Heartland Data Security & Privacy Plan

Purpose

The purpose of this document is to describe the plan for ensuring that confidential data entrusted to Heartland School Solutions ("HSS") remains secure.

Scope

This plan applies to the District's confidential data that is stored within the MySchoolBucks and Hosted MCS and Mosaic systems. To the extent District has the installed version of HSS software, District is responsible for the information security of its data.

Executive Summary

HSS maintains industry standard 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). HSS has implemented policies and practices that reflect a variety of security standards, as well as applicable laws and regulations, relating to the security and safeguarding of confidential data. However, no precautions, means, transmission using the internet, or storage system is absolutely 100% secure. For these reasons, HSS cannot guarantee absolute security of the District's confidential data.

Sharing Confidential Data

HSS complies with the limitations in FERPA, and does not share student data with any third party for marketing or advertising purposes. HSS uses confidential data only 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. HSS also complies with all applicable state laws, including New York's Education Law and the California Consumer Privacy Act.

Parents' Bill of Rights

HSS may enter into agreements with District-authorized parents, guardians, or other users accessing the MySchoolBucks site (collectively "MySchoolBucks Parents"). Notwithstanding any provision of the agreement between MySchoolBucks Parents and HSS to the contrary, HSS adheres to the following Parents' Bill of Rights:

1. HSS will not sell or release a student's personally identifiable information for any commercial purpose.
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 HSS uses safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, when data is stored or transferred by HSS.
4. A complete list of all student data elements stored within the relevant software will be made available upon request.
5. Parents have the right to make complaints about possible breaches of student data. Such complaints should be sent to the postal address listed under Contact Us in the Privacy Policy on the MySchoolBucks website, located at https://www.myschoolbucks.com/ver2/etc/getprivacy.

Implementation – Data Security

HSS has implemented numerous security initiatives designed to ensure compliance with applicable laws and contracts regarding data security. Our internal control processes are audited for SSAE 18 certification, and we are certified as a Level 1 Service Provider with the Payment Card Industry Data Security Standards ("PCI DSS"). PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. HSS engages a third-party Qualified Security Assessor for annual PCI compliance audits. Both the District and HSS need to certify PCI-DSS compliance to accept and process credit and debit card payments.

PCI DSS includes the following requirements:

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 robust antivirus software in all systems.
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.

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.