Parent Data Privacy Notice

Effective Date: May 9, 2018

Introduction

Protecting privacy and maintaining the trust of our customers, students, and their parents has always been a key priority for us. To enhance learning, we need access to data, measurement, insight and other feedback that inform us about students' knowledge, skill levels and learning development.

Our goal is to use the data obtained in the course of current learning activities to provide adaptive pathways of learning; not to drive commerce.

We want to communicate with parents and schools about the educational benefit of using technology to create a personalized learning path based on past performance, and the need to use student information for educational purposes.

We want to build trust around the way we use personally identifiable student data for educational purposes.

Questions? Contact us:

Any questions or complaints regarding this notice or the collection, use, disclosure, or transfer of PII (as defined below) covered by this notice should be directed to the McGraw-Hill Education Data Protection Officer.

Please direct any questions or complaints to the Data Protection Officer by emailing 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 contact McGraw-Hill Education's Local Privacy Official.

Our commitment to privacy and innovation goes beyond compliance, it is part of our culture:

- We have implemented policies and procedures to support customers in their compliance with privacy laws, including: GDPR, COPPA, and FERPA.

- We've taken a leadership role with Future of Privacy Forum (FPF) and the Software and Information Industry Association (SIIA) in setting the agenda for self-regulatory goals for student privacy in the industry.

- We have an internal Privacy Council comprised of senior leaders throughout our company that provides the tone at the top to perpetuate best practices across our business.

- We do not support business models that create tolls and taxes on interoperability.

- We conduct regular scans of our applications to prevent and detect security breaches. We recognize that no system is 100% secure, but we take steps to prevent and mitigate the impact of adverse events.

By increasing awareness and transparency, we hope to better understand the concerns and learn how to talk with each other about privacy, security, and confidentiality.

Educational institutions, as data controllers, are ultimately responsible for providing a full understanding of the privacy practices around how their students' personally identifiable information is collected, shared, and used. To obtain more detailed information about how data is collected, used, and shared by an educational institution, please contact the appropriate representative at that institution.

For further details on our privacy practices around student data, please review the Student Data Privacy Notice. The Student Data Privacy Notice details practices around how we collect and use student information, whether they are a student at an educational institution or an individual using a product on their own

If you have purchased an MHE product for your child please also review the Customer Data Privacy Notice for information on how we handle your personally identifiable information.

If you have purchased an MHE product and created an account for yourself as an educator, please also review the Educator Data Privacy Notice. The Educator Data Privacy Notice also applies to educators at educational institutions.

If you choose to communicate with or receive communications from MHE 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 information requested by you.