

EXHIBIT D**Data Sharing and Confidentiality Agreement**

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. Purpose

- (a) This Exhibit supplements the Master License and Service Agreement (“MLSA”) to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES’ Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES’ website.
- (b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service (“TOS”) that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. Definitions

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

- (a) “Student Data” means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (b) “Teacher or Principal Data” means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (c) “Protected Data” means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor’s Product.

- (d) “Participating Educational Agency” means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor’s Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor’s Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

- (a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.
- (b) Vendor will maintain the confidentiality of all Protected Data it receives in accordance with applicable federal and state law (including but not limited to Section 2-d) and this DSC Agreement, as may be amended by the Parties, and Erie 1 BOCES’ policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, and that Erie 1 BOCES will provide Vendor with a copy of its policy upon request.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES’ Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is attached hereto and incorporated by reference herein as Exhibit D (continued). In addition, Vendor’s Data Security and Privacy Plan is attached hereto and incorporated by reference herein as Exhibit E, and Vendor’s posted Britannica Education Privacy Policy (<https://corporate.britannica.com/privacy.html>) is attached hereto and incorporated by reference herein as Exhibit E-1.

Additional elements of Vendor’s Data Security and Privacy Plan are as follows:

- (a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES’ data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor’s policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.
- (b) As required by the NIST Cybersecurity Framework, in order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA,

- a. Vendor will have the following reasonable administrative, technical, operational, and physical safeguards and practices in place throughout the term of the MLSA:
 - i. Data Security:
 - 1. Data-at-rest & data-in-transit is encrypted
 - 2. Data leak protections are implemented
 - ii. Information Protection Processes and Procedures:
 - 1. Data destruction is performed according to contract and agreements
 - 2. A plan for vulnerability management is developed and implemented
 - iii. Protective Technology:
 - 1. Log/audit records are ascertained, implemented, documented, and reviewed according to policy
 - 2. Network communications are protected
 - iv. Identity Management, Authentication and Access Control:
 - 1. Credentials and identities are issued, verified, managed, audited, and revoked, as applicable, for authorized dev
- (c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.
- (d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.
- (e) Vendor [check one] ☒ will _____ will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.
- (g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

- (a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).
- (b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.
- (c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.
- (d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:
 - (i) the parent or eligible student has provided prior written consent; or
 - (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.
- (e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;
- (f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.
- (h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

- (a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven

(7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

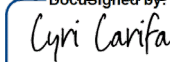
- (b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).
- (c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.
- (d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.
- (e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)**ERIE 1 BOCES****PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

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

- (1) A student's personally identifiable information cannot be sold or released for any commercial purposes.
- (2) Parents have the right to inspect and review the complete contents of their child's education record.
- (3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
- (4) A complete list of all student data elements collected by the State is available for public review at <http://www.nysed.gov/data-privacy-security/student-data-inventory>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
- (5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>.

BY THE VENDOR:


 E973001A0B94E7...
 Signature

 Cyri K. Carifa
 Printed Name

 Assistant General Counsel & DPO, CIPP/US
 Title

 May 6, 2024
 Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT

BETWEEN

ERIE 1 BOCES AND BRITANNICA EDUCATION, A DIVISION OF ENCYCLOPAEDIA BRITANNICA, INC.

Erie 1 BOCES has entered into a Master License and Service Agreement (“MLSA”) with ENCYCLOPAEDIA BRITANNICA, INC. which governs the availability to Participating Educational Agencies of the following Product(s):

Britannica Expedition: Learn!

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law (“Protected Data”).

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor’s subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: (i) ensuring that each of these subcontractors has committed to comply with requirements equal to or greater than those set forth in Processor’s contract with the Erie 1 BOCES, including, without limitation, the obligations and commitments set forth in Data Sharing and Confidentiality Agreement; and (ii) in accordance with Processor’s Vendor Management policy and procedures, auditing each sub-contractor on a no-less-than annual basis to confirm each sub-contractor’s continued and ongoing compliance with Processor’s contractual and legal obligations. In addition, as needed, Processor will enter into data protection agreements with its subcontractors.

Duration of MLSA and Protected Data Upon Expiration:

The MLSA commences on May 6, 2024 and expires on June 30, 2027.

Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.

Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.



EXHIBIT E

Data Security and Privacy Plan

INCLUDING BRITANNICA EDUCATION PRIVACY POLICY

In accordance with Section 4 of the Data Sharing and Confidentiality Agreement (the “**Agreement**”), Encyclopaedia Britannica, Inc. (the “**Processor**”) agrees that the following terms shall be incorporated into the Agreement and Processor shall adhere to both its Britannica Education Privacy Policy (<https://corporate.britannica.com/privacy.html>), a copy of which is attached hereto and incorporated by reference herein as **Exhibit E-1**, and the following Data Security and Privacy Plan:

PROCESSOR’S DATA SECURITY AND PRIVACY PLAN:

1. **Implementation of all state, federal, and local data security and privacy contract requirements over the life of the Agreement, consistent with Erie 1 BOCES’s data security and privacy policy.** In general, over the life of the Agreement and consistent and in accordance with the Erie 1 BOCES’s Parents Bill of Rights for Data Privacy and Security, Processor will implement all requirements imposed on it by federal, state, and local data security and privacy contract requirements (including, without limitation, requirements imposed by FERPA, COPPA, PPRA, IDEA, and NY Education Law 2-d) as follows:

Processor will:

- Collect and disclose students' PII only as necessary and only for educational purposes.
- Minimize the collection, processing and transmission of PII.
- Have safeguards in place to protect students' PII when it is stored or transferred. These safeguards must meet industry standards and best practices.
- Not sell, use, or disclose PII for marketing, advertising, or other commercial purposes.
- Train staff in applicable laws, policies, and safeguards associated with industry standards and best practices.
- Not maintain copies of PII once it is no longer needed for the agreed upon educational purpose. Outside parties should permanently and securely delete PII no later than when the contract ends.
- Abide by the Parents' Bill of Rights for Data Privacy and Security within their written agreement with the Erie-1 BOCES and provide supplemental information for parents about their agreement with the Erie-1 BOCES.



In addition, with respect to each of FERPA, PPRA, COPPA and NY Education Law 2-d, Processor confirms the following:

- a) **FERPA/PPRA.** The Services are designed to meet Processor's responsibilities under FERPA (including as amended by PPRA) to protect personal information from students' educational records. Processor will collect, receive and use student personal information as a "School Official" that performs an outsourced institutional function, subject to the direction and control of the BOE. Processor agrees to work with the BOE and each school to jointly ensure compliance with the FERPA regulations and the Erie 1 BOCES's data security and privacy policy to protect the confidentiality of educational records, provide parents and eligible students the opportunity to access and review such records, and limit further disclosure of personal information only as necessary to support the BOE's educational purposes.
 - b) **COPPA.** In accordance with COPPA and the Erie 1 BOCES's data security and privacy policy, Processor will not knowingly collect personal information from a child under 13 unless and until the Erie 1 BOCES or a school has authorized us to collect such information through the provision of the Services on the Erie 1 BOCES's or a school's behalf. Consistent with COPPA, Processor relies on K – 12 schools to provide appropriate consent and authorization for a student under 13 to use the Services and for Processor to collect personal information from each student. Processor uses and processes student data solely for the purpose of providing the subscribed-to services to the Erie 1 BOCES and each school and does not collect or retain student data for longer than is necessary to provide the services or as otherwise provided in our Agreement with the Erie 1 BOCES. Processor also provides subscribing schools with the opportunity to review and delete the personal information collected from their students, and Processor will work with the Erie 1 BOCES and each school to provide parents with the same level of access, upon request.
 - c) **New York State Education Law § 2-d.** Processor's practices are in alignment with the finalized provisions of New York State Education Law §2-d, and Processor confirms its commitment to upholding and adhering to the NY State model Parent's Bill of Rights and the Erie 1 BOCES's Parents Bill of Rights for Data Privacy and Security. Accordingly, Processor will:
2. **Administrative, operational and technical safeguards and practices Processor has in place to protect the Protected Information that it will receive under the contract.**



- a) Processor maintains role-based, least-privileged access to our customer data. Only those individuals with direct responsibilities for creating/deleting user accounts, providing technical support or otherwise providing the subscribed-to services as requested by a customer have access to this data and we use a ticketing system with extensive audit trails to follow through. Processor ensures that any of its employees who have access to personally identifiable information (PII) receive training on the federal and state laws governing confidentiality of such information. For those who have privileged access, they must use an individual VPN connection to access customer data when working remotely. All transactions are performed on TLS with secure authentication. Our Information Security policies contain strict policies for employees who need to transport customer data on portable devices. If an employee is switching to a new (non-privileged) role at Processor, or is leaving the company, we revoke their access on the same day.
 - b) Our building entrance is staffed with 24x7 security guards. Beyond that, our office entrance doors are always locked with receptionist(s) attending to the entrances. Every employee must use a security pass (fob) to unlock the door to enter the premises. We also maintain security cameras and monitor all the entrances and hallways. Our internal data center has an additional lock with a separate security access card—issued only to a few IT staff, along with an additional security camera. We use cloud-based inventory control software to keep close inventory of our company technology assets. When needed, we wipe all the hard disks using DoD 3-pass technique. When hardware reaches the end of life, we use a 3rd party professional firm to destroy disks in a secure way.
 - c) At the transaction level all data is transmitted over secure transmission (TLS) protocol and data is encrypted while in transit and at rest. At the database level, data is protected by firewall and username/password and other access control requirements. Personal data is stored in a secure encrypted cloud database behind web applications protected by strong firewalls. Processor conducts ongoing reviews in an effort to ensure the maintenance of its database security and conducts ongoing vulnerability management scanning, among other processes. Processor stores data provided in connection with use of its Services in the AWS Cloud and encrypts the same using an industry standard AES-256 encryption algorithm.
3. **Demonstration of compliance with the requirements of the Erie 1 BOCES's Parents' Bill of Rights for Data Privacy and Security.** To ensure compliance with the Erie 1 BOCES's Parents' Bill of Rights for Data Privacy and Security, Processor will:



- Collect and disclose students' PII only as necessary and only for educational purposes.
 - Minimize the collection, processing and transmission of PII.
 - Have safeguards in place to protect students' PII when it is stored or transferred. These safeguards must meet industry standards and best practices.
 - Not sell, use, or disclose PII for marketing, advertising, or other commercial purposes.
 - Train staff in applicable laws, policies, and safeguards associated with industry standards and best practices.
 - Not maintain copies of PII once it is no longer needed for the agreed upon educational purpose. Outside parties should permanently and securely delete PII no later than when the contract ends.
 - Abide by the Parents' Bill of Rights for Data Privacy and Security within their written agreement with the Erie-1 BOCES and provide supplemental information for parents about their agreement with the Erie-1 BOCES.
4. **Specify how officers or employees of the third-party contractor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.**
- a) **Employees and Processors.** All Processor employees receive data security and privacy training materials upon onboarding as well as annually, including using a third-party privacy training and assessment platform through which Processor requires employees to review and complete training modules and assessments on a regular basis and Processor captures a record of completion by each employee. In addition, Processor's IT policies, including its information and network security and data breach notification policies (among others) are posted for access and reference by Processor's U.S. employees and representatives on Processor's intranet site and shared with all Processor employees and representatives globally during onboarding and in connection with Processor's annual security and privacy awareness training sessions. In addition, all employees and representatives sign confidentiality agreements by which they commit to maintain and continuously ensure the confidentiality, both during and after their engagement with the Processor, of all data or information learned, received or otherwise processed by such employee or representative that relates to or is controlled by Processor or its customers and that is non-public, contains personally identifiable information, or pertains to confidential or proprietary business matters. In addition, An employee sanction procedure is in place to communicate that an employee or contractor may be disciplined for noncompliance with a policy and/or procedure and employees and contractors



are required to complete security awareness training upon hire and annually thereafter to confirm their understanding regarding their internal control responsibilities.

- b) **Third Party Service Providers.** Processor audits all third-party service providers for compliance with Processor's contractual and legal obligations and has a Vendor Management policy and procedures in place to ensure ongoing compliance by its third-party service providers. In addition, if applicable, Processor enters into data protection agreements with its third-party service providers.
5. **Specify if Processor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected.** To support Processor's systems, Processor will utilize sub-contractors that may process Protected Information as "sub-processors" on Processor's behalf and at Processor's direction to assist Processor in its performance of its obligations under its contract with the Erie 1 BOCES. To ensure Protected Information is protected, Processor will (i) ensure that each of these sub-contractors has committed to comply with requirements equal to or greater than those set forth in Processor's contract with the Erie 1 BOCES, including, without limitation, the obligations and commitments set forth in this Data Privacy and Security Plan; and (ii) in accordance with Processor's Vendor Management policy and procedures, audit each sub-contractor on a no-less-than annual basis to confirm each sub-contractor's continued and ongoing compliance with Processor's contractual and legal obligations. In addition, as needed, Processor will enter into data protection agreements with its subcontractors.
 6. **Specify how the Processor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify Erie 1 BOCES.** Processor uses a third-party service that enables Processor to perform (1) vulnerability assessments across its products and digital environment; and (2) penetration testing across its products and digital environment on a regular basis. In addition, Processor has a Data Breach Notification Policy in place that describes the steps employees need to take in the event they suspect a breach incident may have occurred (digital and physical assets included), including reporting the same to Processor's Chief Technology Officer and Data Protection Officer and General Counsel for investigation. In addition, in accordance with Processor's Incident Response Plan and this Agreement, if Processor identifies a breach or unauthorized release of PII hereunder that requires notice to the Erie 1 BOCES, Processor will:



- a) Promptly notify, without unreasonable delay, Erie-1 BOCES (by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell)) of (i) any unauthorized release or other Processing of Confidential Information, whether by the Processor, its Authorized Users or any other party that shall have gained access to the affected Confidential Information, or any other Security Incident; or (ii) any other breach of contractual obligations relating to data privacy and security under this Agreement or any other applicable Agreement (together with a Security Incident, a "Reportable Data Event"). In no event shall such notification occur more than twenty-four (24) hours after confirmation of an event described in clause (i) of the previous sentence, or more than seventy-two (72) hours after confirmation of an event described in clause (ii) of the previous sentence.
 - b) Provide will include a description of the breach that 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 Processor's investigation; and the contact information for representatives who can assist the Erie 1 BOCES.
 - c) Processor shall cooperate with the Erie 1 BOCES and law enforcement to protect the integrity of the investigation of any breach or unauthorized release of PII.
 - d) Where a breach or unauthorized release is attributed to the Processor, the Processor shall pay for or promptly reimburse the Erie 1 BOCES for the full cost of such notification.
7. **Describe whether, how and when data will be returned to the Erie 1 BOCES, transitioned to a successor contractor, at the Erie 1 BOCES's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.** Processor will retain data for the duration of the relationship and as long as necessary to permit Processor to use it for the legitimate business purposes that Processor has communicated to the Erie 1 BOCES and to comply with applicable laws and regulations and the Agreement. Upon termination of the Agreement and receipt of a written request from the Erie 1 BOCES and in accordance with any requirements in the Agreement, Processor will securely transfer any Erie 1 BOCES PII in Processor's possession to the Erie 1 BOCES in a format agreed to in writing by the parties and/or securely delete, destroy, or render unusable and such data. Certification of the same will be provided to the Erie 1 BOCES by Processor's Data Protection Officer upon receipt of a written request for the same from the Erie 1 BOCES.



EXHIBIT E-1

Britannica Education Privacy Policy

Last Updated and Effective as of: February 7, 2024

We've made some changes to our Privacy Policy.

Please know, our data collection practices have not changed, just the way we describe them to you.

In this updated Privacy Policy, we have tried to make it easier for you to understand your rights.

Britannica Education is proud to be a Student Privacy Pledge signatory.

Table of Contents

[Introduction](#)

[EU Representative and Data Protection Officer](#)

[Information that You Provide to Us](#)

[How We Use Information that You Provide to Us](#)

[Purposes of Processing the Information that You Provide to Us](#)

[Links to Other Websites](#)

[Information Collected Automatically-Opt Out & Cookie Policy](#)

[Children's Privacy & Student Data](#)

[Security of Your Information](#)

[Data Storage and Retention](#)

[Consent to Processing and Transfer of Information about You](#)

[Correcting, Updating, or Removing Personal Information; Account Deletion](#)

[Your California Privacy Rights](#)

[EU Data Subject Rights](#)

[Copyright](#)

[Business Transfers](#)

[Acceptance of Privacy Policy Terms and Conditions](#)

[Questions, Comments or Complaints](#)

Introduction

Your privacy is important to us. We understand that you are aware of and care about your own personal privacy interests, and we take that seriously. Encyclopaedia Britannica, Inc. (Britannica) provides this Britannica Education Privacy Policy to describe our and certain of our subsidiaries' policies and practices regarding the collection and use of your personal data through our Britannica Education websites, mobile applications or online services that link to this Privacy Policy (and any software provided on or in connection with these Britannica services) (collectively, the Services, and each a Service), and sets forth your privacy rights. In connection with the Britannica Education Services:



- We only collect such personal information or student data that is necessary to provide the subscribed-to Services to our institutional customers and their authorized users.
- We only use student data for the educational purposes for which it was collected.
- We only share personal information and student data with third-party vendors who help us operate and support the Services.
- The Services do not contain any third-party advertising or targeted advertising.

We recognize that information privacy is an ongoing responsibility, and so we may update this Privacy Policy to reflect changes to our personal data practices or our business. If we make any material changes to this Privacy Policy that impact your privacy rights, we will notify you by email (sent to the email address in your account) and by a notice on the Services prior to the effective date of such changes with an opportunity for you to review the same, unless otherwise required by applicable law. This Privacy Policy replaces our former privacy policy dated December 26, 2022. You can request a copy of our former privacy policy by sending an email to legal@eb.com.

EU Representative and Data Protection Officer

Britannica is headquartered in Chicago, Illinois USA. Britannica has appointed an EU representative and data protection officer for you to contact if you have any questions or concerns about Britannica's personal data policies or practices.

Our EU representative's name and contact information are:

Encyclopaedia Britannica, Inc. EU Representative
 Unity Wharf, 13 Mill Street
 London SE1 2BH UNITED KINGDOM
GDPR-EURep@eb.com

Our data protection officer's name and contact information are:

M.G. Kim
 Encyclopaedia Britannica Data Protection Officer
 325 N. LaSalle Street, Suite 200
 Chicago, IL USA 60654
dpo@eb.com

Information that You Provide to Us

Britannica protects the identity of visitors to the Services by limiting the collection of personal information. Personal information provided by you to us will not be posted or published by us, and will be shared with third parties only as provided herein. You can enjoy many of our Services and their special features without giving us your personal information.

Please see [Children's Privacy & Student Data](#) below for specific information about children's privacy and our Services.



Subscription Services

When you or an institution on your behalf subscribes to one of our subscription-based, advertisement-free Britannica Education Services, such as [Britannica School](#), [Britannica ImageQuest](#) or [Britannica LaunchPacks](#) (among others), we may collect information about you (in accordance with applicable data protection and child privacy laws), when you submit it voluntarily. Categories of information we collect include: (1) identity data, which includes your name, email address or other similar identifiers; (2) contact data, which includes postal or physical address, email address or telephone number; and (3) financial data, which includes credit card and other payment information.

In addition, we may also collect certain other types of information that, along with identity data, contact data and financial data, may be considered personal information in certain jurisdictions, such as: (1) technical data, which includes general and precise location information, your internet protocol (IP) addresses, browser type, internet service provider, referring/exit pages, the files viewed on our Services, search terms, type of device, device identifiers, statistical identifiers, operating system, and date/time stamp; (2) usage data, which includes your interaction with our Services, such as movement; and (3) marketing and communications data, which includes your preferences in receiving marketing from us.

Provision of your personal information is voluntary. However, when we need to collect your personal information in accordance with applicable law or under the terms of a contract and you fail to provide that information, we may not be able to provide you with access to our Services.

Subscribers may edit their information at any time to change, add or remove certain personal information by sending a request to edsupport@eb.com. We process your personal information to administer and manage your subscription, deliver subscriber benefits to you, inform you of prizes and other benefits or opportunities associated with your subscription and respond to your information requests. We may also use this information for legitimate business purposes that help us analyze the demographic of our subscribers and understand our users' needs and interests to better tailor our products and services to meet user needs and deliver additional services to our users.

Promotions and other special features

For certain promotions and to access certain features available throughout our Services, we collect information voluntarily submitted by you to us to deliver the requested feature (such as 'My Britannica') that may include (but not be limited to) your name, email address, city, state and age. You may edit this information at any time to change, add or remove it from our Services by sending a request to edsupport@eb.com. We process your personal information to deliver the requested feature to you and to inform you of other benefits or opportunities associated with our Services. We may also use this information for legitimate business purposes that help us understand our users' needs and interests to better tailor our products and services to meet your needs.

Payment card information

You may choose to purchase goods or services from Britannica using a payment card. Typically, payment card information is provided directly by a User, via the Services, into the PCI/DSS-compliant payment



processing service to which Britannica subscribes, and Britannica does not, itself, process or store your card information.

How We Use Information that You Provide to Us

Subscriber Communications

As a benefit of membership, Britannica subscribers may receive the following communications from us:

- **Communications related to subscription maintenance activities.** These communications may include, without limitation, notices regarding material changes to Britannica Service policies, service updates, service enhancements, and account management procedures. Since these communications are necessary to ensure Britannica provides its subscribers with the highest quality of services, our subscribers are not permitted to opt out from receipt of these communications.
- **Newsletter Communications.** As a benefit of a Britannica subscription, we may send Britannica subscribers our exclusive Britannica newsletters. To unsubscribe to a newsletter, a User can either (i) follow the instructions at the bottom of any newsletter or (ii) send an email to privacy@eb.com.
- **Communications containing information about Britannica products and services.** We may send promotional emails and other outbound communications to Britannica site subscribers regarding products and services from Britannica. Any Britannica site subscriber that does not wish to receive such product and service communications can choose to remove his or her contact information from our contact list at any time by (i) following the instructions at the bottom of any promotional email or (ii) sending an email to privacy@eb.com.

Authorized service providers

For legitimate business interests, we may share your personal information with third-party service providers that perform certain services on our behalf, such as processing credit card payments, providing cloud storage solutions, performing business and sales analysis, and supporting our Services' functionality.

Surveys

We may occasionally conduct on-line surveys. All surveys are voluntary and you may decline to participate.

Law enforcement

We also may disclose your information: In response to a subpoena or as otherwise required by law. When we believe disclosure is appropriate in connection with efforts to investigate, prevent, or take other action regarding illegal activity, suspected fraud or other wrongdoing; to protect and defend the rights, property or safety of Britannica, our Users, our employees, or others; to comply with applicable



law or cooperate with law enforcement; or to enforce our Service Terms and Conditions or other agreements or policies.

Purposes of Processing the Information That You Provide to Us

As explained above, Britannica processes your data to provide you with the subscribed-to Services. Sometimes we use third-party service providers to facilitate the delivery of the services described above, and these third-party service providers may be supplied with or have access to your personal information for the sole purpose of providing services to you on our behalf.

We also use your data for legitimate business purposes that enable us to refine our products and services to better tailor them to your needs and communicate with you about other products and services offered by Britannica. In addition, we may disclose your personal information in special legal circumstances. For instance, such information may be used where it is necessary to protect our copyright or intellectual property rights, or if the law requires us to do so.

You can update your personal information and change your marketing preferences at any time by sending an email to edsupport@eb.com.

Links to Other Websites

This Privacy Policy only governs information collected on the Britannica Education Services by Britannica. The Services also contain links to websites or content operated and maintained by third parties, over which we have no control. We encourage you to review the privacy policy of a third-party website before disclosing any personal information to the website. Do not supply Personal Information to these sites unless you have verified their security and privacy policies.

Information Collected Automatically-Opt Out & Cookie Policy

Britannica Activities & Opting Out

Like other commercial websites, Britannica and our authorized third-party service providers may use cookies (small files transferred from a website to its visitors' hard drives or browsers for record-keeping purposes), including essential, functional and analytical cookies, and other similar information gathering technologies throughout our Services to collect certain information automatically and store it in log files for a variety of legitimate business interests and purposes. This information may include (but is not limited to) internet protocol (IP) addresses, mobile device identifiers, the region or general location where your computer or device is accessing the internet, browser type, operating system and other usage information about your use of our Services, including a history of the pages you view.

Web beacons, tags and scripts may be used on our Services or in email or other electronic communications we send to you. These assist us in delivering cookies, counting visits to our Websites, understanding usage and campaign effectiveness and determining whether an email has been opened and acted upon. We may receive reports based on the use of these technologies by our third-party service providers on an individual and aggregated basis.



Britannica and its authorized third-party Service providers may use cookies, beacons and other similar technologies on our Services for legitimate business interests that enable us to allow you to navigate our websites, use our Services and access secure areas of our Services. We also use these technologies for statistical purposes and to analyze and improve the use of our Services and prepare aggregated usage reports.

We may also use your IP address to help diagnose problems with our server and to administer our website, analyze trends, track visitor movements, and gather broad demographic information that assists us in identifying visitor preferences.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Services. For more information about cookies, please visit <http://www.allaboutcookies.org>.

- **Analytics & usage data**

For our legitimate business interests, we may process your personal information for analytic purposes on all of our Services as described in this section.

Together with Google Analytics, we use cookies and software logs to monitor the use of the Services and to gather non-personal information about visitors to the Services. These monitoring systems allow us to track general information about our visitors, such as the type of browsers (for example, Firefox or Internet Explorer), the operating systems (for instance, Windows or Macintosh), or the Internet providers (for instance, Comcast) they use. This information is used for statistical and market research purposes to tailor content to usage patterns and to provide services requested by our customers.

We also have implemented Google Analytics Demographics and Interest reporting, which is a Google Analytics Advertiser feature. This tool uses cookies to collect and store standard Internet log and visitor information on our behalf, including information about what pages you visit, how long you are on the Services, how you got here, and what you click on during your visit. This Google Analytics data is not tied to personal information, so this information cannot be used to identify who you are. We use the data provided by Google Analytics Demographics and Interest reports to develop our services and content around our User demographics, interests, and behavior on our Services. You can opt out of this Google Analytics Advertiser feature using the Ads Settings located at <https://www.google.com/settings/ads>. In addition, you can use the Google Analytics Opt-Out Browser Add-on to disable tracking by Google Analytics. To delete these cookies, please see your browser's privacy settings or follow the above instructions.

Children's Privacy & Student Data

A note to minors: If you are under the age of 16, please get permission from your parent/legal guardian or school before using the Services. If we discover that we have collected any personal information from a child under the age of 16 without the proper consent required by law, we will suspend the associated account or remove that information from our database as soon as possible.



Britannica does not knowingly collect or solicit personal information from or about children under 16, except as permitted by law, contract or otherwise provided herein. If we discover we have received any personal information from a child under 16 in violation of this policy, we will delete that information immediately. If you believe Britannica has any personal information from or about anyone under 16, please contact us at privacy@eb.com.

Student Data

If you are a student with access to our Services through an Institutional Subscription License Agreement between your academic institution and us, your student service data is processed in a way that is COPPA- and FERPA-compliant. As you use the Services, you will enter student data or interact with student data that has already been entered. Under the terms of our contracts with academic institutions, we agree to act as a "School Official" as defined by the Family Educational Rights and Privacy Act (FERPA), meaning that we:

- Perform an institutional service or function for which the school or district would otherwise use its own employees;
- Have been determined to meet the criteria set forth in the school's or district's annual notification of FERPA rights for being a School Official with a legitimate educational interest in the education records;
- Are under the direct control of the school or district regarding the use and maintenance of education records; and
- Use education records only for authorized purposes and will not re-disclose from education records to other parties (unless we have specific authorization from the school or district to do so and it is otherwise permitted by FERPA).

However, FERPA requires limitations on disclosure of those records and implementation of appropriate security measures to protect those records. To help your school district comply with FERPA, we have adopted certain practices, and require that educators using this site fulfill certain responsibilities to safeguard student data.

The following statement explains our practices and your responsibilities regarding the student data processed by Britannica in connection with subscribed-to Services.

Student Data Security & Confidentiality Statement

Purposes of Data Entry

You control what student data is entered on this site and you always retain ownership of the student data. Student data entered on this site should be limited to information that is relevant to the legitimate educational purpose of improving student performance. We will not ask you to enter, and you are instructed not to enter, data about students that is not relevant to this legitimate educational purpose.

Therefore, only a minimum amount of personally identifiable student data required for the setup of the subscribed-to Service's system is requested. Additional data, not specific to the student, may also be



required to complete the subscribed-to Service's system setup, including the teacher's first and last name, class name, grade level, and school name.

Use, Disclosure, and Storage

We will use the student data to provide the subscribed-to Services to your academic institution. We will not keep the student data after you or the school district instructs us to delete it.

We will only disclose student data to authorized employees or representatives of the school institution and will not knowingly disclose the student data to any third person without express written authorization. When, at the request of the school institution, we acquire assessment or other information, including personally identifiable student data, from a third-party source we treat that information with the same confidentiality and security safeguards as though it were provided directly by the school institution. Additional agreements may be required by the third party to authorize transmission of data to us.

Your academic institution may from time-to-time request that we provide student data to third parties of its choosing. We will do so with written authorization, which acknowledges that we are providing that data as the requesting institution's agent and that once the data is received by the third party, we no longer have any control over the use or disposition of the data.

We may also use aggregated data in our research, product development, and marketing. That aggregated, non-personally identifiable data (e.g., summary or statistical data) may be shared with third parties. However, we do not use personal information or student data to market any products or services directly to students or their parents.

If we wish, from time to time, to release aggregated data that identifies a school or school district by name, we will enter into a separate agreement with the institution to authorize release and publication.

Britannica uses third-party vendors to help us provide the Services. For example, Amazon Web Services provides our cloud hosting facilities. These vendors can only use your personal information or student data to provide the contracted services, not for their own commercial purposes, and are subject to written security, confidentiality and non-disclosure obligations. If you are a Britannica institutional customer or user and would like more information on the vendors used to help provide the Services to you, please send an email to dpo@eb.com requesting more information. We do not subcontract the provision of the Services to, or share your personal information or student data with, any other third parties.

Security of Your Information

Britannica is committed to keeping your personal information and student data safe and secure. Any personal information collected through the Services is stored on limited-access servers. We maintain a comprehensive information security program and seek to use commercially reasonable organizational, physical, technical and administrative safeguards to protect these servers and the information they store from unauthorized access, use, disclosure, loss or modification. Our security measures include



(among others): encryption of data; security controls that protect the entirety of Britannica's IT infrastructure from external attack and unauthorized access; and internal policies setting out our data security approach and training for employees, including a Data Breach Notification Policy. We update and test our security technology on an ongoing basis. We strive to restrict access to your personal information to those employees who need to know that information to provide benefits or services to you. In addition, we strive to ensure that all our employees are aware of the importance of confidentiality and maintaining the privacy and security of your information.

If there is an unauthorized disclosure of personal information or student data in Britannica's possession or control, we will take steps in accordance with our written Incident Response Policy to investigate and mitigate the impact of the breach and notify affected institutional customers in the manner required by applicable laws or our contracts with the affected institutional customers. In addition, we will cooperate with our institutional customers in notifying affected students or their parents/legal guardians and in taking any other legally required actions.

Data Storage and Retention

Your personal information and student data is stored by us using Amazon Web Services (AWS) cloud storage solutions in the AWS Cloud – U.S. East (N. Virginia) Region, with backups in the AWS Cloud - Asia Pacific (Singapore) Region and Brazil (Sao Paulo) Region. We retain your information for the duration of your business relationship with us and as long as necessary to permit us to use it for the legitimate business purposes that we have communicated to you and comply with applicable law or regulations. For more information on where and how long your personal data is stored, and for more information on your rights of erasure and portability, please contact the Britannica's data protection officer at dpo@eb.com.

Consent to Processing and Transfer of Information about You

Britannica's headquarters are in the United States. Information we collect from you will be processed in the United States and may be stored, transferred to, and processed in any country where we have facilities or in which we engage third-party service providers. These countries may be outside your country of residence, including the United States, and may have different data protection laws than your country.

If you are located in the European Economic Area (EEA), Britannica collects and transfers personal data out of the EEA only: with your consent; to perform a contract with you; or to fulfill a compelling legitimate interest of Britannica in a manner that does not outweigh your rights and freedoms. Britannica endeavors to apply suitable safeguards to protect the privacy and security of your personal data and to use it only consistent with your relationship with us and the practices described in this Privacy Policy.

Correcting, Updating, or Removing Personal Information; Account Deletion



Users may opt out of certain Services or correct, update, or remove certain personal information that Britannica has collected about them through any of the means listed below. Please be sure to include the following information in your correspondence:

Your email address
Your first and last name
Your mailing address (street, city, state, zip code, and country)
The name of the Britannica Service to which the request applies

Email us at:

edsupport@eb.com

Call us at:

(800) 323-1229 (within the United States), or
(312) 347-7159 (outside the United States)
Monday - Friday, 8:00 a.m. to 6:00 p.m. (U.S. Central Time).

Write us at:

Britannica Customer Service, Attn: Removal from Mailing List
325 North LaSalle Street, Suite 200
Chicago, IL 60654-2682

Please allow up to six (6) weeks for mailed-in or faxed opt-out requests to be processed.

Account Deletion:

If you no longer wish to have a registered account, you may terminate your account by sending an email to edsupport@eb.com. Because of the way we maintain the Britannica Services, such deletion may not be immediate, and residual copies of your profile information or posts may remain on backup media for up to ninety (90) days.

Your California Privacy Rights

If you are a California resident, you are entitled to prevent sharing of your personal information with third parties for their own marketing purposes through a cost-free means. If you send a request to the address above, Britannica will provide you with a California Customer Choice Notice that you may use to opt-out of such information sharing. To receive this notice, submit a written request to privacy@eb.com, specifying that you seek your "California Customer Choice Notice." Please allow at least thirty (30) days for a response.

EU Data Subject Rights



The EU GDPR and other countries' privacy laws provide certain rights for data subjects. A good explanation of them (in English) is available on the website of the United Kingdom's [Information Commissioner's Office](#).

If you wish to confirm that Britannica is processing your personal data, or to have access to the personal data Britannica may have about you, please contact us at edsupport@eb.com.

Copyright

All of the content on the Services is copyrighted by Encyclopaedia Britannica, Incorporated, 354 N. LaSalle St., Suite 200, Chicago, Illinois 60654, or its licensors, and it cannot be redistributed or used for commercial purposes. More detailed information about Britannica's copyrights and trademarks is available on our [Copyright Notice](#) page.

Business Transfers

As we continue to develop our business, we might sell or buy subsidiaries, or business units. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Policy (unless, of course, the customer consents otherwise). Also, in the unlikely event that Britannica, or substantially all of its assets are acquired, customer information will be one of the transferred assets, and will remain subject to our Privacy Policy.

Acceptance of Privacy Policy Terms and Conditions

By using the Services, you signify your agreement to the terms and conditions of this Britannica Education Privacy Policy. If you do not agree to these terms, please do not use the Services. We reserve the right, at our sole discretion, to change, modify, add, or remove portions of this Privacy Policy at any time. If we make any material changes to this Privacy Policy that impact your privacy rights, we will notify you by email (sent to the email address in your account) and by a notice on the Services prior to the effective date of such changes with an opportunity for you to review the same, unless otherwise required by applicable law. All non-material amended terms automatically will take effect when they are posted on the Services. Please check this page periodically for any modifications. Your continued use of any of the Services following the posting of any non-material changes to these terms shall mean that you have accepted those changes. All other amended terms will take effect 30 days after you are notified of the same.

Questions, Comments or Complaints

If you have questions about Britannica or its products, visit our [Contact Us](#) page to find email addresses and other contact information for the appropriate department. To correct, update, or remove personal information, please email us at edsupport@eb.com. If you have any questions or concerns, please send an email to dpo@eb.com or privacy@eb.com.

©2024 Encyclopædia Britannica, Inc. All Rights Reserved.

