School 21
Data Privacy & Protection Plan

Last Updated: August 16, 2021

Introduction and Purpose

School 21 seeks to provide an outstanding customer experience in every regard. To provide this experience, we gather certain information about customers, and that information must be safeguarded. This Data Privacy & Protection Plan outlines how School 21 ensures that customer data is protected and kept private.

This plan helps ensure that School 21:

- Aligns with applicable laws and best practices
- Protects the rights of our customers
- Can communicate transparently to key stakeholders about our policies
- Is protected from data breaches and other events that could cause harm to our customers and School 21 itself

This plan is intended to help key stakeholders, including customers and employees, understand how School 21 policies support the goals listed above.

Data Protection and Privacy Laws and Best Practices

School 21 provides online education services to customers in a variety of locations. Depending on a particular customer location, various federal, state, local and other laws may apply to how customer data must be protected.

In addition, technological and organizational management best practices, that may not be legally required, have been established to protect customer data and privacy.

To best serve our customers, School 21 aligns with these laws and best practices. Some of the key ways School 21 aligns with these laws and best practices, across locales, include the following:

- We only gather the Personally Identifiable Information (PII), such as names and emails, that is necessary for School 21 to provide an excellent experience to our customers
- We only retain PII for as long as a customer is active with School 21, and we take steps to securely destroy PII when it is no longer necessary to serve the associated customer(s)
- We only share customer PII (for instance, student progress data) with institutions (such as schools and districts) or individuals (such as parents) who have engaged School 21 to serve those customers; we do not share PII with any other third parties unless legally required to do so (such as by a law enforcement agency), and we do not sell customer PII to other third parties
- We have policies to protect customer information, including:
    - Limiting the number of School 21 personnel who have access to customer PII
    - Training School 21 personnel on how to protect customer data
    - Taking steps to respond if customer PII is compromised

Guidelines for School 21 Personnel
All School 21 personnel (including owners, employees and subcontractors) have responsibility to protect customers data. The following policies outline those responsibilities.

General Guidelines

School 21 policy requires that:

- The only personnel who are able to access customer PII are those who need it to do their work
- Customer PII should not be shared informally
- All personnel undergo training, provided by School 21, to help them understand their responsibilities when handling customer PII
- All personnel should keep data secure, by taking sensible precautions and following the guidelines below
- Customer PII should not be disclosed to unauthorized people

Data Storage

School 21 data is primarily stored electronically. The following policies apply to data storage:

- Data should be protected from unauthorized access, accidental deletion and malicious attacks
- Strong passwords should be used for any systems that access customer PII; passwords must not be shared
- When stored electronically, customer PII should only be stored on designated drives and servers
- In general, data should not be transferred to removable media or paper unless necessary; any removable media or paper storing sensitive data should be physically locked away securely when not in use
- Data should be backed up periodically

Data Use

School 21 personnel should use the following best practices when using or accessing customer PII:

- Sensitive data should only be accessed when required to perform a necessary task
- Sensitive data should not be transferred manually unless encrypted
- When sensitive data is transferred by systems, it should be encrypted (e.g, through https)
- Personnel should never share data informally (such as through email), unless it is absolutely necessary to serve our customers
- Personnel should ensure that the screens of their computers are locked when left unattended

Data Accuracy

Per applicable laws and best practices, School 21 takes reasonable efforts to ensure that customer data is accurate within our systems, specifically:

- We provide customers the ability to update their data in our system, directly through the School 21 interface and by emailing support@school21.net
- Customer data is stored in as few places as possible
- When we discover that data is inaccurate, we take reasonable steps to correct the inaccuracy

Customer Access and Information Sharing

Per applicable laws and best practices, School 21 will respond to customer requests about their data, with the following information:

- What data we collect about customers, and what data we have about the customer making the request
- How customers can gain access to and update their PII data from School 21
- How they can keep their data on School 21 up to date
- At a high level, the steps we take to protect PII data
- How we use their data
- Our Privacy Policy, which addresses many of the components of this Data Privacy & Protection Plan

Cybersecurity

School 21 aligns its management of cybersecurity issues to the Cybersecurity Framework (version 1.1) of the National Institute of Standards and Technology (NIST). The following table outlines, at a high level, this alignment.

Framework Component	Description	School 21 Alignment
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities	School 21 has analyzed, and continues to analyze ongoing, the business context and resources that enable the prioritization of risk management strategies, addressing: business environment, risk assessment, risk management strategy, asset management, and governance
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services	School 21 has put into place systems and processes to limit and/or contain the impact of a potential cybersecurity event, addressing: identity management and access control; awareness and training; data security; data backup; information protection processes; policies and procedures; maintenance; and protective technology
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event	School 21 has instituted appropriate monitoring processes and/or systems to detect the occurrence of a cybersecurity event
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident	School 21 has put into place processes for how to respond in the case of a cybersecurity event, including communications plans, key personnel and roles, and steps to be taken

Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident	School 21 has developed plans for how to recover from a cybersecurity event, including communication plans, key personnel and roles, and steps to be taken