ELECTRONIC PAYMENTS IMPLEMENTATION AND CREDIT CARD DATA SECURITY POLICY

Original Date: _____
Last Revision Effective: _____
Policy Contact: _____

Statement of Intent

Wonderful Day School (WDS) acknowledges the growing use of electronic and online payments as a means of providing greater convenience to parents, streamlining internal processes and remaining current for our community. WDS further acknowledges a fiduciary obligation to ensure that implementing an electronic payments system maximizes campus-wide benefits while minimizing costs and negative impacts. Accordingly, to ensure that benefits are maximized and costs and negative impacts are minimized, it is WDS's intent to establish a consistent campus-wide electronics payment implementation and credit card data security policy. This policy will ensure that all stakeholders understand the true and total costs and impacts including the risk/cost/benefit in acquiring, implementing and using electronic payments. This policy serves as an umbrella that governs all WDS procedures pertaining to electronic payment usage on campus, and complies with the WDS Financial Services and Information Services IT Security Audit.

The WDS Electronic Payments Implementation and Credit Card Data Security Policy is acknowledged as a "living" document that may require alteration periodically to address changes in technology, applications, procedures, legal and social imperatives, and unanticipated dangers.

Applicability

This policy applies to all members of the WDS community, with specific duties and responsibilities placed upon departments that accept credit card payments or eCheck payments, in person or via the internet. This policy applies to all campus facilities, equipment and services that are managed by the WDS information resources department, including off-site data storage, computing and telecommunications equipment. This policy also applies to ecommerce application-related services purchased from commercial concerns, and internet-related applications and connectivity.

Intended Exemptions

If applicable, delineate exemptions here.

Campus-Wide Managed Approach

It is the sole responsibility of the Business Office to provide oversight of all tasks and procedures that directly pertain to maintaining an optimal campus-wide electronic payment infrastructure at all times. It is the responsibility of all members of the school community to participate and share this obligation, as specified by all supportive policies and procedures pertaining to electronic payments use on campus.

An optimal electronic payment infrastructure meets the following criteria:

- Enables ongoing campus-wide compliance with Payment Card Industry Data Security Standard (PCI-DSS) with minimal time, effort and cost.
- Enables the streamlining of payments in a manner that reflects positively on the school and that provides convenience to both parents and staff.
- Leverages the lowest cost electronic payments such as debit card and eCheck when practical.
- Leverages the total campus-wide volume to negotiate the best rates for credit card acceptance with one or the fewest possible and most value-adding providers.
- Minimizes to the lowest reasonable number the types of interfaces (gateways and terminals) to allow for lowest cost of integration and easy staff training.
- Avoids, whenever practical, relationships with vendors who contractually dictate the use of specific gateways and/or electronic payment providers.

An optimal electronic payment infrastructure will be maintained at WDS by upholding the following guidelines and standards:

- WDS will operate in a manner consistent with the PCI-DSS and NACHA rules for the protection of sensitive data and business transactions. These two data security standards are embedded into the WDS's Information Security Policy.
- WDS will operate in a manner consistent with the FTC Red Flag Rules to ensure correct and prompt reporting of any signs of an attempt to breech data or access information which could compromise an individual's identity.
- WDS will maintain an updated full inventory of all electronic payment related services, systems and associated personnel at all times.
- WDS requires that all school staff contemplating or researching a change to the resources in the inventory involve the business office in the process early, to ensure that all options are evaluated with campus-wide goals and objectives in mind.
- WDS requires a cost/benefit and PCI-DSS impact report to be done prior to approving any changes to a point of electronic payment on the inventory.
- WDS will ensure that all school employees are appropriately familiar with all electronic payments policies and procedures, and are aware of their personal responsibilities to evaluate, use and manage electronic payment resources on campus. WDS will provide training to each employee in the security procedures for which they are responsible.

- WDS will review its electronic payments processes, contracts, policies, procedures, and practices annually. In the event of any significant changes to its business, computing, or environments, WDS will make appropriate updates as necessary.
- A compliance audit of this electronic payment policy will be conducted every three years and will be performed by knowledgeable parties independent of WDS employees, such as the school auditor.

RESPONSIBLITIES

Business Office (BO)
The Business Office is responsible for:

- Maintaining the Campus-Wide Electronic Payments Inventory on behalf of the school including comprehensive documentation of all processes.
- Reviewing, approving and signing all contracts related to electronic payment assets.
- Training and educating the department heads regarding their role and responsibilities in adhering to the electronic payments policy.
- Providing the school with secure web applications, payment services, infrastructures, and procedures for addressing the electronic payment needs of the school.
- Following and enforcing internal standards established for creating and maintaining an optimal electronic payments infrastructure campus-wide.
- Notifying human resources and the appropriate administrator(s) when an individual or individuals have knowingly compromised the electronic payment policy or any related IT security policy on campus.

Department Heads (DH)
Each Department Head is responsible for:

- Engaging the business office early and often in initiatives aimed at changing an electronic payment asset, so that negotiation can set expectations with the prospective vendor early in the process.
- Informing the business officer immediately if the electronic payment asset vendor indicates any changes in terms, process or technology.
- Drafting, submitting to the business office for approval and abiding by the approved and documented processes for using any electronic payment asset.

DEFINITIONS

Electronic Payments

‘Electronic payment’ is defined as any credit card, debit card, stored value, ACH and eCheck payment that originates via the school’s web site or by the keying in of payment account information by school staff into a credit card terminal or virtual terminal.

Electronic Payments Assets

‘Electronic payment assets’ are defined as all types payment facilitating systems, services and data stored or transmitted on behalf of the school. This may include but is not limited to payment processing contracts, payment gateways, web application and credit card terminals.

Payment Card Industry Data Security Standards (PCI-DSS)

The PCI Data Security Standard represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information. Compliance is a term / condition of every merchant agreement.

REVISION HISTORY

Original _____

Revision _____

APPROVED BY

_____

Name, Title

_____

Name, Title