Heartland Data Security and Privacy Plan

Purpose
The purpose of this document is to describe the plan for ensuring that confidential data entrusted to Heartland remains secure.

Scope
This plan applies to the District's confidential data that is stored within the MySchoolBucks and Hosted Mosaic systems.

Executive Summary
Heartland seeks to provide a secure computing environment for its hosted service offerings, including MySchoolBucks and Mosaic Cloud. Heartland maintains reasonable administrative, technical and physical safeguards to protect the confidentiality of information transmitted online, including but not limited to encryption, firewalls, password protection, and SSL (Secure Sockets Layer). Heartland has implemented policies and practices pursuant to various security rules and regulations relating to the security and safeguarding of confidential data. However, no precautions, means, or method of transmission which uses the internet or method of storage is absolutely 100% secure. For these reasons, Heartland cannot guarantee absolute security of your confidential data.

Sharing Confidential Data
Heartland may use confidential data for the purposes identified in the agreement with the district. Such purposes may require that the confidential data be shared with third parties, including financial entities that facilitate the flow of funds to/from the district.

Parents' Bill of Rights
Heartland may enter into agreements with parents, guardians, or users authorized by the District, referenced collectively as MySchoolBucks Parents. Notwithstanding any provision of the Agreement between MySchoolBucks Parents and Heartland to the contrary, Heartland adheres to the following Parents' Bill of Rights:

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 stored within MySchoolBucks and Hosted Mosaic will be made available upon request.
5. Parents have the right to have complaints about possible breaches of student data addressed. Such complaints should be sent to the postal address listed under Contact Us in the Privacy Policy on the MySchoolBucks website. https://www.myschoolbucks.com/ver2/etc/getprivacy

Implementation – Data Security
Consistent with industry standards, Heartland applies the PCI DSS guidelines to secure confidential data. The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.

As prescribed by the PCI DSS framework, Heartland implements the following initiatives to address data security issues, including access, data storage, privacy and protection.

1. Install and keep updated a firewall between the public network and the confidential information.
2. Change vendor-supplied passwords that come with network and information processing systems.
3. Safeguard the confidential data stored for business purposes or regulatory purposes.
4. Encrypt all transmissions of customer data over any public network.
5. Maintain antivirus software in all of your computers.
6. Develop and maintain secure systems and applications.
7. Limit access to the confidential data to as few people as possible on the "need-to-know" basis within your business.
8. Identify and authenticate access to system components.
9. Restrict physical access to the systems.
10. Track and monitor access to network resources and confidential data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

Best Practices – Data Storage, Privacy and Protection

As stated in the foregoing, Heartland applies the PCI DSS guidelines to address data security issues, including access, data storage, privacy and protection. These guidelines are the current best practices and industry standards. In a practical sense, all 12 requirements work together to provide a baseline of technical and operational requirements.

Other Data

MySchoolBucks Parents may supply data, including confidential data, to utilize the MySchoolBucks service. The MySchoolBucks Terms of Use and Privacy Policies govern the sharing of data supplied by MySchoolBucks Parents.

Legal Compliance

Heartland has implemented security initiatives that are designed to ensure compliance with applicable laws and contracts regarding data security.

- Our co-location facilities and internal control processes are audited for SSAE 16 certification.
- Heartland engages a third-party Qualified Security Assessor (QSA) for annual PCI compliance audits.
- Heartland is certified for compliance with the Payment Card Industry – Data Security Standard (PCI-DSS) as a Level 1 Service Provider.