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 the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's 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.. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

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 set forth below.

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) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA:

- Maintain secure firewalls and security rules of the production environment.
- Use TLS to prevent snooping on site traffic and encryption to secure data at rest.

- Block bad requests using a web application firewall (WAF) where possible.
- Use strong passwords to prevent guessing or brute force attacks against privileged credentials.
- Employ software to monitor security settings and perform periodic security scans of the environment.
- Minimize collection of personal data (generally limited to email address, first name, and last name and a security question for LearningExpress products that do not include our resume builder functionality.)
- Ensure that production user data does not leave the Production environment.
- Maintain an audit log of account events.
- Alert administrators in the case of unusual events to speed investigation and remediation.
- Leverage the AWS shared responsibility model, which provides the facilities for security compliance but requires LearningExpress to implement them in a secure fashion. For instance, incoming traffic can be secured down to a single IP address (but this rule needs to be specified).
- Perform daily backups and deletion of old backups on a frequent basis.
- Provide ability for site patrons to view, download and delete their account details.
- Maintain network segregation between production systems and other environments.
- Patch systems on a regular basis.

A copy of EBSCO's Information Security Whitepaper has been included for your review.

(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 __✔____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)

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:

Alex Saltzman
Signature

Alex Saltzman
Printed Name

Sr. Vice President of Inside Sales
Title

11/11/2020
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND EBSCO INDUSTRIES, INC.

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with EBSCO Industries, Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

PrepSTEP for High Schools
Job & Career Accelorator
Personal Success Skills

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:

- Maintain access controls to systems and limit permissions to those needed for carrying out the subcontractors role.
- Minimize the amount of personally identifiable information collected.
- Legally require vendors to promise they will not retain any copy of data outside the LearningExpress environment and they will not try to sell any part of our data.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on [date] and expires on [date].

- 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.

For legal purposes, only the English language version of the Privacy Policy is binding. Non-english versions are translated from the English language version for your convenience.

EIS PRODUCTS AND SERVICES PRIVACY POLICY

LAST UPDATED: May 4, 2020

This EIS Products and Services Privacy Policy sets forth EBSCO Information Services' privacy practices when you use our software, mobile applications, and other products or services (collectively, "Services"), including:

Contents

To learn about the privacy practices in effect at our marketing and general audience websites and information gathered when you initiate requests for information about our products or services, please see the EIS WEBSITE PRIVACY POLICY.

This Privacy Policy applies to the following entities (collectively, "EBSCO Information Services" or "we" or "us" or "our"):

- EBSCO Information Services Division of EBSCO Industries, Inc. and its applicable subsidiaries*
- EBSCO Publishing, Inc. and its subsidiaries
- EBSCO International, Inc. and its applicable subsidiaries
- DynaMed, LLC
- Yankee Book Peddler, Inc. dba GOBI Library Solutions from EBSCO

**For a list of Data Protection Representatives see the table at the end of this Privacy Policy.*

EBSCO Information Services respects the privacy of its users and we are committed to protecting our users' privacy through our compliance with this Privacy Policy.

EBSCO Information Services wants you to have a positive experience in connection with our products and services. Our goal is to provide you with an experience that delivers the information, resources, and services that are helpful to you. In order to achieve this goal, we may collect information from you. This Privacy Policy describes our information collection practices and the privacy principles we follow.

To exercise your privacy rights or to ask us questions about this Privacy Policy or our privacy practices, you can submit a request by contacting us using any of the methods provided in the "How Can I Exercise My Rights?" section of this Privacy Policy.

What Information is Collected and How is it Used?

[Information about children's data and Services directed toward children can be found at Section I of this Policy]

A. What Information Do We Collect?

1. Personal Information: EBSCO Information Services collects, and has collected during the preceding 12-month period, the following categories of personal information (information that identifies you as an individual or relates to an identifiable individual) (collectively, "Personal Information"):

Category of Personal Information Collected**	Categories of Sources from Which Personal Information is Collected	Business or Commercial Purpose(s) for Which Personal Information is Collected	Categories of Third Parties with Whom Personal Information is Shared
Personal Identifiers	• Individuals • Customers • Service Providers (single sign-on)	• Authentication • Researcher productivity tools • Use of our Services • Product-related communications	• Service Providers (operating systems and platforms; communication providers; data analytics providers)
Other Personal	• Individuals	• Payment	• Service Providers

Information Categories	• Customers	processing • Reporting continuing education credits • Use of our Services	(payment processors) • Continuing education accrediting agencies
Commercial Information	• Individuals • Customers	• Use of our Services • Sales order processing • Billing and invoicing	• Service Providers (operating systems and platforms)
Internet or Other Electronic Network Activity Information	• Service Providers (operating systems and platforms; other information technology systems; data analytics providers)	• Delivery, operation, and security of our Services • Analytics • Improving the user experience	• Service Providers (data analytics providers; internet service providers; operating systems and platforms)
Geolocation Data	• Individuals (user's device) • Service Providers (data analytics providers; internet service providers; operating systems and platforms)	• Use of our Services features	• None
Education Information	• Individuals • Customers	• Use of our Services	• Service Providers (operating systems and platforms)

*** See Appendix for specific examples of the types of personal information included in each category.*

If you submit any Personal Information relating to other individuals to us or to our service providers in connection with our Services, you represent that you have the authority to do so and to permit us to use the information in accordance with this Privacy Policy.

2. Non-Personal Information: EBSCO Information Services collects information that does not directly reveal your identity or does not directly relate to an identifiable individual. This may include a unique identifier (unconnected to an individual's Personal Information) and related analytics and usage information that we use to track usage of our Services, track trends in our Services, administer the Services, and improve our users' experience.

B. How Do We Collect the Information?

The categories of sources from which we collect Personal Information are described in the table above.

We only collect and use Personal Information when you voluntarily provide it to us or when an institutional customer provides it to us in connection with its method of authenticating users for access to our Services, with the exception of your IP address, geolocation, and certain device information which may be automatically captured when you access our Services.

If you provide us Personal Information about others, or if others give us your Personal Information, we will only use that information for the specific reason for which it was provided to us.

In order to use some of the unique functions within our Services, a user must first complete a registration form or provide an email address that will require the user's disclosure of limited Personal Information. Such disclosure is strictly voluntary.

Because of how email communication works, you will have to disclose an email address to us if you choose to contact us or communicate with us by email.

We automatically collect non-Personal Information generated from your use of our Services. We use this non-Personal Information in the aggregate. We do not combine these types of non-Personal Information with Personal Information.

Cookies and Similar Technologies: For information about the cookies and other tracking technologies used by our Services and how to manage your settings for these cookies and technologies, please visit our Cookie Policy.

C. How Do We Use the Information?

The business or commercial purpose(s) for which Personal Information is collected is described in the table above.

We use the Personal Information we collect for the limited purposes of processing your transactions, establishing and/or verifying a person's or account holder's identity, customer service, improving and customizing our Services and their content, authorization, content processing, content classification, and providing you with information concerning our Services. We will retain this information for as long as your account is active or as needed to provide you Services, comply with our legal obligations, resolve disputes, and enforce our agreements.

For example, our EBSCOhost Service employs a personalization feature that requires completion of a registration form before a user can use that feature. The personalization feature of EBSCOhost is a powerful tool that provides users with the means to create and save histories of searches they have conducted. We believe the personalization feature is a useful tool that will enhance the user's experience with the Service, but it does require the user to provide Personal Information to us.

We use the non-Personal Information we collect to administer the Services, improve access to the Services, perform diagnostics, collect content-specific usage statistics, protect the Services and their content from inappropriate use, and improve the user's experience.

We may use the Personal Information and non-Personal Information we collect by sharing it with third-party agents, vendors, contractors, partners, or content providers of EBSCO Information Services (collectively, "Service Providers") for purposes of managing purchases of our products and services, providing access to our products and services, servicing our systems, and obtaining support services for our businesses. We are not in the business of selling Personal Information to third-parties or Service Providers and will share it with Service Providers only as we describe in this Privacy Policy. In situations where we share Personal Information with Service Providers, we ensure access is granted to the Service Providers only upon the condition that the Personal Information is kept confidential and is used only for carrying out the services these Service Providers are performing for EBSCO Information Services. As part of making the determination whether we will share Personal Information with Service providers, we will obtain assurances that they will appropriately protect and maintain the confidentiality of Personal Information consistent with this Privacy Policy and as required by applicable law.

The Personal Information we collect from you may be transferred to, and processed in, countries other than the country in which you live. These countries may have data protection laws that are different than the laws of your country. Specifically, the servers we use to provide our Services are located in the United States. This means that when we collect your Personal Information, we may process it in the United States or the country where you live. However, when we process your Personal Information, irrelevant of its processing location, we take appropriate measures, as discussed below, to ensure that your Personal Information remains protected in accordance with this Privacy Policy.

We may share your usage data related to our Services with our affiliates and certain Service Providers for purposes of providing or improving our Services. We will not disclose any information about your usage data related to our Services to unaffiliated third-parties, except as necessary to provide our Services, enhance the product experience, service the legal agreement between us and your employer or affiliated institution under which you are provided access to our Services, to enforce the terms of use, to meet our contractual obligations to report aggregated usage data to content providers, or as required by law.

We also reserve the right to disclose your Personal Information if we are required to do so by law, or in the good faith belief that disclosure of the information is reasonably necessary to comply with legal process, and to the extent permitted by applicable local law, to respond to claims, or to protect or advance the rights, property, safety, or well-being of our company, our employees, customers, or the public.

We will not use your Personal Information for automated-decision making.

In the unlikely event that all or substantially all of the assets of EBSCO Information Services or any of its applicable subsidiaries are acquired, customer information, which may include Personal Information, may be one of the transferred assets unless restricted by applicable local law, in which case the acquiring entity will be subject to the same commitments for such customer information.

D. What is Our Legal Basis for Collecting and Using Personal Information?

Our legal basis for collecting and using the Personal Information described above will depend on the Personal Information concerned and the specific context in which we collect it.

However, we will normally collect Personal Information from you only:

- where we need the Personal Information to perform a contract with you or your organization;

- where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms; or
- where we have your consent to do so.

In some cases, we may also have a legal obligation to collect Personal Information from you or may otherwise need the Personal Information to protect your vital interests or those of another person.

If we ask you to provide Personal Information to comply with a legal requirement or to provide the Services or a feature of the Services pursuant to a contract with your institution, we will make this clear at the relevant time and advise you whether the provision of your Personal Information is mandatory or not (as well as of the possible impact if you do not provide your Personal Information).

Similarly, if we collect and use your Personal Information in reliance on our legitimate interests (or those of any third party), we will make clear to you at the relevant time what those legitimate interests are.

If you have questions about or need further information concerning the legal basis on which we collect and use your Personal Information, please contact us using the contact information provided below.

E. How Do We Secure Personal Information?

EBSCO Information Services has taken appropriate technical and organizational measures to ensure that Personal Information we have collected or will collect in the future is secure. For example, we have limited the number of people who have access to Personal Information, by electronic security systems and authentication methods that guard against unauthorized access.

As a reminder, EBSCO Information Services provides links to third-party websites. These websites may not have the same privacy policies as EBSCO Information Services. We take reasonable care in recommending these websites, but we are not responsible for their content or privacy policies. We urge users to read the privacy statement of a third-party website when leaving our Services and linking to a third-party website.

We always use industry-standard technologies when transferring and receiving consumer data we receive. We have appropriate security measures in place in our physical facilities to protect against the loss, misuse, or alteration of information that we have collected from you in connection with our Services.

F. What Are My Rights?

Depending on your country or state of residency, you may have legal rights with respect to your Personal Information, including one or more of the following (each of which may be subject to certain exceptions that will be analyzed on a case-by-case basis):

Right to be Informed	An organization must provide certain information to individuals when collecting and processing their Personal Information.

Right of Access / Right to Know	Individuals have a right to obtain confirmation as to whether or not their Personal Information is being collected and/or processed. Individuals also have a right to request that an organization disclose the Personal Information it collects, uses, discloses, sells, and/or otherwise processes.
Right to Rectification	Individuals have the right to require an organization to correct inaccurate Personal Information concerning the individual and to have incomplete Personal Information completed, including by means of providing a supplementary statement.
Right to Restrict Processing	Individuals have the right to require an organization to restrict the processing of their Personal Information.
Right of Data Portability	Individuals have a right to receive a copy of their Personal Information in a portable and readily usable (structured, commonly used, and machine-readable) format that can be transmitted to certain third parties without hindrance.
Right to Object or Opt-out	Individuals can request an organization to stop processing and/or selling (if applicable) their Personal Information.
Right to Withdraw Consent	Individuals have the right to withdraw their consent to the processing of their Personal Information at any time when the processing is based on the individual's consent. Withdrawal of consent does not affect processing that occurred prior to such withdrawal (it only has future effect).
Right to Erasure or Deletion	Individuals can request the deletion of their Personal Information collected or maintained by an organization.
Right to Non-discrimination	An organization cannot discriminate against an Individual because of the exercise of their legal rights with respect to their Personal Information.
Right to not be Subject to Automated Decision Making	Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, if such processing has a legal effect or otherwise significantly affects the individual.
Right to Lodge a Complaint	If you are located in the European Union (EU) or European Economic Area (EEA), you have the right to lodge a complaint with a supervisory authority in relation to the processing of your Personal Information.

Additional Information Regarding the Right to Know and the Right to Opt-out

EBSCO Information Services does not and will not sell Personal Information to third parties for a business or commercial purpose and has not sold Personal Information to third parties for a business or commercial purpose during the preceding 12 months or at any other time. Likewise, we do not and will not sell Personal Information of minors under 16 years of age without affirmative authorization and have not sold Personal Information of minors under 16 years of age during the preceding 12 months or at any other time.

We disclose, and have disclosed during the preceding 12-month period, the following categories of personal information to third parties for a business or commercial purpose:

Categories of Personal Information Disclosed**
- Personal Identifiers
- Other Personal Information Categories
- Commercial Information
- Internet or Other Electronic Network Activity Information
- Geolocation data
- Education Information

*** See Appendix for specific examples of the types of personal information included in each category.*

Additional Information Regarding the Right to Object

If we process your Personal Information based on our legitimate interests, you can object to this processing in certain circumstances. In such cases, we will cease processing your Personal Information unless we have compelling legitimate grounds to continue processing or where it is needed for compliance and/or legal reasons. Where we use your Personal Information for direct marketing purposes, you can always object or opt-out by using the unsubscribe link in such communications or by submitting a request using any of the methods provided below.

G. How Can I Exercise My Rights?

We want to assure you that you can exercise any legal rights that you have with respect to your Personal Information. Upon request, we will tell you whether or not we have collected or processed any of your Personal Information.

If you would like to manage, change, limit, or delete your Personal Information, you can do so through your account settings within the Services or by submitting a request using any of the methods provided below.

To exercise any other legal rights with respect to your Personal Information, you may submit a request using any of the methods provided below.

We will respond to your request as soon as reasonably possible, but no later than the legally required timeframe.

To exercise your rights (or to ask us questions about this Privacy Policy or our privacy practices), you can submit a request using any of the methods below:

1. Via Web: Please click here: https://privacyportal-cdn.onetrust.com/dsarwebform/3dc851a7-8ce1-41dc-8d75-358b1fe8c84d/cd99c5d8-e12d-40bd-829b-e59b5ec502c9.html (This hyperlink will redirect to our privacy management platform provided by our vendor, OneTrust, Inc.)

2. Via Toll-Free Telephone: 1-833-705-0124

3. Via Mail: EBSCO Information Services 5724 Highway 280 E
Birmingham, AL 35242, USA

Attn: Data Privacy Officer, Legal Department

4. Via Email: privacy@ebsco.com

Verification of Requests

All requests submitted to us will be verified to ensure that the person making the request (the "Requstor") is the individual about whom we have collected Personal Information. The method we use to verify the Requestor's identity may vary based on the type of customer or user, the Services used, and the type of Personal Information we have collected. In most cases, we will require the Requestor to provide the following information when submitting a request:

- Type of Customer or User
- First Name
- Last Name
- Email Address
- Country
- State
- Legal Relationship to the Subject of the Request

We will use this identifying information to communicate with the Requestor and receive confirmation that they submitted the request, and then match this identifying information with the Personal Information we already maintain. We may also use the contact information that we already maintain to communicate with the individual to confirm that they submitted the request. In rare cases, we may ask for additional information to verify the request, which may include a signed declaration under penalty of perjury that the Requestor is the individual whose Personal Information is the subject of the request.

If the Requestor submits a request to delete Personal Information, we will separately confirm that the individual wants their Personal Information deleted.

We may deny a request if we cannot verify the identity of the Requestor to a reasonable degree of certainty or a reasonably high degree of certainty (depending on the type of request, the sensitivity of the Personal Information, and the risk of harm to the individual posed by a unauthorized request) or, in the case of a request to delete Personal Information, we may deny a request if we are not able to separately confirm that the individual wants their Personal Information deleted.

Authorized Agent

If you use an authorized agent to submit a request, we will require that you:

- provide the authorized agent written permission to act as your authorized agent; and
- verify the authorized agent's identity directly with us.

The above authorized agent requirements do not apply if you have provided the authorized agent with legally binding power of attorney in accordance with applicable law.

We may deny a request from an agent that does not submit proof that they have been authorized by you to act on their behalf.

H. What Choices Do I Have?

We understand that you may not want to allow our disclosure of your Personal Information to our Service Providers, or to let us use that information for purposes that you believe may be incompatible with the purpose for which it originally was collected or that you later may authorize. Therefore, you may contact us to inform us that you do not want to permit these uses of your Personal Information. To do so, please contact us using the contact information provided above.

It is important to us that the Personal Information we collect is appropriate and relevant to the purposes for which we intend to use it. We will use Personal Information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the person providing the information. EBSCO Information Services will take reasonable steps to ensure that Personal Information is relevant to its intended use, accurate, complete, and current.

You may sign-up to receive email newsletters or other marketing materials from us. If you would like to discontinue receiving this information, you may immediately update your email preferences free of cost by using the "Unsubscribe" link found in emails we send to you or through your account settings within the Services or by submitting a request using any of the methods provided above.

I. Collection and Use of Information from Children: Information for Parents

Most of our Services are not directed toward children. For our Services that are designed to be used by children under 16 years of age, we comply with the provisions of the Children's On-Line Privacy Protection Act ("COPPA") and other applicable laws. If a user under 16 years of age wants to use our personalization features, we ask the user to register with their first name (not considered personal information by the US Federal Trade Commission) and a unique identifier only.

To the extent we collect any information of minors under 16 years of age that is considered personal information under any applicable law, we do not and will not sell such information without affirmative authorization and have not sold such information during the preceding 12 months or at any other time.

If you are a parent and have questions about our practices, please feel free to contact us using the contact information provided above.

J. How Long Do We Retain This Information?

We retain Personal Information we collect from you where we have an ongoing legitimate business interest or other legal need to do so (for example, to provide you with a service you have requested or to comply with applicable legal, tax or accounting requirements).

When we have no further legitimate business interest or legal need to process your Personal Information, we will either delete or anonymize it or, if this is not possible (for example, because your Personal Information has been stored in backup archives), then we will securely store your Personal Information and isolate it from any further processing until deletion is possible.

EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield

EBSCO Industries, Inc. and its subsidiaries EBSCO International, Inc., EBSCO Publishing, Inc. dba EBSCO Information Services, DynaMed, LLC, Plastic Research and Development Corporation dba PRADCO Outdoor Brands, Summit Treestands, LLC, Luxor Workspaces, LLC, and Yankee Book Peddler, Inc. dba GOBI Library Solutions from EBSCO (collectively, the "EBSCO Covered Entities") comply with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (collectively, "Privacy Shield") as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Information transferred from the European Union, the European Economic Area (EEA), or Switzerland to the United States in reliance on Privacy Shield. The EBSCO Covered Entities have certified to the Department of Commerce that they adhere to the Privacy Shield Principles with respect to such Personal Information. If there is any conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield Frameworks and to view our certification, visit the U.S. Department of Commerce's Privacy Shield List at https://www.privacyshield.gov/list.

This Privacy Policy describes the types of Personal Information we collect, the types of third parties to which we disclose this information, and the purposes for which we do so. Residents of the EU, EEA, and Switzerland have the right to access the Personal Information that the EBSCO Covered Entities maintain, and in some cases, may have the right to correct or amend Personal Information that is inaccurate or has been processed in violation of the Privacy Shield Principles, to the extent allowed by law. To exercise this right, contact us at privacy@ebsco.com.

The EBSCO Covered Entities remain liable if they transfer Personal Information to third parties who process this Personal Information in a manner inconsistent with the Privacy Shield Principles.

With respect to Personal Information received or transferred pursuant to the Privacy Shield Frameworks, the EBSCO Covered Entities are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, the EBSCO Covered Entities may be required to disclose Personal Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the Privacy Shield Principles, the EBSCO Covered Entities commit to resolve complaints about their collection or use of your Personal Information. EU, EEA, and Swiss individuals with inquiries or complaints may contact the EBSCO Covered Entities by mail at 5724 Highway 280 E, Birmingham, AL 35242 USA, Attn: Data Privacy Officer or by email at privacy@ebsco.com. The EBSCO Covered Entities have further committed to refer unresolved Privacy Shield complaints to an alternative dispute resolution provider located in the U.S. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Under certain conditions, more fully described on the Privacy Shield website at https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

Questions

If you have any questions, comments, or concerns regarding this Privacy Policy or our practices, please use the contact information found at that page or provided above.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Changes to Privacy Policy

We will notify you of changes to this Privacy Policy by posting an updated policy on this page. You acknowledge that any use of our Services is based on this Privacy Policy, current at the time of use. If we make any material changes, we will notify you by email notification or a notice via the Services (such as a banner or pop-up) prior to the changes becoming effective and provide you with the ability to consent to these changes (such as an "I agree" or "OK" button, or a prominent statement indicating the changes are in effect and continued use of the Services signifies consent). We encourage you to periodically review this page for the latest information on our privacy practices.

Miscellaneous

This Privacy Policy does not apply to information collected by LearningExpress, LLC. To learn more about the information practices of LearningExpress, LLC, please visit its website, www.learningexpresshub.com

Alternative Format / Accessibility: To access this Privacy Policy in an alternative format, click here to download a PDF version. If you have accessibility questions, please contact accessibility@ebsco.com.

Do Not Track Signals: EBSCO Information Services does not recognize automated browser signals regarding tracking mechanisms, which may include 'do not track' instructions.

Data Protection Representatives

Data Protection Representative	Country of Business Registration
EBSCO International, Inc.	United Kingdom and Sweden
EBSCO Information Services SAS	France
EBSCO GmbH	Austria
EBSCO Information Services GmbH	Germany
EBSCO Information Services B.V.	Netherlands
EBSCO Information Services S.r.l.	Italy
EBSCO Subscription Services Espana S.L.U.	Spain
EBSCO Information Services s.r.o.	Czech Republic
EBSCO Sp. z.o.o	Poland

For legal purposes, only the English language version of the Privacy Policy is binding. Non-english versions are translated from the English language version for your convenience.

EIS WEBSITE PRIVACY POLICY

LAST UPDATED: January 1, 2020

This EIS Website Privacy Policy sets forth the privacy practices in effect at EBSCO Information Services' marketing and general audience websites (collectively, the "Websites") and information gathered when you initiate requests for information regarding our products or services, including:

Contents

The Websites do not include those sites which host our products, services, software, and mobile applications, which are governed by their own privacy policies.

This Privacy Policy applies to the following entities (collectively, "EBSCO Information Services" or "we" or "us" or "our"):

- EBSCO Information Services Division of EBSCO Industries, Inc. and its applicable subsidiaries*
- EBSCO Publishing, Inc. and its subsidiaries
- EBSCO International, Inc. and its applicable subsidiaries
- DynaMed, LLC
- Yankee Book Peddler, Inc. dba GOBI Library Solutions from EBSCO

**For a list of Data Protection Representatives see the table at the end of this Privacy Policy.*

EBSCO Information Services respects the privacy of its users and we are committed to protecting our users' privacy through our compliance with this Privacy Policy.

EBSCO Information Services wants you to have a positive experience at our Websites. Our goal is to provide you with an experience that delivers the information, resources and services that are helpful to you. In order to achieve this goal, we may collect information from you. This Privacy Policy describes our information collection practices and the privacy principles we follow.

To exercise your privacy rights or to ask us questions about this Privacy Policy or our privacy practices, you can submit a request by contacting us using any of the methods provided in the "How Can I Exercise My Rights?" section of this Privacy Policy.

What Information Is Collected and How is it Used?

[Information about children's data and our Websites can be found at Section I of this Policy]

A. What Information Do We Collect?

1. Personal Information: EBSCO Information Services collects, and has collected during the preceding 12-month period, the following categories of personal information (information that identifies you as an individual or relates to an identifiable individual) (collectively, "Personal Information"):

Category of Personal Information Collected**	Categories of Sources from Which Personal Information is Collected	Business or Commercial Purpose(s) for Which Personal Information is Collected	Categories of Third Parties with Whom Personal Information is Shared
Personal Identifiers	• Individuals • Customers • Service Providers (single sign-on)	• Authentication • Researcher productivity tools • Use of our Services • Product-related	• Service Providers (operating systems and platforms; communication providers; data analytics providers)

		communications	
Other Personal Information Categories	• Individuals • Customers	• Payment processing • Reporting continuing education credits • Use of our Services	• Service Providers (payment processors) • Continuing education accrediting agencies
Commercial Information	• Individuals • Customers	• Use of our Services • Sales order processing • Billing and invoicing	• Service Providers (operating systems and platforms)
Internet or Other Electronic Network Activity Information	• Service Providers (operating systems and platforms; other information technology systems; data analytics providers)	• Delivery, operation, and security of our Services • Analytics • Improving the user experience	• Service Providers (data analytics providers; internet service providers; operating systems and platforms)
Geolocation Data	• Individuals (user's device) • Service Providers (data analytics providers; internet service providers; operating systems and platforms)	• Use of our Services features	• None
Education Information	• Individuals • Customers	• Use of our Services	• Service Providers (operating systems and platforms)

*** See Appendix for specific examples of the types of personal information included in each category.*

If you submit any Personal Information relating to other individuals to us or to our service providers, you represent that you have the authority to do so and to permit us to use the information in accordance with this Privacy Policy.

2. Non-Personal Information: EBSCO Information Services collects information that does not directly reveal your identity or does not directly relate to an identifiable individual. This may include a unique identifier (unconnected to an individual's Personal Information) and related analytics and usage information that we use to track usage of our Websites, track trends in our Websites, administer the Websites, and improve our users' experience.

B. How Do We Collect the Information?

The categories of sources from which we collect Personal Information are described in the table above.

We only collect and use Personal Information when you voluntarily provide it to us, with the exception of your IP address, geolocation, and certain device information which may be automatically captured when you access our Websites.

Under limited circumstances, we also collect limited business contact information from legitimate third parties (for example, third parties that provide attendee lists or business prospect lists). This helps us to update or expand our records. If you provide us Personal Information about others, or if others give us your Personal Information, we will only use that information for the specific reason for which it was provided to us. Examples of the types of Personal Information that may be obtained from public sources or purchased from third parties and combined with information we already have about you, may include name, email address, job title, and company/institution affiliation.

In order to use some portions of our Websites, a user must first complete a registration form or provide an e-mail address that will require the user's disclosure of limited Personal Information. Such disclosure is strictly voluntary.

Because of how email communication works, you will have to disclose an email address to us if you choose to contact us or communicate with us by email.

We automatically collect non-Personal Information generated from your use of our Websites. We use this non-Personal Information in the aggregate. We do not combine these types of non-Personal Information with Personal Information.

Cookies and Similar Technologies: For information about the cookies and other tracking technologies used by our Websites and how to manage your settings for these cookies and technologies, please visit our Cookie Policy.

Social Media Features: Our Websites may use social media features, such as the Facebook 'like' button ("Social Media Features"). These features may collect your IP address and which page you are visiting on our Websites, and may set a cookie to enable the feature to function properly. You may be given the option by such Social Media Features to post information about your activities on our Websites to a profile page of yours that is provided by a third-party Social Media network in order to share with others within your network. Social Media Features are either hosted by a third party or hosted directly on the Websites. Your interactions with these features are governed by the privacy policy of the company providing the relevant Social Media Features.

C. How Do We Use the Information?

The business or commercial purpose(s) for which Personal Information is collected is described in the table above.

We use the Personal Information we collect for limited internal purposes that may include, but are not limited to, processing your transactions, establishing and/or verifying a person's or account holder's identity, customer service, improving and customizing our Websites and their content, development of products and services,

content processing, content classification, and providing you with information concerning our products and services. We will retain this information for as long as it is needed for the purposes for which it was collected, and/or to comply with our legal obligations, resolve disputes, and enforce our agreements.

We use the non-Personal Information we collect to administer the Websites, perform diagnostics, collect content-specific usage statistics, protect the Websites and their content from inappropriate use, and improve the user's experience.

We may use the Personal Information and non-Personal Information we collect by sharing it with third party agents, vendors, contractors, partners, or content providers of EBSCO Information Services (collectively, "Service Providers") for purposes of managing purchases of our products and services, servicing our systems, and obtaining support services for our businesses. We are not in the business of selling Personal Information to third parties or Service Providers and will share it with Service Providers only as we describe in this Privacy Policy. In situations where we share Personal Information with Service Providers, we ensure access is granted to the Service Providers only upon the condition that the Personal Information is kept confidential and is used only for carrying out the services these Service Providers are performing for EBSCO Information Services. As part of making that determination whether we will share Personal Information with Service Providers, we will obtain assurances that they will appropriately protect and maintain the confidentiality of Personal Information consistent with this Privacy Policy and as required by applicable law.

The Personal Information we collect from you may be transferred to, and processed in, countries other than the country in which you live. These countries may have data protection laws that are different than the laws of your country. Specifically, the servers we use to provide our Services are located in the United States. This means that when we collect your Personal Information, we may process it in the United States or the country where you live. However, when we process your Personal Information, irrelevant of its processing location, we take appropriate measures, as discussed below, to ensure that your Personal Information remains protected in accordance with this Privacy Policy.

We may share your usage data related to our Websites with our affiliates and certain Service Providers for purposes of providing or improving our Websites. We will not disclose any information about your usage data related to our Websites to unaffiliated third-parties, except as necessary to enhance the website experience, to enforce the terms of use, or as required by law.

We also reserve the right to disclose your Personal Information if we are required to do so by law, or in the good faith belief that disclosure of the information is reasonably necessary to comply with legal process, and to the extent permitted by local law, to respond to claims, or to protect or advance the rights, property, safety, or well-being of our company, our employees, customers, or the public.

We will not use your Personal Information for automated-decision making.

In the unlikely event that all or substantially all of the assets of EBSCO Information Services or any of its applicable subsidiaries are acquired, customer information, which may include Personal Information, may be one of the transferred assets unless restricted by applicable local law, in which case the acquiring entity will be subject to the same commitments for such customer information.

D. What is Our Legal Basis for Collecting and Using Personal Information?

Our legal basis for collecting and using the Personal Information described above will depend on the Personal Information concerned and the specific context in which we collect it.

However, we will normally collect Personal Information from you only:

- where we need the Personal Information to perform a contract with you or your organization;
- where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms; or
- where we have your consent to do so.

In some cases, we may also have a legal obligation to collect Personal Information from you or may otherwise need the Personal Information to protect your vital interests or those of another person.

If we ask you to provide Personal Information to comply with a legal requirement or to perform a contract, we will make this clear at the relevant time and advise you whether the provision of your Personal Information is mandatory or not (as well as of the possible impact if you do not provide your Personal Information).

Similarly, if we collect and use your Personal Information in reliance on our legitimate interests (or those of any third party), we will make clear to you at the relevant time what those legitimate interests are.

If you have questions about or need further information concerning the legal basis on which we collect and use your Personal Information, please contact us using the contact information provided below.

E. How Do We Secure Personal Information?

EBSCO Information Services has taken appropriate technical and organizational measures to ensure that Personal Information we have collected or will collect in the future is secure. For example, we have limited the number of people who have access to Personal Information, by electronic security systems and authentication methods that guard against unauthorized access.

As a reminder, EBSCO Information Services provides links to third-party websites. These websites may not have the same privacy policies as EBSCO Information Services. We take reasonable care in recommending these websites, but we are not responsible for their content or privacy policies. We urge users to read the privacy statement of a third-party website when leaving our Websites and linking to a third-party website.

We always use industry-standard technologies when transferring and receiving consumer data we receive. We have appropriate security measures in place in our physical facilities to protect against the loss, misuse, or alteration of information that we have collected from you in connection with our Websites.

F. What Are My Rights?

Depending on your country or state of residency, you may have legal rights with respect to your Personal Information, including one or more of the following (each of which may be subject to certain exceptions that will be analyzed on a case-by-case basis):

Right to be Informed	An organization must provide certain information to individuals when collecting and processing their Personal Information.
Right of Access / Right to Know	Individuals have a right to obtain confirmation as to whether or not their Personal Information is being collected and/or processed. Individuals also have a right to request that an organization disclose the Personal Information it collects, uses, discloses, sells, and/or otherwise processes.
Right to Rectification	Individuals have the right to require an organization to correct inaccurate Personal Information concerning the individual and to have incomplete Personal Information completed, including by means of providing a supplementary statement.
Right to Restrict Processing	Individuals have the right to require an organization to restrict the processing of their Personal Information.
Right of Data Portability	Individuals have a right to receive a copy of their Personal Information in a portable and readily usable (structured, commonly used, and machine-readable) format that can be transmitted to certain third parties without hindrance.
Right to Object or Opt-out	Individuals can request an organization to stop processing and/or selling (if applicable) their Personal Information.
Right to Withdraw Consent	Individuals have the right to withdraw their consent to the processing of their Personal Information at any time when the processing is based on the individual's consent. Withdrawal of consent does not affect processing that occurred prior to such withdrawal (it only has future effect).
Right to Erasure or Deletion	Individuals can request the deletion of their Personal Information collected or maintained by an organization.
Right to Non-discrimination	An organization cannot discriminate against an Individual because of the exercise of their legal rights with respect to their Personal Information.
Right to not be Subject to Automated Decision Making	Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, if such processing has a legal effect or otherwise significantly affects the individual.
Right to Lodge a Complaint	If you are located in the European Union (EU) or European Economic Area (EEA), you have the right to lodge a complaint with a supervisory authority in relation to the processing of your Personal Information.

Additional Information Regarding the Right to Know and the Right to Opt-out

EBSCO Information Services does not and will not sell Personal Information to third parties for a business or commercial purpose and has not sold Personal Information to third parties for a business or commercial purpose during the preceding 12 months or at any other time. Likewise, we do not and will not sell Personal Information

of minors under 16 years of age without affirmative authorization and have not sold Personal Information of minors under 16 years of age during the preceding 12 months or at any other time.

We disclose, and have disclosed during the preceding 12-month period, the following categories of personal information to third parties for a business or commercial purpose:

Categories of Personal Information Disclosed**

- Personal Identifiers
- Other Personal Information Categories
- Internet or Other Electronic Network Activity Information
- Geolocation data

*** See Appendix for specific examples of the types of personal information included in each category.*

Additional Information Regarding the Right to Object

If we process your Personal Information based on our legitimate interests, you can object to this processing in certain circumstances. In such cases, we will cease processing your Personal Information unless we have compelling legitimate grounds to continue processing or where it is needed for compliance and/or legal reasons. Where we use your Personal Information for direct marketing purposes, you can always object or opt-out by using the unsubscribe link in such communications or by submitting a request using any of the methods provided below.

G. How Can I Exercise My Rights?

We want to assure you that you can exercise any legal rights that you have with respect to your Personal Information. Upon request, we will tell you whether or not we have collected or processed any of your Personal Information.

If you would like to manage, change, limit, or delete your Personal Information, you can do so through your account settings on our Websites (if applicable) or by submitting a request using any of the methods provided below.
To exercise any other legal rights with respect to your Personal Information, you may submit a request using any of the methods provided below.

We will respond to your request as soon as reasonably possible, but no later than the legally required timeframe.

To exercise your rights (or to ask us questions about this Privacy Policy or our privacy practices), you can submit a request using any of the methods below:

5. Via Web: Please click here: https://privacyportal-cdn.onetrust.com/dsarwebform/3dc851a7-8ce1-41dc-8d75-358b1fe8c84d/cd99c5d8-e12d-40bd-829b-e59b5ec502c9.html (This hyperlink will redirect to our privacy management platform provided by our vendor, OneTrust, Inc.)

6. Via Toll-Free Telephone: 1-833-705-0124

7. Via Mail: EBSCO Information Services 5724 Highway 280 E
Birmingham, AL 35242, USA

Attn: Data Privacy Officer, Legal Department

8. Via Email: privacy@ebsco.com

Verification of Requests

All requests submitted to us will be verified to ensure that the person making the request (the "Requstor") is the individual about whom we have collected Personal Information. The method we use to verify the Requestor's identity may vary based on the type of customer or user, the Websites used, and the type of Personal Information we have collected. In most cases, we will require the Requestor to provide the following information when submitting a request:

- Type of Customer or User
- First Name
- Last Name
- Email Address
- Country
- State
- Legal Relationship to the Subject of the Request

We will use this identifying information to communicate with the Requestor and receive confirmation that they submitted the request, and then match this identifying information with the Personal Information we already maintain. We may also use the contact information that we already maintain to communicate with the individual to confirm that they submitted the request. In rare cases, we may ask for additional information to verify the request, which may include a signed declaration under penalty of perjury that the Requestor is the individual whose Personal Information is the subject of the request.

If the Requestor submits a request to delete Personal Information, we will separately confirm that the individual wants their Personal Information deleted.

We may deny a request if we cannot verify the identity of the Requestor to a reasonable degree of certainty or a reasonably high degree of certainty (depending on the type of request, the sensitivity of the Personal Information, and the risk of harm to the individual posed by a unauthorized request) or, in the case of a request to delete Personal Information, we may deny a request if we are not able to separately confirm that the individual wants their Personal Information deleted..

Authorized Agent

If you use an authorized agent to submit a request, we will require that you:

- provide the authorized agent written permission to act as your authorized agent; and
- verify the authorized agent's identity directly with us.

The above authorized agent requirements do not apply if you have provided the authorized agent with legally binding power of attorney in accordance with applicable law.

We may deny a request from an agent that does not submit proof that they have been authorized by you to act on their behalf.

H. What Choices Do I Have?

We understand that you may not want to allow our disclosure of your Personal Information to our Service Providers, or to let us use that information for purposes that you believe may be incompatible with the purpose for which it originally was collected (as permitted by this Privacy Policy) or that you later may authorize. Therefore, you may contact us to inform us that you do not want to permit these uses of your Personal Information. To do so, please contact us using the contact information provided above.

It is important to us that the Personal Information we collect is appropriate and relevant to the purposes for which we intend to use it. We will use Personal Information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the person providing the information. EBSCO Information Services will take reasonable steps to ensure that Personal Information is relevant to its intended use, accurate, complete, and current.

You may sign-up to receive email newsletters or other marketing materials from us. If you would like to discontinue receiving this information, you may immediately update your email preferences free of cost by using the "Unsubscribe" link found in emails we send to you or through your account settings on our Websites or by submitting a request using any of the methods provided above.

I. Collection and Use of Information from Children: Information for Parents

Our Websites are not intended for children under 16 years of age. No one under 16 years of age may provide any Personal Information to or on the Websites. We do not knowingly collect Personal Information from children under 16 years of age. If you are under 16 years of age, do not use or provide any information on our Websites or on or through any of their features. If we learn we have collected or received Personal Information from a child under 16 years of age without verification of

parental consent, we will delete that information. If you believe we might have any information from or about a child under 16 years of age, please contact us using the contact information provided above.

To the extent we collect any information of minors under 16 years of age that is considered personal information under any applicable law, we do not and will not sell such information without affirmative authorization and have not sold such information during the preceding 12 months or at any other time.

If you are a parent and have questions about our practices, please feel free to contact us using the contact information provided above.

J. How Long Do We Retain This Information?

We retain Personal Information we collect from you where we have an ongoing legitimate business interest or other legal need to do so (for example, to provide you with a service you have requested or to comply with applicable legal, tax or accounting requirements).

When we have no further legitimate business interest or legal need to process your Personal Information, we will either delete or anonymize it or, if this is not possible (for example, because your Personal Information has

been stored in backup archives), then we will securely store your Personal Information and isolate it from any further processing until deletion is possible.

EU- U.S. Privacy Shield and Swiss-U.S. Privacy Shield

EBSCO Industries, Inc. and its subsidiaries EBSCO International, Inc., EBSCO Publishing, Inc. dba EBSCO Information Services, DynaMed, LLC, Plastic Research and Development Corporation dba PRADCO Outdoor Brands, Summit Treestands, LLC, Luxor Workspaces, LLC, and Yankee Book Peddler, Inc. dba GOBI Library Solutions from EBSCO (collectively, the "EBSCO Covered Entities") comply with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (collectively, "Privacy Shield") as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Information transferred from the European Union, the European Economic Area (EEA), or Switzerland to the United States in reliance on Privacy Shield. The EBSCO Covered Entities have certified to the Department of Commerce that they adhere to the Privacy Shield Principles with respect to such Personal Information. If there is any conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield Frameworks and to view our certification, visit the U.S. Department of Commerce's Privacy Shield List at https://www.privacyshield.gov/list.

This Privacy Policy describes the types of Personal Information we collect, the types of third parties to which we disclose this information, and the purposes for which we do so. Residents of the EU, EEA, and Switzerland have the right to access the Personal Information that the EBSCO Covered Entities maintain, and in some cases, may have the right to correct or amend Personal Information that is inaccurate or has been processed in violation of the Privacy Shield Principles, to the extent allowed by law. To exercise this right, contact us at privacy@ebsco.com.

The EBSCO Covered Entities remain liable if they transfer Personal Information to third parties who process this Personal Information in a manner inconsistent with the Privacy Shield Principles.

With respect to Personal Information received or transferred pursuant to the Privacy Shield Frameworks, the EBSCO Covered Entities are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, the EBSCO Covered Entities may be required to disclose Personal Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the Privacy Shield Principles, the EBSCO Covered Entities commit to resolve complaints about their collection or use of your Personal Information. EU, EEA, and Swiss individuals with inquiries or complaints may contact the EBSCO Covered Entities by mail at 5724 Highway 280 E, Birmingham, AL 35242 USA, Attn: Data Privacy Officer or by email at privacy@ebsco.com. The EBSCO Covered Entities have further committed to refer unresolved Privacy Shield complaints to an alternative dispute resolution provider located in the U.S. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Under certain conditions, more fully described on the Privacy Shield website at https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

Questions

If you have any questions, comments, or concerns regarding this Privacy Policy or our practices, please contact us using the contact information provided above.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Changes to Privacy Policy

We will notify you of changes to this Privacy Policy by posting an updated policy on this page. You agree that any use of the Websites is based on this Privacy Policy, current at the time of use. If we make any material changes, we will notify you by means of a notice on our Websites (such as a banner or pop-up) prior to the changes becoming effective and provide you with the ability to consent to these changes (such as an "I agree" or "OK" button, or a prominent statement indicating the changes are in effect and continued use of the Websites signifies consent). We encourage you to periodically review this page for the latest information on our privacy practices.

Miscellaneous

This Privacy Policy does not apply to information collected by LearningExpress, LLC. To learn more about the information practices of LearningExpress, LLC, please visit its website, www.learningexpresshub.com.

Alternative Format / Accessibility: To access this Privacy Policy in an alternative format, click here to download a PDF version. If you have accessibility questions, please contact accessibility@ebsco.com.

Do Not Track Signals: EBSCO Information Services does not recognize automated browser signals regarding tracking mechanisms, which may include 'do not track' instructions.

Data Protection Representatives

Data Protection Representative	Country of Business Registration
EBSCO International, Inc.	United Kingdom and Sweden
EBSCO Information Services SAS	France
EBSCO GmbH	Austria
EBSCO Information Services GmbH	Germany
EBSCO Information Services B.V.	Netherlands
EBSCO Information Services S.r.l.	Italy
EBSCO Subscription Services Espana S.L.U.	Spain
EBSCO Information Services s.r.o.	Czech Republic
EBSCO Sp. z.o.o	Poland

APPENDIX

Examples of Types of Personal Information Included in Each Category

Category of Personal Information Collected	Examples
Personal Identifiers	Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, login credentials, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
Other Personal Information Categories	Personal information categories described in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)), which in addition to the identifiers described above, also lists a person's signature; physical characteristics or description; state identification card number; insurance policy number; education; professional affiliations; employment or employment history; bank account number, credit card number, debit card number, or any other financial information; and medical information or health insurance information.
Commercial Information	Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies, such as content checkout and retrieval information and saved searches.
Internet or Other Electronic Network Activity Information	Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
Geolocation Data	Location information obtained from a user's device. Inferred location information based on IP address.
Education Information	Education information, defined as nonpublic personally identifiable information under the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g and 34 C.F.R. Part 99).

EBSCO Information Services

Information Security Practices

White Paper

Introduction

Information Security (IS) is a priority at EBSCO Information Services (EBSCO). Our mission is to incorporate security and risk management practices into our policies, procedures, and day-to-day operations within the organization. This approach enables appropriate diligence to ensure adequate protection of information assets and systems.

EBSCO's IS practices and strategies provide controls at multiple levels of the data lifecycle, from receipt to access, transfer, and destruction.

EBSCO is an international corporation producing products and services for customers across multiple markets. Our approach and tools will accommodate variances in requirements based on market or locale. We are committed to the confidentiality, integrity and availability of our information assets.

Information Security Policies & Management

EBSCO's Information Security Policy stands as the core of our IS program. Policies address security-related topics across the information asset lifecycle: from general policy roles – outsourcing security controls, change management, data classification, data retention and disposal, paper and electronic media, and system configuration requirements – to more specialized policies addressing anti-virus, encryption, backup, logging, and physical security controls. Our policies are developed in conjunction with the EBSCO Chief Information Officer (CIO) as well as the Legal, EBSCO Information Security and Business Continuity Management teams. The EBSCO IS office is responsible for maintaining all of EBSCO's information security policies, facilitating the development of processes for secure application development and security assessments, and auditing current practices to ensure compliance with policy.

EBSCO's Information Security team
The EBSCO IS team holds specific certifications (ISC2, SANS/GIAC) specializing in Information Systems, Intrusion Analysis / Prevention, Incident Handling, Computer Forensics, in addition to having years of experience working with industry security best practices.

IS is responsible for developing a strategy and approach to achieve objectives consistent with EBSCO's desired information security posture. EIS InfoSec is also responsible for developing, facilitating and/or overseeing the information policies, standards, guidelines, strategies and procedures; for conducting risk assessments; for managing incidents, and for providing internal / external reporting.

Lastly, IS constantly evaluates the effectiveness of ongoing security operational processes and monitors compliance for internal and external requirements. As such, a core component of our approach to protecting our information assets is continuous training and awareness of information security policies and procedures across all levels of personnel at EBSCO. As examples, EBSCO continues to mature its practices in the following areas:

- On-boarding education of EBSCO's information security policies and practices
- IS training and awareness based on roles and responsibilities, on handing and securing information assets
- Targeted information security discussion and presentations on security-related topics
- IS team access and membership to information security communities and organizations such as SANS, IAPP, BCI, DRI, etc.
- IS communications to EBSCO's employee population regarding latest threats, practices, guidelines, etc.

Information Asset Protection

EBSCO security policies provide a series of threat prevention and infrastructure management procedures, including the following:

Incident Management
EBSCO has an incident management approach that ensures security issues are handled accordingly. This involves ensuring incident response procedures are followed in order to contain or eradicate any threats or issues, taking due diligence in investigating and reporting the incident, taking appropriate steps to recover from the incident, and, if necessary, taking appropriate steps to escalate issues to senior management, law enforcement, or other key stakeholders. Events that directly impact customers are highest priority.

Post-event assessments are conducted to determine the root cause for events, regardless of threat, to understand if the causes are one-time, or trends, to adjust response or prevent recurrence.

Incident management procedures are exercised based on threat scenarios (e.g., insider threats, phishing, social engineering, software vulnerabilities) as needed to ensure that processes are efficient and stakeholders understand protocol.

Monitoring
EBSCO employs monitoring across its environments with multiple tools (a combination of open source and commercial tools) to identify, track, monitor, and report on pertinent risks, vulnerabilities (e.g., host availability, application response time, security events, etc.) Monitoring tools are set up to provide alarms and notices to EBSCO staff, who review and assess system logs to identify malicious activity.

Ongoing analysis across environments helps identify potential threats for escalation to EBSCO IS staff.

Vulnerability Management
The EBSCO IS team scans for security threats using commercial, automated and manual methods. The team is also responsible for tracking and following up on any potential vulnerabilities that might be detected. The team has the capability to scan environments (both internal and external) and is updated on new systems within our environment.

Once EBSCO's Technology and IS teams have identified a vulnerability, it is prioritized according to severity and impact and remediated accordingly. The EBSCO IS team tracks risk and vulnerabilities until remediation.

Malware Prevention, Detection & Remediation
EBSCO uses multiple tools to address malware and phishing risks (e.g., firewalls, anti-virus, backups, automated and manual scanning, end-user awareness). EBSCO's IS team periodically evaluates new technologies to mitigate malware and Advance Persistent Threats (APTs) to stay as protected as possible from these risks.

Network Security
EBSCO employs multiple layers of defense to secure information under our control, including protecting the network perimeter from external attacks – allowing only authorized services and protocols to access EBSCO's systems and services.

EBSCO's network security strategies, among other capabilities, include network segregation (e.g., production vs. testing, DMZ, service delivery vs. corporate).

Application Security
EBSCO employs Next Generation and Application Firewall technologies to mitigate the latest threat and attack vectors such as:

- Zero Day exploits
- Web application attacks (OWASP Top10)
- "Brute Force" and "Low and Slow" attacks
- Content scraping/harvesting
- Phishing/Spear Phishing
- Botnet/SpamBot activity
- Known malicious sources/actors

EBSCO leverages these technologies coupled with commercial threat intelligence feeds to create a comprehensive solution to detect and mitigate targeted application attacks before they have a chance for success.

Logical System Access
EBSCO has controls and practices to protect the security of customer information and employees. EBSCO maintains detailed logical access control security. Group access is used to grant employees access based upon their assigned function and job responsibility.

Each system user is assigned a unique user ID and password, and users are required to enter their current password prior to creating a new password.

Media Disposal
EBSCO utilizes a combination of internal processes and third-party vendors for media disposal. Destruction is based on the information asset classification and retention requirements. Certificates of destruction are collected, as required, from external third parties.

Logging Controls
EBSCO's policies provide that all event logs must be collected and protected from unauthorized access. The viewing of logs occurs only as required. The logs are further protected by a file integrity monitoring system that alerts the IS department of unauthorized access and modification.

Personnel Controls
EBSCO employees are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

EBSCO will verify an individual's education and previous employment, and perform internal and external reference checks. Where local laws or statutory regulations permit, EBSCO may also conduct criminal, credit, immigration, and security checks. The extent of background checks is dependent on the desired position.

Upon acceptance of employment at EBSCO, all employees are required to execute a confidentiality agreement that documents the receipt of, and compliance with, EBSCO policies.

At EBSCO, all employees are responsible for information security. As part of this responsibility, they are tasked with communicating security and privacy issues to designated management in Technology, IS, and/or the CIO.

Physical and Environmental Security

EBSCO has policies, procedures, and infrastructure to handle both the physical security of its data centers as well as the environment in which the data centers operate. These include:

Physical Security Controls
EBSCO's data centers employ a variety of physical security measures. The technology and security mechanisms used in these facilities may vary depending on local conditions such as building location and regional risks. The standard physical security controls implemented at EBSCO data centers includes the following:

- electronic card access control systems
- intrusion detectors and alarms
- computer inventory control
- interior and exterior cameras
- 24/7 security guard access

Access to areas where systems, or system components, are installed or stored is segregated from general office and public areas such as lobbies. The cameras and alarms for each of these areas are centrally monitored. Activity records and camera footage are kept for later review, as needed.

Access to all data center facilities is restricted to authorized EBSCO employees, approved visitors, and approved third parties whose job it is to operate the data center. EBSCO maintains a visitor access policy and procedures on approvals for visitors, third parties, and employees who do not normally have access to data center facilities. EBSCO audits who has access to its data centers on a regular basis.

EBSCO restricts access to its data centers based on role.

Environmental Controls

- **Power and Utilities –** EBSCO data centers have redundant electrical power which includes backup generators as well as multiple utility providers, services, and systems. Alternate power supplies provide power until diesel engine backup generators engage and are capable of providing emergency electrical power, at full capacity, as needed, and the redundancy of our multiple oil providers, geographically diverse, allows for continuous operation, if needed.

- **Climate Control –** EBSCO maintains redundant cooling systems to control our data center environments.

- **Fire detection, protection and suppression –** EBSCO fire protection systems include fire alarms, automatic fire detection, and fire suppression systems. Should a fire arise in our data centers, visible and audible alerts are activated and proper response is initiated, which include automated response as well as the use of physical fire extinguishers located throughout our data centers.

Scott Macdonald,
VP of Information Security and Operations