

4.5.4 Are appropriate measures in place for the secure disposal and/or destruction of Confidential Information that is no longer required?

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

"Audit" means a systematic examination to determine whether activities involving the processing of Confidential Information are carried out in accordance with EdClub's policies. Audits may be performed internally by authorized individuals within EdClub or externally by third parties authorized by EdClub.

"Confidential Information" shall mean important or valuable business or personal information that is not available to the public. Confidential information includes but is not necessarily limited to: customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; personnel information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

"Data Breach" shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

"EdClub" or "company" shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

"Employees" shall mean EdClub's employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

"Information Systems" shall mean EdClub's network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub's business purposes or that EdClub permits to access EdClub's Information Systems, such as Employees' personal mobile phones to the extent that Employees use such personal devices for EdClub's business purposes.

"Personal Information" shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

"Social Media" shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub's internal networking tools.

EDCLUB, INC.
DATA BREACH RESPONSE POLICY

1. Overview

This document sets out the processes to be followed in the event that EdClub experiences a Data Breach or suspects that a Data Breach has occurred. It also includes best practices for preventing a Data Breach from recurring, and remedial measures aimed at preventing recurrence once a particular existing Data Breach has been resolved.

This policy mandates that any individual who suspects that a Data Breach has occurred or is about to occur shall contact, and immediately provide a description of the situation to their manager or a member of the Data Breach Response Team. Effective security is a team effort requiring the participation and support of every EdClub employee and affiliate who handles Confidential Information and/or information systems. Every computer user is responsible for knowing these guidelines and reporting potential theft, Data Breaches, or exposures of Confidential Information in accordance with them.

EdClub will investigate all reported Data Breaches and suspected Data Breaches to confirm whether the Data Breach occurred. EdClub shall follow the procedures in this policy if a Data Breach or suspected Data Breach is reported.

2. Purpose

The purpose of the policy is to establish the goals and procedures for responding to a Data Breach. This policy defines what a Data Breach is; roles and responsibilities of staff; and EdClub's reporting, remediation, and feedback mechanisms. The policy shall be well publicized within EdClub and made easily available to all personnel.

Through this policy, EdClub intends to emphasize the importance of data security and detecting and responding to Data Breaches, as well as how EdClub should respond in the context of its established culture of openness, trust, and integrity. EdClub is committed to protecting its customers, employees, partners, and the company itself from illegal or harmful activity by individuals, entities, or state actors, either knowingly or unknowingly.

3. Scope

This policy applies to Employees and covers all Confidential Information and Information Systems.

4. Policy

4.1 Internal Reporting

4.1.1 Anyone who becomes aware of an actual or potential Data Breach shall immediately alert EdClub management or a member of the Data Breach Response Team.

4.1.2 When reporting an actual or potential Data Breach, the following information shall be provided to the extent it is available:

(a) When the actual or potential Data Breach occurred (time and date).

(b) Description of the actual or potential Data Breach (type of Confidential Information involved).

(c) Cause of the actual or potential Data Breach or how it was discovered.

(d) Which systems are affected by the actual or potential Data Breach.

(e) Whether corrective action has occurred to remedy or mitigate the actual or potential Data Breach.

4.2 Assessing a Potential Data Breach

4.2.1 The criteria for determining whether a Data Breach has occurred include:

(a) Is Confidential Information involved? If so, is the Confidential Information of a sensitive nature?

(b) Is Personal Information involved?

(c) Has there been unauthorized access to Confidential Information or Personal Information? Was Confidential Information or Personal Information not appropriately secured, leaving it accessible to malicious actors?

4.2.2 The criteria for determining severity of a Data Breach include:

(a) The type and extent of Confidential Information, including Personal Information, involved.

(b) Whether multiple individuals have been affected.

(c) Whether the information is protected by any security measures (e.g., password protection or encryption).

(d) The person or kinds of people who may now have access to Confidential Information, electronic or computing devices, or network resources.

(e) Whether there is (or could be) a real risk of serious harm to the affected individuals.

(f) Whether there could be media or stakeholder attention as a result of the actual or potential Data Breach.

4.3 Data Breach Response Team

4.3.1 EdClub will assemble a team of experts to conduct a comprehensive response in the event of an actual or potential Data Breach.

4.3.2 The EdClub Data Breach response team will include the following individuals:

(a) The Incident Lead. This person manages the company's response efforts to any actual or potential Data Breach. The Incident Lead may be an internal EdClub employee or an external individual. This is often a legal professional who is experienced in data security matters. Responsibilities of the Incident Lead include acting as an intermediary between senior management and other employees, managing and documenting all response efforts, identifying key tasks, managing the budget and resources needed to handle a Data Breach, and analyzing response efforts to develop forward-looking best practices.

(b) Company executives. EdClub leaders shall participate in the Data Breach response team to ensure proper leadership, backing, and resources are devoted to the Data Breach response plan.

(c) IT / security personnel. These individuals will help identify compromised data and train the rest of the Data Breach response team to properly preserve evidence and safely take compromised machines offline.

(d) Customer care and human resources personnel. These individuals will help to respond to external inquiries about the Data Breach.

(e) Legal representatives. Internal or external legal data security and compliance experts will help shape any Data Breach response and minimize the risk of litigation and fines. The company's legal representatives should establish relationships with necessary outside counsel before a data breach occurs to ensure necessary support is immediately available during a Data Breach.

4.4 Actions to Take Before a Data Breach Occurs

(a) Preparedness Training. The Data Breach Response Team shall develop best practices for Data Breach prevention and preparedness for each department at the company. Each member of the Data Breach response team shall work with their department to integrate data security efforts into daily work habits. Employees shall undergo security training at least once per year.

(b) Regularly update policies. As technology advances and the company updates its systems, data security and mobile device policies shall be reviewed and updated annually or more frequently as necessary to address the adoption of new technology or other material changes in business practices. All changes to data security policies shall be clearly communicated to anyone covered under the scope of this policy.

(c) Invest in proper cyber security. The company shall periodically engage an independent third party to audit its cyber security software, encryption devices, and firewall protection to make sure these security measures are up to date and effective against potential security threats.

(d) Contract with vendors ahead of time. The company will establish relationships with forensics experts, data security attorneys, and breach notification experts to make sure these individuals are vetted and available to assist as soon as a Data Breach is suspected or has occurred.

4.5 Responding to a Data Breach

4.5.1 Each incident must be dealt with on a case-by-case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

4.5.2 The Data Breach Response Team has the discretion to make changes to this procedure to adapt to the facts of the Data Breach. The following steps shall be taken in response to a Data Breach:

(a) Record the date and time when the Data Breach was discovered, as well as the date and time when response efforts begin.

(b) Alert the Data Breach response team and external resources about the Data Breach and begin executing response procedures.

(c) Immediately contain the Data Breach. Take all affected equipment offline, but do not turn any machines off until the forensic experts arrive. Closely monitor all entry and exit points, especially those involved in the Data Breach. If possible, put clean machines online in place of affected ones. In addition, update credentials and passwords of authorized users. Secure physical areas potentially related to the Data Breach, including installing locks and changing access codes as needed.

(d) Evaluate and document the risks associated with the Data Breach, including collecting all available evidence of the Data Breach. Interview people who discovered the Data Breach and all other staff members who have information pertaining to the Data Breach.

(e) Engage legal counsel with data privacy and security expertise to assess EdClub's potential reporting obligations.

(f) Create a comprehensive communications plan that reaches all affected audiences — Employees, customers, investors, business partners, and other stakeholders. Do not make misleading statements about the Data Breach or withhold key details that could help individuals protect themselves and their information. Also, do not publicly share information that could put individuals at further risk.

(g) Develop a media strategy, including the timing, content, and method of any announcements to individuals, regulators, or the media.

4.6 Data Breach Notification

4.6.1 State and federal regulations may require EdClub to notify those who have been affected by the Data Breach, but specific requirements and deadlines for these notifications vary. The General Data Protection Regulation "(GDPR") may impose additional notification requirements for breaches involving data of individuals who live in the European Union. Therefore, the company shall engage legal counsel to help tailor the notification process to the particular circumstances of the data breach. As required by law, EdClub will provide incident response documents to relevant government regulators upon request, and will reasonably comply with requests from such regulators for follow-up actions reasonably necessary to secure Confidential Information.

4.6.2 The following general guidelines may be used when determining appropriate customer notification procedures:

(a) Maintain communication with law enforcement. In some jurisdictions, EdClub may delay notification if law enforcement believes it would interfere with an ongoing investigation.

(b) Multiple state laws may apply to one Data Breach because such laws generally depend on where the affected individuals reside, not where the business is located.

(c) If some affected individuals live in a jurisdiction that mandates notification and others live in a jurisdiction that does not, the company should notify all affected individuals to avoid the appearance of unequal treatment.

(d) Consider hiring a professional data breach resolution vendor to handle the notification process, including the administrative requirements associated with printing and mailing notification letters to affected individuals.

(e) If the breach involved data of individuals who reside in the European Union, ensure all applicable GDPR requirements are met.

4.7 Remedial Measures After a Data Breach

4.7.1 Identify lessons learned and remedial action that can be taken to reduce the likelihood of recurrence and implement the necessary administrative, technical, and physical safeguards necessary to prevent recurrence. This may involve a review of policies and training programs.

4.7.2 The following steps may be taken to prevent additional Data Breaches from occurring in the future:

(a) If service providers were involved in the Data Breach, examine whether those service providers have access to Confidential Information and consider changing, limiting, or revoking their access to such data in the future.

(b) Consider conducting an audit to reduce the likelihood of such a Data Breach reoccurring in the future.

(c) Check network segmentation to make sure the segmentation plan worked as intended.

5. Policy Compliance

5.1 Compliance Measurement

EdClub will verify compliance with this policy through various methods, including but not limited to, business tool reports and internal and external audits.

5.2 Non-Compliance

An Employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

"Confidential Information" shall mean important or valuable business information that is not available to the public or personal information. Confidential information includes: Personal Information; customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; Employee information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

"Data Breach" shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

"EdClub" or "company" shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

"Employees" shall mean EdClub's employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

"Information Systems" shall mean EdClub's network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub's business purposes or that EdClub permits to access EdClub's Information Systems, such as Employees' personal mobile phones to the extent that Employees use such personal devices for EdClub's business purposes.

"Personal Information" shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

"Social Media" shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub's internal networking tools.