STUDENT DATA SECURITY AND PRIVACY

Children's Scholarship Fund ("CSF") has been empowering families to find the education option that best fits their children's needs since 1998. CSF is committed to the protection of student data privacy.

CSF will:

- Use data for authorized education purposes only

- Implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Student Personally Identifiable Information and non-public information.

- Enforce strict limits on data retention and destruction (See: Records Retention and Document Destruction Policy)

- Be transparent about the collection and use of data

- Inform the State of any security incident or Data Breach in accordance with NH RSA Chapter 359-C:20: Notice of Security Breach.

Student Personally Identifiable Information ("PII")

Student Personally Identifiable Information or PII is defined as data or information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information which includes but is not limited to, the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, and other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name.

How CSF Protects Student Privacy, PII and State Data

- CSF contracts with third-party, SOC II (System and Organization Controls 2) compliant providers/vendors to secure, encrypt, store and backup data.

- CSF does not sell, use or disclose student PII for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purposes or permit another party to do so.

- CSF requires that third-party vendors maintain the confidentiality of Student PII in accordance with state and federal law.

- CSF does not include Student PII in public reports without prior permission by parents or the eligible student. CSF may share pictures, videos, and/or newsletters that celebrate the achievements of students. Such media may contain student names, images, or information pertaining to a student's achievement with prior permission.

- CSF will only report aggregated (non-identifying) student data which is required by law to the New Hampshire Education Department ("NHED").

What is SOC II Compliance?

SOC 2 is a framework applicable to all technology service or SaaS companies that store customer data to ensure the organization continues to mitigate the risk of data exposure. It outlines five trust service principles of security, availability, processing integrity, confidentiality, and privacy of customer data as a framework for safeguarding data.

SOC 2 compliance is part of the American Institute of CPAs' Service Organization Control reporting platform. Its intent is to ensure the safety and privacy of customer data, that the company will comply with regulations, and that it has the processes in place to mitigate risk.

What is a SOC II Compliance Report?

A SOC II Compliance Report is designed to certify the security, processing integrity, availability, confidentiality, and privacy of hosted systems and the data that they store or process.

SOC II Compliant Providers/Vendors

CSF contracts with Neon One. Neon One is SOC II Compliant and utilizes Amazon Web Services ("AWS") for server hosting in connection with the Neon One services. AWS provides highly secure data centers that use state-of-the art electronic surveillance and multi-factor access control systems. Neon One uses a variety of industry best practices including but not limited to SSL technology, Server Digital Certificates and 2-Factor Authentication (2FA) to encrypt and secure sensitive data traffic over the Internet. Data replication is over private connections and the database is not directly accessible by IP address from the public Internet.

CSF contracts with Kleo, Inc. dba ClassWallet ("ClassWallet"). ClassWallet is SOC II Compliant and provides a digital wallet and spend management technology platform designed for school districts, nonprofits and state agencies. ClassWallet utilizes Amazon Web Services ("AWS") and industry best practices including but not limited to SSL technology and Server Digital Certificates to secure its data systems.

CSF utilizes Microsoft Office 365 (SOC II Compliant), to provide Microsoft Corporation's Office 365 ("O365"). O365 services are designed to provide performance, scalability, security, management capabilities, and service levels required for mission-critical applications and systems used by business organizations. O365 is physically hosted in Microsoft-managed datacenters utilizing industry best practices including but not limited to SSL technology and 2- Factor Authentication (2FA).

Approved: October, 2021