Privacy Policy

Introduction
Oregon Episcopal School or its licensors (hereinafter referred to as OES) are committed to protecting your privacy as an Internet user whenever you transfer funds to a Merchant through Authorize.Net. The Merchant will generally be using Authorize.Net when the cardholder is using a credit or debit card over the Internet or an Unattended or Integrated EFTPOS system. OES recognizes its responsibility to keep confidential at all times any information which OES acquires in connection with such a transaction, whether directly from the Cardholders or Fund Transfer. OES protects personal information (at a minimum) to the Payment Card Industry Data Security Standards, and the services OES uses to facilitate such transactions are SSAE 16 Type II compliant. Please note however; OES responsibility is limited to protection by OES of information which OES obtains. OES itself cannot, of course, control the use or disclosure by your supplier of any information which they obtain from you.

Collection of Information
To enable OES to provide secure payment facilities it will typically acquire information which may include the Cardholder’s name, credit card number (with the expiry date), or Check routing and account number for eCheck payment and billing address.

Use and Disclosure of Information
OES uses the information to obtain authorization of the transaction from the issuing bank of the credit card, eCheck, and OES’s own or the Merchant's bank and to process the payment. OES uses a third-party service provider to manage credit card processing. This service provider is not permitted to store, retain, or use billing information except for the sole purpose of credit card processing on the OES’s behalf. Some details from the transaction (such as name, email and delivery address) may be made available to OES through PCR Educator – OES’s Admission and Student information system.

Security
OES is committed to data security, and OES uses appropriate administrative, technical, and physical security measures to protect personal information it receives through its websites. OES uses a variety of technologies and procedures to help protect personal information from unauthorized access, use or disclosure. For example, OES stores the data on hosted computer servers with limited access that are located in controlled facilities secured by the latest in surveillance and security technology. When OES transmits sensitive information (such as credit card numbers), OES protects it through the use of encryption, such as the Secure Socket Layer (SSL) protocol. Credit card details stored onsite are encrypted using 168bit 3DES encryption.
**PCI DSS**

PCI DSS, the Payment Card Industry Data Security Standard, is a set of security requirements relating to the protection of card holder data. The standard is governed by the PCI Security Standards Council, an organization put together by most of the major card schemes including VISA, MasterCard, American Express, JCB, and Discover. It's relevant for any entity that stores or transmits sensitive card holder data, such as the PAN (card number), card security code, track data, and PIN block. The current version of the standard is Version 1.2. Preceding PCI-DSS, the card schemes had their own standards, and the VISA Account Information Security (AIS) standard formed the basis to most of the PCI-DSS requirements.