Brecksville Broadview Heights City School District

Book	Policy Manual
Section	BOARD POLICIES UNDER CONSIDERATION
Title	Copy of Vol. 44, No. 1 - August 2025 New ACCEPTANCE OF PAYMENT BY CREDIT CARD
Code	po6109
Status	Second Reading

New Policy - Vol. 44, No. 1

6109 - **ACCEPTANCE OF PAYMENT BY CREDIT CARD**

The Board authorizes the Treasurer/CFO to manage credit card transactions pursuant to applicable State and Federal laws and regulations, and the regulations of the payment card industry ("PCI").

For purposes of this policy, the term credit card includes branded debit cards (having credit card logo and not requiring PIN input) unless otherwise indicated. Visa, MasterCard, Discover, American Express cards will be accepted for payments.

All fees and charges associated with credit card payments are the responsibility of the payer. Fees will be added to the total cost of the invoice amount.

Compliance with PCI DSS

Credit card data is high-risk confidential information that is protected by State and Federal law and the Board has a legal obligation to protect it. Credit card associations require all merchants to follow protocols entitled Payment Card Industry Data Security Standards ("PCI DSS"). The PCI DSS includes a comprehensive set of international security requirements to help protect cardholder data and prevent fraud and identity theft. Credit card companies require that all merchants comply with PCI DSS before accepting credit cards and must also certify their compliance annually.

All acquirers and card issuers must comply, and must also ensure the compliance of their merchants and service providers who store, process, or transmit customer data.

In order to ensure compliance, the Board is required to:

A. Build and maintain a secure network, which includes installation and maintenance of firewall configurations to protect cardholder data.

B. Not use vendor-supplied defaults for system passwords and other security parameters.

C. Protect cardholder data.

1. The card verification code or value (three (3) digit or four (4) digit code printed on the front or back of the credit card) is not to be stored under any circumstances.

2. The personal identification number ("PIN") or the encrypted PIN block is not to be stored under any circumstances.

3. All primary account numbers ("PANs") should be masked. Viewing will be limited to employees and other parties with a legitimate need to know.

D. Encrypt transmission of cardholder data across open, public networks.

E. Maintain a vulnerability management program, which includes protection against malware and the use of antivirus software that is routinely updated.

F. Develop and maintain secure systems and applications.

G. Implement strong access control measures.

H. Identify and authenticate access to system components.

I. Restrict physical access to cardholder data internally and externally. All paper and electronic records must be stored in secure locations.

J. Track and monitor all access to network resources and cardholder data.

K. Regularly test security systems and processes.

L. Maintain an Information Security Policy – maintain a policy that addresses information security. The policy outlines the Board's incident response plan.

The Treasurer/CFO shall perform periodic audits and advise the Board of the results of such audits and evaluations and of any related action necessary to maintain compliance.

The Treasurer/CFO shall also be responsible for filing annual compliance certificates as required.

Breach of Data

Upon discovering that any Board system has been subject to a breach which compromises personal information, including an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one (1) or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:

A. Social security number;

B. Driver's license number or State identification card number;

C. Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

All employees are required to immediately notify the Treasurer/CFO upon discovering that any system containing personal information has been breached. Failure to do so may result in discipline, up to and including termination.

Following the discovery or notification that a system containing personal information has been compromised, the Treasurer/CFO or designee shall promptly send written or electronic notice to any resident of Ohio whose personal information was or may have been exposed if the access and acquisition by an unauthorized individual or entity causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. Notice must be sent no later than forty-five (45) days after discovering the breach, unless such notice interferes with law enforcement activities. The notice will inform the individual of the data that may have been accessed and acquired, as well as what steps have been taken to restore the system's integrity.

Legal R.C. 1349.19