



Data Security Policy

Freedom School Partners (FSP) takes data security and privacy of highest priority. All personally identifiable information¹ of scholars and families, volunteers, and donors are stored and kept secure in encrypted cloud drives with user control access. Additionally, FSP data security policies and procedures include the following:

- Any Partners, Vendors or Contractors who collect or have access to personally identifiable information must adhere to data storage, use, transfer, and destruction policies. Only FSP staff, partners, vendors, or contractors will have access to FSP data.
- FSP will work with all contractors or vendors to ensure the transfer to the vendor includes only the minimal level of data needed. Contractor/Vendors will store all FSP data in a secure, password protected environment, and any PII data a contractor receives must be destroyed after the intended use of the data.
- FSP has two confidentiality agreements parents are asked to review and sign. On these, parents indicate whether their scholars' individual level data and/or photographs of the scholar may be used by FSP.
- For reporting, any sub group less than five will be reported as <5 to prevent potential re-identification of students. Sharing out of any personally identifiable data for any unapproved reasons is *strictly* prohibited

¹PII include: Names, DOBs, Addresses, Phone Numbers, Email Addresses

Aug 8, 2024