EMATH INSTRUCTION DATA SECURITY AND PRIVACY COMPLIANCE MEASURES

For School Districts Requesting Information on Data Security and Privacy Compliance with 2-d and Section 121.3 (Version April 2020)

What data do we receive from schools and why?

1. We **DO NOT** ask for, collect, or receive any student data.
2. We **DO NOT** ask for, collect, or receive any principal data.
3. We **DO NOT** ask for, collect, or receive any educational data including grades, test scores, disciplinary information, or educational information.
4. We ask for, collect, and receive teacher name and email address **ONLY**. This is information is used for the purpose of maintaining user accounts. These user accounts provide user access to mathematics materials for educational purposes only.

How do we implement State and federal data security and privacy requirements throughout the life of the contract?

5. We make reasonable efforts to comply with NIST Cybersecurity Framework guidelines.

We use data encryption technology to secure the transfer of user data and we comply with PCI compliance requirements. We also limit access to any and all user data to only our team members to help fulfill orders, process refunds and support you. We will not sell or share your personal data with any third parties without your prior consent except where we are required to do so by law.

6. We limit access to PII so that no personnel (whether employee or independent contractor or vendor) has access to PII unless their essential job/contract function requires such access; and in such cases we limit their access to only that PII required for them to perform their essential job/contract function.
7. We do not collect student data, teacher data or principal data from school districts.
8. Our Privacy Policy, which is published and made prominent on our website, clearly communicates what data we collect, how that data is used, how a user may obtain a copy of the data collected about them, and how a user may challenge the accuracy of the data collected or received about them.

How do we implement data security and privacy requirements that are compliant with the district's data security and privacy policy throughout the life of the contract?

1. We use industry-recognized security safeguards to protect the personally identifiable information that you have provided to us from loss, misuse, or unauthorized alteration.
2. We securely transfer all data over encrypted connections and store all user data on our web servers only, for our users privacy. The only data shared with third- party services is general, anonymised data containing no personal identifying information. No personal data is sold or shared with any third parties without your prior consent except where we are required to do so by law.
3. We have a Personal Data Exporter and Removal policy in place and up to date to export/remove personal data associated with all users accounts to meet privacy compliance laws

We comply with Section 121.3(c) of the Commissioner's Regulations by:

1. Not receiving from the school district any student data, teacher data or principal data;
2. Limiting access to PII in compliance with the parents bill of rights for data privacy and security, as set forth in greater detail in other sections of this document;
3. Using data security technology and methods, such as encryption, HTTPS and regular plugin security updates, to ensure such data will be protected and data security and privacy risks mitigated, while in motion or at rest, as set forth in greater detail in other sections of this document;
4. Abiding by Emath's Internal Data Security and Privacy Compliance Policy, which is informed by NIST Cybersecurity Framework guidelines for small business.
5. Publishing in Emath's Privacy Policy how a parent, student, eligible student, teacher or principal may challenge the accuracy of any student data or teacher or principal data collected.

How will our employees and any assignees with access to student data, teacher data or principal data receive training on the relevant confidentiality laws before receiving access to such data?

1. We will ensure that no employee or assignee will receive access to PII unless such access is necessary for them to perform their job functions. AND
2. We will ensure that before any employees or assignees are granted access to PII or to any part of the system from which PII may be accessed, the employee or assignee must first read and agree to abide by Emath's Internal Data Security and Privacy Policy.

Emath from time to may from time to time use subcontractors, who may or may not have access to PII.

1. We will ensure that no subcontractor will receive access to PII unless such access is necessary for them to perform the contracted-for services. AND
2. We will ensure that before any subcontractors are granted access to PII or to any part of the system from which PII may be accessed, the subcontractor must first read and agree to abide by Emath's Internal Data Security and Privacy Policy.

Our action plan for handling any breach or unauthorized disclosure of PII is:

Upon learning of a data breach or unauthorized disclosure, we will promptly :

1. Notify our IT services provider and instruct them to immediately implement technical measures to limit the extent of the breach and secure all uncompromised data;
2. Notify all contracted school districts of the breach or unauthorized disclosure;
3. Notify the owners of the PII (which includes the parents of any minor students) of the breach or unauthorized disclosure;
4. Notify our attorney;
5. Begin an investigation to identify the source of the breach, in particular, whether it originated internally, and to remove system access from any employees, assignees or subcontractors suspected of causing or contributing to the breach or unauthorized disclosure.
6. Implement the continuation plan using backup systems and equipment as necessary while the main system is undergoing forensic investigation and cleaning.
7. Notify any insurers providing cybersecurity coverage to Emath Instruction and/or any contracted school districts.

When the school district contract ends or is terminated, Emath will, within 30 days after the effective termination date:

1. permanently delete from all local equipment and all servers, all data received from the school district over the course of the contract unless the school district, during that __ day period, delivers written instructions to Emath Instruction to return the data to the school district.
2. If Emath, during that 30 day period, receives from the school district written instructions to return the data to school district, Emath will do so by transmitting to the school district, in electronic form in one or more encrypted files, all data received from that school district over the course of the contract. After such transmission, Emath will review its system to ensure any copies of that school district's data have been permanently deleted from all local equipment and all servers.