



Website Privacy/Security Policy

Background:

If a nonprofit organization/school engages in any of the following activities, it's necessary to take serious steps to address cybersecurity risks to the organization's own data security as well as to its donors, individuals and students it serves.

- Conduct e-commerce on its website, such as processing donations or event registrations?
- Store and transfer (such as by sending to the cloud) “personally identifiable information,” about anyone, including donors? (Common examples of personally identifiable information include: clients’ addresses, credit card information, etc.)

Other recommended steps:

- Create inventory tools that ask: What data do we collect about people? What do we do with it? Where do we store it? Who is responsible for it? What is the cost/benefit of maintaining this data? (We may find that there is data SSES is currently asking for and keeping that it does not really need).
- Reduce or limit the data that SSES collects and streamline the storage process (as well as diligently destroying data in accordance with the school’s document retention policy) could be easy first steps towards mitigating risk.
- Document retention policies are one of several good governance policies that the IRS highlights on the IRS Form 990 by asking whether the filing nonprofit has adopted a written record retention policy.
- Know whether the data SSES collects and maintains is covered by federal or state regulations as “personally identifiable information.” Forty-seven states’ laws including Pennsylvania require nonprofits to inform persons whose “personally identifiable information” is disclosed in a security breach. Protecting personally identifiable information is all about training staff how to collect/store/dispose of and generally protect this data. Even if we are collecting data that doesn’t rise to the level of “personally identifiable information,” such as a community theatre collecting information on attendees’ preferences for plays or musicals, a breach of that data can be harmful to the organization’s reputation and ability to bring in contributions. All data reflecting personal preferences are important to keep secure.

Purpose

With the increased reliance upon electronic data, and the maintenance of personal information of students, employees, potential families, and donors the School Board of Directors is concerned about the risk of a breach in the School's electronic system security and possible disclosure of personal information and acquisition of computerized data that compromises the security and confidentiality of personal information. This policy applies to information SSES collects on the website, in email, text and other electronic messages.

Authority

The St. Stephen's School Board of Directors directs that the Interim Head of School shall provide appropriate notification of a computerized system security breach to any individual whose encrypted and unredacted personal information was or is reasonably believed to have been accessed or acquired by an unauthorized person.

Definitions

Personal information- includes an individual's first initial and last name in combination with and linked to any one or more of the following, when not encrypted or redacted:

1. Social security number
2. Driver's license number or state identification card number issued instead of a driver's license.
3. Financial account information, credit or debit number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

Website Privacy Policy SSES Board Approved 4_19_2021

St. Stephen's Episcopal School (SSES) is committed to protecting the privacy of visitors to its website. This Privacy Policy describes how SSES uses and protects the information we collect from you through this website but does not apply to information we may collect from you offline.

By visiting this website, you consent to SSES's collection, use, storage, deletion, and disclosure of your information as described in this Privacy Policy. This Privacy Policy is effective as of April 19, 2021 and is applicable only to this website and not to any other third-party website that you may be able to access from this website.

St. Stephen's Episcopal School may modify this Website Privacy Policy from time to time and changes will be effective when posted on this page.