

**McGraw-Hill Education Subscription Agreement Registration Page – CT Version**

The Subscription Agreement (the "Agreement") by and between McGraw-Hill School Education , LLC ("MHE") and the educational institution set forth below ("Subscriber," "Customer" or "School") consists of the following: (i) this Registration Page, (ii) the Terms of Service available on the MHE website and attached hereto as Exhibit A (the "Terms of Service"), (iii) any purchase order(s), and (iv) any written addenda or amendments to any of the foregoing that are agreed to by both parties. In the event of a conflict between the terms of this Registration Page and the Terms of Service, the terms of this Registration Page will control. The Agreement shall be effective as of the date on which MHE has signed below (the "Effective Date").

1. **NAMES & ADDRESSES OF THE PARTIES:** McGraw-Hill School Education, LLC, a limited liability company with an address at 8787 Orion Place, Columbus Ohio 43240 ("MHE"), and *Berlin Public Schools*, a 238 Kensington Rd, Berlin, CT 06037 ("Subscriber," "Customer" or "School").
2. **RELATIONSHIP OF THE PARTIES.** Subscriber's End Users (as defined in the Terms of Service) will use certain online educational products and services (the "Services") and related content provided by MHE in connection with courses offered by Subscriber. Subscriber and/or its End Users may provide personally identifiable information of the End Users to MHE in connection with accessing and using the Services. End Users that are instructors or administrators are required to agree to MHE's Terms of Use and the Privacy Notice (each available on the MHE website and attached hereto as Exhibit B and Exhibit C, respectively) before accessing the Services.
3. **DATA PRIVACY AND SECURITY.** MHE maintains reasonable procedures in accordance with its policies and practices and applicable law to protect the confidentiality, security, and integrity of personally identifiable information received by MHE in connection with provision of the Services to the End Users. The MHE Data Privacy and Security Guidelines (available on the MHE website and attached hereto as Exhibit D).
4. **TERM.** This Agreement shall remain in effect as long as MHE provides Services to Subscriber. In no event shall MHE be obligated to provide any Services beyond any Subscription Term end date(s) set forth in the applicable purchase order or controlling purchasing document without the prior written consent of MHE and Subscriber.
5. **SUBSCRIBED MATERIALS.** By placing an order for the digital products set forth below (the "Subscribed Materials"), Subscriber agrees to be bound by the Terms of Service. Subject to Subscriber's payment of the fees set out below, MHE hereby grants to Subscriber a non-exclusive, non-transferable license to allow only the number of End Users that corresponds to the quantity of Subscribed Materials set forth below to access and use the Subscribed Materials under the terms described in the Terms of Service. The subscription term for the Subscribed Materials shall be as set forth in the Product Description below. If no subscription term is specified, the initial term shall be one (1) year from the Effective Date (the "Initial Subscription Term"), and thereafter shall renew for additional one (1) year terms (each a "Subscription Renewal Term" and together with the Initial Subscription Term, the "Subscription Term"), provided MHE has chosen to renew the subscription and has sent an invoice for such Subscription Renewal Term to Subscriber, and Subscriber has paid for such Subscription Renewal Term.
6. **PRODUCT PURCHASE.** Subscriber shall purchase the MHE products (the "Products") set forth below at the prices set forth below.

ISBN Number	Product Description	Price

{00040546 2 }

May 2018 - CT

---

**7. PROVISIONS REQUIRED BY CONNECTICUT GENERAL STATUTE §§ 10-234.**

7.1. All Subscriber Data (as defined in the Terms of Service) provided or accessed pursuant to this Agreement is not the property of, or under the control of, MHE.

7.2. Subscriber must have access to and the ability to delete any Subscriber Data in MHE's possession. Subscriber may request the deletion of Subscriber Data by submitting MHE's Personal Information Request Form: <https://www.mheducation.com/privacy/privacy-request-form>

7.3. MHE shall not use Subscriber Data for any purposes other than those authorized pursuant to this Agreement.

7.4. A student, parent or legal guardian of a student may review Personally Identifiable Information (as defined in the Terms of Service) concerning the student End User and correct any erroneous information, if any, in such Personally Identifiable Information, by Subscriber submitting MHE's Personal Information Request Form: <https://www.mheducation.com/privacy/privacy-request-form>.

7.5. MHE shall take actions designed to ensure the security and confidentiality of Subscriber Data.

7.6. The MHE Data Privacy and Security Guidelines (available on the MHE website and attached hereto as Exhibit D) contain a description of the procedures that MHE will follow to notify the local or regional board of education, in accordance with Conn. Gen. Stat. § 10-234dd, when there has been a Security Incident (as defined therein).

7.7. Personally Identifiable Information concerning End Users shall not be retained by, or available to, MHE after the earlier of (i) MHE's standard data retention period and (ii) Subscriber's written request to delete Personally Identifiable Information concerning End Users unless a student, parent or legal guardian of a student chooses to establish or maintain an electronic account with MHE for the purpose of storing student-generated content.

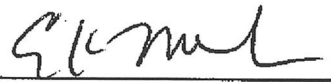
7.8. The parties shall each ensure their own compliance with the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, as amended from time to time.

7.9. The laws of the State of Connecticut shall govern the rights and duties of the parties.

7.10. If any provision of this Agreement or the application of this Agreement is held invalid by a court of competent jurisdiction, the invalidity does not affect other provisions or applications of this Agreement which can be given effect without the invalid provision or application.

**IN WITNESS WHEREOF**, the parties hereto intending to be legally bound have caused this Agreement to be executed by their duly authorized representatives.

**Subscriber**

By: 

Print Name: D. Erin McGurk

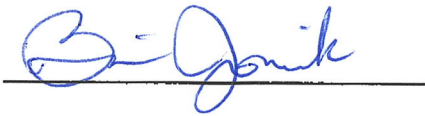
Title: Asst. Superintendent

Address: 238 Kensington Rd.  
Berlin, CT 06037

Email: emcgurk@berlinschools.org

Date: 12/3/18

**McGraw-Hill School Education, LLC**



Brian Joniak

Sr. Director Finance/Controller

8787 Orion Place  
Columbus, OH 43240

brian.joniak@mheducation.com

Date: \_\_\_\_\_

## Exhibit C

### McGraw-Hill Education Student Data Privacy Notice

Effective Date: May 22, 2018

#### Introduction

As a global leader in providing digital learning systems for educators and students, McGraw-Hill Education ("MHE") is deeply committed to protecting the privacy of our end users. Whether you are using Connect, ConnectEd, Engrade or any of our other solutions, we collect Personally Identifiable Information that we use to provide, maintain and improve the solution. We are providing the below information so that you can understand how we protect and use your information. If you are under 18, we suggest that you review this information with your parents.

This information applies to all end users of our digital learning system. Since McGraw-Hill Education is a service provider to your institution, your institution Educational institutions are best able to provide you with a full understanding of their privacy practices and more information on how their end user's Personally Identifiable Information (PII) is collected, shared, and used. To obtain more detailed information about how PII is collected, used, and shared by your educational institution, please contact the appropriate individual at that institution.

In limited circumstances, end users may also be customers of MHE and MHE may market to them as a customer. For example, end users may purchase products or create personal accounts in our web sites. In these circumstances, they would be treated as a customer. For more information on how your data is used as a customer, please review the Customer Data Privacy Notice. By contrast, this End User Data Privacy Notice applies to end users with respect to the information collected and processed as part of a course of instruction within the digital learning solution as determined by their educational institution or employer. Aggregated de-identified end user PII is leveraged by MHE to improve existing or develop new educational products and services.

MHE is a global organization. We follow privacy laws and regulations that are applicable to our company and our services in the areas where we do business. Should our privacy practices change, we will update it here, but more importantly, we will notify your educational institution in writing and obtain their consent before implementing any material impact to your privacy rights.

#### Questions? Contact us:

Any questions or complaints regarding this notice or the collection, use, disclosure, or transfer of PII collected by your educational institution through our digital learning systems should be directed to the appropriate representative at your educational institution.

Otherwise, if you have purchased or received an MHE product outside of an educational institution, please direct any questions or complaints to the MHE Data Protection Officer by emailing [privacy@mheducation.com](mailto:privacy@mheducation.com) or calling +1-646-766-3199. If applicable, you may choose to lodge a complaint with your national data protection authority at any time. For local privacy contact information, please see [McGraw-Hill Education's Local Privacy Official](#).

#### *What is personally identifiable information (PII)?*

Personally identifiable information, or PII, is any information relating to an identified or identifiable natural person ("data subject") including personal data as defined under applicable local law. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

***What PII do we collect?***

***We collect PII, such as contact information and education details, in order to provide you with the product and/or service requested.***

We only collect the information required to provide, maintain and improve the digital learning solution you use. When you register, or are registered within one of our digital learning solutions, we collect your name, school, instructor, class, and login information. Once you begin using one of our solutions, we collect your input to questions, technical specifications, and other information about how you use the solution. You are not required to provide PII; however, in order to use certain services, we may need to collect certain PII for that service to function properly or for us to provide you with requested information.

Depending on the product, the PII we collect includes information from the following categories:

1. Name, initials, and personal or business-related contact information
  - a. For our digital learning systems, we collect your name/initials and contact information when you create an account. However, we collect additional PII, or confirm existing PII, if you contact customer service with an issue or question.
2. Education & professional information
  - a. For some digital learning systems, we collect PII related to your position as an educator or student. This includes the state, district, name of school, courses, etc.
3. In some instances, we collect PII from third parties who provide single-sign-on functions via Learning Management Systems or related tools.

***We automatically collect computer metadata and content to provide, improve, and maintain our products and services.***

When you use our digital learning systems, we automatically collect certain information from you through the use of cookies, web beacons or other tracking mechanisms. This includes information about your experience such as your IP address, operating systems, pages viewed, and time spent.

Third parties also collect information automatically from you across websites and over time through the use of their own cookies, web beacons, and tracking mechanisms. This information is used to enable the functions of the digital learning system, as well as customize, maintain, and improve our digital learning systems. You may disable cookies via your browser or third party mechanisms. However, some features of our digital learning systems may not function properly without them. Third party cookies that we use include Google Analytics and Webtrends.

If you choose to communicate with or receive communications through our services via phone, text, chat, email, or any other platform for technical support, customer service, or other assistance, those interactions may be recorded and monitored to deliver the solution or information requested by you.

***How do we use PII and on what legal basis?***

As mentioned above, we use your information to provide you with the digital learning solution on behalf of your school, in order to meet our contractual obligation to you or your school with respect to the service. For

example, to assist with identifying users across products and providing consistent service and to enable sharing of data between our products and your school's learning management system.

We will also process your PII to meet our legitimate interests, for example to improve the quality of services and products.

Except as described in this notice, we limit the use, collection, and disclosure of your PII to the minimum level necessary to deliver the service or information requested by you or your institution. We do not collect, use, or disclose PII that is not reasonably related to a legitimate business purpose necessary to serve you. Your information may also be used in order to maintain and/or improve our services.

Some of our digital learning solutions will use your previous responses to customize your learning experience. This customization is designed to ensure the best possible learning environment for a student without directly driving any determinative outcome.

Provision of your PII may be necessary in order to use the chosen digital learning solution. Failure to provide us with your PII may preclude you from using the digital learning solution.

#### ***Do we sell or use your PII to market to you?***

**We will not sell end user PII or use information from educational records for marketing purposes.**

We will not sell PII to other organizations, nor will we market to students using the information from their educational records (education records are defined as records directly related to a student and maintained by an educational agency or institution, or by a party acting for the agency or institution).

#### ***When do we share your PII with third parties?***

***In general, we only share your PII in order to provide, maintain, or improve our products or services, or respond to legal requests.***

1. **Co-branded/Other Web Sites and Features** – We may share your PII with third-party business partners for the purpose of providing the service to you. These third-party business partners include cloud service providers, learning management systems (LMS), other educational software providers, etc. These business partners will be given limited access to the PII that is reasonably necessary to deliver the service, and we will require that such third parties follow the same privacy and security practices as MHE.
2. **Business Transfer** – In the event of a sale, merger or acquisition, we will be able to transfer your PII to a separate entity. We will use commercially reasonable efforts to require this entity to use your PII only for authorized purposes and by authorized persons in a manner consistent with the choices end users have made under this notice, and that security, integrity, and privacy of your PII is maintained.
3. **Agents/Service providers** – We hire other companies to perform certain business-related functions on our behalf and according to our instructions. For example, we provide your PII to service providers that host our platform data in the cloud (e.g., AWS).
4. **Affiliates** – McGraw-Hill Education is a global corporation that consists of multiple organizations. We share your PII between organizations within McGraw-Hill Education to provide, maintain, and improve our products and services. A list of the companies within the MHE group is available [here](#).
5. **Educational Institutions** – As we provide products and services to your school, we share your data with approved individuals at your school, such as administrators or educators.
6. **Law Enforcement** – In the event that McGraw-Hill Education receives a legal demand for end user data from a law enforcement agency, that request will only be honored if:

- a. The request complies with all laws and clearly establishes the legal need for disclosure.
- b. The request is related to a specific investigation and specific user accounts are implicated in that investigation.
- c. Whenever legally permissible, users shall receive notice that their information is being requested.

MHE reserves the right to disclose to third parties non-personally identifiable information about our users and their use of the MHE services. For example, MHE may disclose aggregate data about the overall patterns or demographics of the users of the MHE products or services.

***What rights do you have?***

***As a user, you have the rights to access, export, be informed about, rectify, object to the further processing of, restrict the processing of, withdraw consent to the processing of, and erase your PII.***

***If you are a student at an educational institution using an MHE product, you should direct any requests to exercise your data subject rights to the appropriate representative at your institution. If you are an educator or administrator you may reach out to MHE directly on the requests below:***

1. Access and rectification – We strive to ensure that the PII we have about you is accurate and current. You may obtain confirmation as to whether or not PII concerning you exists, regardless of whether PII has already been recorded, and be communicated such information in a readily understandable form.
2. Choice & Objection to processing – With limited exceptions, you may choose to change how we use your PII at any time. However, if the PII is required in order to provide you with the service or process a transaction, you may not be able to opt-out without canceling the transaction or service. You may object, in whole or in part, on legitimate grounds, to the processing of your PII, even where such processing is relevant to the purpose of the collection. Please know that if we do receive a request to objection to the further processing of your information, you may no longer be able to access or use the digital learning solution.
3. Withdraw consent – Your educational institution is responsible for obtaining your consent, where required. MHE obtains consent from your institution to collect, process, and store your PII.
4. Restriction of processing: In specific cases (e.g., if you challenge the accuracy of the PII, while this is being checked), you can request a restriction on the processing of your PII, which can only be processed to file or defend claims.
5. Information – You have the right to be informed a) of the source of the PII; b) of the purposes and methods of the processing; c) of the logic applied to the processing, if processing is carried out with the help of electronic means; d) of the identity of the data controller and data processors; and e) of the entities or categories of entities to whom the PII may be communicated and who may have access to such PII in their capacity as data processor(s) or person(s) in charge of the processing.
6. Data portability – You have the right to export your PII from our systems in a readily accessible file type.
7. Erasure – You may request erasure, anonymization or blocking of a) PII that have been processed unlawfully; b) PII whose retention is unnecessary for the purposes for which it has been collected or subsequently processed. You can obtain certification to the effect that such operations, as well as their contents, have been notified to the entities to whom the data were communicated, unless this requirement proves impossible or involves a manifestly disproportionate effort. Since your educational institution has hired us to manage this information for them, we ask that you or your parent make any request to delete your information directly to your school. Please know that if we

do receive a request to delete your information, you may no longer be able to access or use the digital learning solution.

***How do we protect your PII?***

***Our IT security team has established industry standard security measures to protect your PII from unauthorized access and use.***

MHE takes reasonable precautions to protect your information. When you submit PII via the digital learning system, your information is protected both online and off-line. MHE utilizes reasonable security measures to protect the security and confidentiality of your PII from unauthorized access and use.

***How long do we retain your data?***

We will retain your data for the minimum amount of time necessary to accomplish the purpose for which it was collected, and thereafter no longer than is permitted under MHE's data retention policies. We will retain and use your data as necessary to comply with our obligations, resolve disputes and enforce agreements.

For information on the retention period that applies, reach out to the Privacy Office by emailing [privacy@mheducation.com](mailto:privacy@mheducation.com) or calling +1-646-766-3199.

***When do we store, transfer or process PII internationally?***

***McGraw-Hill Education is a global organization. Depending on your location, and the product or service, your information may be stored and processed within secure data centers at one or many of our locations. MHE has committed to meeting the requirements of local data protection laws, including EU law, to the extent required. If your data is stored locally, then your local laws prevail.***

We recognize and acknowledge current data protection laws in the European Union, Switzerland, and around the world. To comply with privacy laws in the European Union, we have implemented appropriate contracts for the international transfer of PII, on the basis of the standard contractual clauses approved by the European Commission and other international models as required by local law, to provide a legal mechanism for transferring data to MHE locations globally. For more information on the aforementioned model contracts and how to obtain a copy of the contract, please contact the Privacy Office at [privacy@mheducation.com](mailto:privacy@mheducation.com) or +1-646-766-3199.



## Exhibit D

### Data Privacy and Security Guidelines

This Data Privacy and Security Guidelines (“DPSG” or “Security Guidelines”) document sets forth the duties and obligations of MHE (defined below) with respect to Personally Identifiable Information (defined below). In the event of any inconsistencies between the DPSG and the Agreement (defined below), the parties agree that the DPSG will supersede and prevail. Capitalized terms not defined herein shall have the meaning ascribed to them in the Agreement.

#### 1. Definitions.

- a. **"Agreement"** means the Agreement between the McGraw-Hill Education entity (“MHE”) and Subscriber to which these Security Guidelines are referenced and made a part thereof
- b. **"Applicable Laws"** means federal, state and international privacy, data protection and information security-related laws, rules and regulations applicable to the Services and to Personally Identifiable Information
- c. **"End User Data"** means the data provided to or collected by MHE in connection with MHE’s obligations to provide the Services under the Agreement
- d. **"Personally Identifiable Information" or "PII"** means information provided to MHE in connection with MHE’s obligations to provide the Services under the Agreement that (i) could reasonably identify the individual to whom such information pertains, such as name, address and/or telephone number or (ii) can be used to authenticate that individual, such as passwords, unique identification numbers or answers to security questions or (iii) is protected under Applicable Laws. For the avoidance of doubt, PII does not include aggregate, anonymized data derived from an identified or identifiable individual
- e. **"Processing of PII"** means any operation or set of operations which is performed upon PII, such as collection, recording, organization, storage, use, retrieval, transmission, erasure or destruction
- f. **"Third Party"** means any entity (including, without limitation, any affiliate, subsidiary and parent of MHE) that is acting on behalf of, and is authorized by, MHE to receive and use PII in connection with MHE’s obligations to provide the Services
- g. **"Security Incident"** means the unlawful access to, acquisition of, disclosure of, loss, or use of PII
- h. **"Services"** means any services and/or products provided by MHE in accordance with the Agreement

#### 2. Confidentiality and Non-Use; Consents.

- a. MHE agrees that the PII is the Confidential Information of Subscriber and, unless authorized in writing by Subscriber or as otherwise specified in the Agreement or this DPSG, MHE shall not Process PII for any purpose other than as reasonably necessary to provide the Services, to exercise any rights granted to it under the Agreement, or as required by Applicable Laws.
- b. MHE shall maintain PII confidential, in accordance with the terms set forth in this Security Guidelines and Applicable Laws. MHE shall require all of its employees authorized by MHE to access PII and all Third Parties to comply with (i) limitations consistent with the foregoing, and (ii) all Applicable Laws.
- c. Subscriber represents and warrants that in connection with any PII provided directly by Subscriber to MHE, Subscriber shall be solely responsible for (i) notifying End Users that MHE will Process their PII in order to provide the Services and (ii) obtaining all consents and/or approvals required by Applicable Laws.

3. Data Security.

MHE shall use commercially reasonable administrative, technical and physical safeguards designed to protect the security, integrity, and confidentiality of PII. MHE's security measures include the following:

- a. Access to PII is restricted solely to MHE's staff who need such access to carry out the responsibilities of MHE under the Agreement
- b. Access to computer applications and PII are managed through appropriate user ID/password procedures
- c. Access to PII is restricted solely to Subscriber personnel based on the user role they are assigned in the system (provided, however, that it is the Subscriber's responsibility to ensure that user roles match the level of access allowed for personnel and that their personnel comply with Applicable Law in connection with use of such PII)
- d. Data is encrypted in transmission (including via web interface) at no less than 128-bit level encryption
- e. MHE or an MHE authorized party performs a security scan of the application, computer systems and network housing PII using a commercially available security scanning system on a periodic basis

4. Data Security Breach.

- a. In the event of a Security Incident, MHE shall (i) investigate the Security Incident, identify the Impact of the Security Incident and take commercially reasonable actions to mitigate the effects of any such Security Incident, (ii) timely provide any notifications to Subscriber or Individuals affected by the Security Incident that MHE is required by law, subject to applicable confidentiality obligations and to the extent allowed and/or required by and not prohibited by Applicable Laws or law enforcement.
- b. Except to the extent prohibited by Applicable Laws or law enforcement, MHE shall, upon Subscriber's written request, provide Subscriber with a description of the Security Incident and the type of data that was the subject of the Security Incident.

5. Security Questionnaire.

Upon written request by Subscriber, which request shall be no more frequently than once per twelve (12) month period, MHE shall respond to security questionnaires provided by Subscriber, with regard to MHE's information security program applicable to the Services, provided that such information is available in the ordinary course of business for MHE and it is not subject to any restrictions pursuant to MHE's privacy or data protection or information security-related policies or standards. Disclosure of any such information shall not compromise MHE's confidentiality obligations and/or legal obligations or privileges. Additionally, in no event shall MHE be required to make any disclosures prohibited by Applicable Laws. All the information provided to Subscriber under this section shall be Confidential Information of MHE and shall be treated as such by the Subscriber.

6. Security Audit.

Upon written request by Subscriber, which request shall be no more frequently than once per twelve (12) month period, MHE's data security measures may be reviewed by Subscriber through an informal audit of policies and procedures or through an independent auditor's inspection of security methods used within MHE's infrastructure, storage, and other physical security, any such audit to be at Subscriber's sole expense and subject to a mutually agreeable confidentiality agreement and at mutually agreeable timing, or, alternatively, MHE may provide Subscriber with a copy of any third party audit that MHE may have commissioned.

7. Records Retention and Disposal.

- a. MHE will use commercially reasonable efforts to retain End User Data in accordance with MHE's End User Data retention policies.
- b. MHE will use commercially reasonable efforts to regularly back up the Subscriber and End User Data and retain any such backup copies for a minimum of 12 months.