MSBOA Privacy Policy

Your privacy is very important to us. Accordingly, we have developed this Policy in order for you to understand how we collect, use, communicate and disclose and make use of personal information. The following outlines our privacy policy.

- Before or at the time of collecting personal information, we will identify the purposes for which information is being collected.

- The collect and use of personal information solely with the objective of fulfilling those purposes specified by us and for other compatible purposes, unless we obtain the consent of the individual concerned or as required by law.

- We will only retain personal information as long as necessary for the fulfillment of those purposes.

- We will collect personal information by lawful and fair means and, where appropriate, with the knowledge or consent of the individual concerned.

- Personal data should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete, and up-to-date.

- We will protect personal information by reasonable security safeguards against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

We are committed to conduct our activities in accordance with these principles in order to ensure the confidentiality of personal information is protected and maintained.

MSBOA Refund Policy

It is the practice and policy of the Michigan School Band and Orchestra Association to not refund any fees unless there is a clear and uncontested transaction of over payment.

MSBOA Policy for Delivery/Shipping of Services

Upon receipt of your order, the services will be performed to you in accordance with the terms applicable to the services that you purchased. The nature of the services you purchased and the date of your purchase may impact the timing of performance of the services. The services will be deemed to be successfully delivered to you upon performance of the services.

MSBOA Terms and Conditions

for

Credit Card Transactions

Purpose

In order to accept credit card payments, the Michigan School Band and Orchestra Association is required to comply with Payment Card Industry Data Security Standards (PCI DSS), which were established by the major credit card companies (American Express, Discover, JCB, MasterCard, and Visa) to protect merchants and cardholders from cardholder information theft. This policy will be reviewed at least annually and will be updated as needed to reflect changes in PCI DSS standards.

Policy

MSBOA will accept credit card transactions for all MSBOA State related activities and functions. Such activities and functions shall be and are not limited to: MSBOA School membership fees, All-State fees, Mid-Level String Clinic fees, State Solo & Ensemble Festival fees, State Band and Orchestra Festival fees, State Jazz Festival fees, Workshop fees and MYAF Soloists audition fees.

Credit card information is defined here to mean the full credit card number, the card verification code or the PIN. Credit card numbers appearing on receipts or reports must be truncated to the last 4 digits.

Devices used to process credit card transactions must be dedicated to processing credit card payments and may not be connected to other network services such as e-mail.

Access to cardholder data must be limited to only those individuals whose jobs require such access. Each individual with access to credit card information must have a unique user ID. User IDs should not be shared with other individuals.

All Information Technology data security standards are required to be followed when accepting credit card payments.

Processing credit card payments over the internet:

1. MSBOA has contracted with an online payment gateway that is PCI DSS compliant for receiving, transmitting and storing credit card data. Cardholder transaction information is collected and securely stored directly with the payment gateway or processor, at no time is credit card information collected or stored on MSBOA computers.

2. MSBOA may obtain information directly from the payment gateway, only the information necessary to apply the payment (such as the name, amount and authorization code) may be retained. Files or print reports should not contain credit card information. The full contents of any data from the magnetic stripe, the card verification code and the PIN must not be stored under any circumstances. In the event of a dispute the transaction can be researched from the processor's website via a secure login.

Reporting security incidents:

MSBOA State Office Staff must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All have the responsibility to assist in the incident response procedures within their particular areas of responsibility.

Examples of security incidents that the State Office might recognize in their day to day activities include, but are not limited to:

- Theft, damage or unauthorized access (i.e. papers missing from their desk, broken locks, missing log files, alert from public safety, evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud – inaccurate information within databases, logs, files or paper records

MSBOA will immediately notify Huntington Bank of any suspected or real security incidents involving cardholder data. Huntington Bank should file an incident report as a result of the notification.