

NobleHour Student Privacy Pledge

Online community engagement first starts with trust between parties. When you register with NobleHour, we're committed to providing you with a secure infrastructure that allows you to privately conduct services or activities during your academic career. It's inevitable that various data such as hour logs, messages, identities, schedules, and affiliations will be exchanged during the course of your membership. Our services, backed by the latest technology and standards, provide a secure environment for this to occur.

We are vigilant in how your personal information is handled, and as a result, have aligned our efforts with the [Student Privacy Pledge](#), a national commitment by school service providers to safeguard the collection, maintenance, and use of your personal information. NobleHour not only exceeds the commitments of this privacy template, but also current federal requirements. The **SPP** states that we will:

- Not collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student.
- Not sell student personal information.
- Not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students.
- Not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student.
- Not make material changes to school service provider consumer privacy policies without first providing prominent notice to the account holder(s) (i.e., the educational institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent) and allowing them choices before data is used in any manner inconsistent with terms they were initially provided; and not make material changes to other policies or practices governing the use of student personal information that are inconsistent with contractual requirements.
- Not knowingly retain student personal information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student.
- Collect, use, share, and retain student personal information only for purposes for which we were authorized by the educational institution/agency, teacher or the parent/student.

- Disclose clearly in contracts or privacy policies, including in a manner easy for parents to understand, what types of student personal information we collect, if any, and the purposes for which the information we maintain is used or shared with third parties.
- Support access to and correction of student personally identifiable information by the student or their authorized parent, either by assisting the educational institution in meeting its requirements or directly when the information is collected directly from the student with student/parent consent.
- Maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.
- Require that our vendors with whom student personal information is shared in order to deliver the educational service, if any, are obligated to implement these same commitments for the given student personal information.
- Allow a successor entity to maintain the student personal information, in the case of our merger or acquisition by another entity, provided the successor entity is subject to these same commitments for the previously collected student personal information.

As a result of our commitments, we would like you to know how your data is handled during the course of your membership. Our team adheres to the following procedures:

- ✓ **We will** only retain your personal information for the period necessary to fulfill the purposes outlined in our [privacy policy](#), in accordance with data retention laws, for fraud detection, or to comply with applicable state and federal laws.
- ✓ **We will** protect any post-deleted data. While some personal data may still exist after account deletion in backup form (for example, social media messages or other unaffiliated services), we will never display, distribute, or use this data for standard operations.
- ✓ **We will** always maintain a comprehensive privacy program that includes third party security audits, employee background checks, technology safeguards, and extensive operational protocols to secure your personal information. For quality assurance purposes, we do test our systems using real data. This data is first anonymized to maintain privacy and then destroyed after testing is completed.
- ✓ **We will** always maintain an open line of communication with our member students, parents, and academic institutions to vigorously promote online privacy and security.

Revision History

6.11.2015

Document approved for circulation.