RAPIDIDENTITY AS A SERVICE

COPPA STATEMENT

IDENTITY AUTOMATION

COPPA[1] BACKGROUND AND SUMMARY

The Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§ 6501–6506 (Pub.L. 105–277, 112 Stat. 2681-728, enacted October 21, 1998, effective April 21, 2000)) is a federal law that applies to the collection of personal information from children under the age of 13, by individuals or companies. The law applies to websites / applications and online social media providers and requires that these entities obtain appropriate parental consent before attempting to gather information from students and children covered under the act. Additionally, the law requires operators to publish clear privacy policy notices, in proper locations, whenever personal information is being obtained and to disclose any personal information that is collected to a child's parents. The act gives parents the right to revoke their consent, as well as to have any applicable information deleted from the site or application, and it requires that proper care is taken to ensure the confidentiality, security, and integrity of all information obtained from the children. Finally, it contains a 'Safe Harbor" provision, which allows for exemptions to specific rules of COPPA, provided an industry group has submitted self-regulatory guidelines and subsequently had them approved by the Federal Trade Commission (FTC).

Depending on the type of identity, data, and access services provided, RapidIdentity may need to store certain amounts of education records. Typically, RapidIdentity provides a platform used by educational institutions to restrict access to these types of records, which are considered "directory" information, and does not store the records. In other instances, RapidIdentity provides full identity and data lifecycles, which requires storing of and processing educational records between source and target endpoints. Therefore, we maintain comprehensive security and privacy guidelines that support COPPA's objective and also have signed the Student Privacy Pledge as part of our commitment to student data privacy and security.[2]

RAPIDIDENTITY AND COPPA

Identity Automation and RapidIdentity guidelines that adhere to COPPA:[3]

- Review and Amend Education Records - RapidIdentity provides users with a view of their user profile that outlines the specific attributes collected for creating and managing one's digital identity. This provides users with a clear view of what data is part of their education record, as well as a means for updating the information if it is not accurate.

- Secure Data Transfer - Data is the lifeblood of any IAM system. IAM systems generally require user data to be collected from authoritative sources, go through various transformations, and then be provisioned to a variety of target systems. In all of these instances, RapidIdentity uses encrypted protocols to ensure the secure connection and transport of user data from end-to-end.

- Consistent Security Policy - Most compliance regulations require organizations to define, implement, and adhere to consistent security policies. RapidIdentity enables organizations to maintain compliance by centrally implementing the configurations outlined in the security policies and automating the actions in a consistent manner. The automation reduces inconsistently implemented COPPA policies among organizational silos and reliance on manual processes that are prone to human error.

- Contextual Security Policy - Organizations often desire contextual based security policies that outline specific use cases or controls, instead of generic directives that are loosely followed and have potential gaps. RapidIdentity thrives on context and can support these detailed COPPA policies. The foundational method for supporting the COPPA policies uses identity data attributes to make granular data requests and collection decisions based on context outlined in the policies. This is important in assuring that data collection can be appropriately tailored by a student's age, ensuring that improper data is not be requested of a child under the provisions of COPPA.
    - For example, a COPPA-appropriate RapidIdentity security policy context of "No challenge / response questions will be established for children 13 and under, which request personal information…." can be derived by identity attributes, such as grade level, attributes containing age / date of birth, school location, or inclusive of combinations of these attributes, in order to make granular decisions upon which data collection can be based. In contrast, a

typical, generic policy of "some students are required…," while providing room for interpretation, would not be strict enough to meet COPPA standards.

- Policy Detail for Challenge / Response - RapidIdentity supports customizable challenge / response policies and provides a "Friendly Policy Description" field that can be used to notify users of the privacy policy and information for the data being requested. This complies with COPPA's requirement to post privacy and informational notices on screens that request / require user-supplied data or personal information. As noted (in Contextual Security Policy), these can be tailored to individual user or age-appropriate groups based on data filters.

- Data Access Control - RapidIdentity supports three levels of access control: Discretionary Access Control (DAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC). The support for coarse and fine-grained access controls ensures the right people have access to the right resources and for the right amount of time.

- Reduce Intrusion Risks - There is no one way to completely eliminate the risk of a cyber intrusion. RapidIdentity mitigates this risk by providing a layered countermeasure approach of prevention, detection, and response. Identity functions, such as privileged account management, strong password policies, detailed auditing, and multi-factor authentication, help mitigate intrusion attempts that lead to information disclosure, a direct violation of COPPA.

- Time-based access expiration - RapidIdentity offers time-based access expiration, which enforces security without being dependent on periodic and manual re-certification campaigns. Access is renewed only when it is necessary, significantly reducing COPPA violations.

- MOA and/or Legal Contract Agreement - Identity Automation typically signs a legally binding Memorandum of Agreement and/or other contract that outlines the COPPA (and other compliance) requirements for organizations that must adhere to specific parameters. Examples include:
  - Vendor is not allowed to maintain, use, disclose, or share student information in a manner not allowed by federal law or regulation.
  - Vendor may not use the data shared under the agreement for any purpose other than authorized research and analysis.
  - Require all Vendor employees, contractors, and agents of any kind to comply with all applicable provisions of COPPA and other federal laws, with respect to the data shared under the agreement.
  - Maintain all data obtained pursuant to the agreement in a secure environment and not copy, reproduce, or transmit data obtained, except as necessary to fulfill the purpose of the original request.
  - Not to disclose any data obtained under the agreement in a manner that could identify an individual student, except as authorized by COPPA, to any other entity.
  - Destroy all data and provide verification in writing of the destruction of all copies of the data obtained under the agreement upon contract termination.

- Agreement for Sharing of Data - Identity Automation receives written approval from an education entity before distributing any user data to integrated target applications.

- Project Management and Documentation - Identity Automation documents and maintains all user data mappings between source systems, IAM components, and target systems as part of our standard project management and documentation processes. This ensures Identity Automation, the education organization, and other parties know exactly which user data attributes are being used and (securely) exchanged in support of identity services.

- Workflow for Privileged Account Management - In RapidIdentity, Workflow describes the step-by-step process to request, approve, certify, and revoke access beyond what is provisioned, based on a user's organizational role. Resource access states are called entitlements. Generally, users request an entitlement, the request is directed to the entitlement owner, the request is approved or denied, and then the user is notified accordingly. For example, a user may need system administration rights to perform a search across an entire school system; however, access to this role increases organizational risk as it provides a single person with access to more education records. To mitigate risk, but allow for reasonable productivity, the workflow could be granted with a stringent access time period (e.g. 3 hours). This is another way RapidIdentity ensures proper access control through least

privilege to align with COPPA objectives.

- Delegated Administration - RapidIdentity supports delegated administration by allowing privileged users and roles the ability to perform IT-related tasks. Possible actions include: Change Password, Edit Profile, Change Challenge Responses, Enable, Disable, Unlock, Export Data, and Print Data. Custom delegations support Attribute Based Access Control (ABAC) and RapidAppliance Roles. Common custom delegations include allowing a project manager to see specific project team leaders and enabling teachers to see students in the classes they teach. Both the project manager and teacher can be delegated the ability to enable and disable users on their teams or in their classes, along with other delegation actions as necessary. This is another way RapidIdentity ensures proper access control through least privilege to align with COPPA objectives.

As K-12 schools and Higher Education institutions are two of the larger customer groups to whom Identity Automation provides solutions, and given our identity and access management (IAM) offering, we're in a unique position to see all sides of the student privacy issue. We are responsible for protecting students individually, as well as the school or school district as an organization. In some situations, the prospects we talk with assume there is a dichotomy that exists — we can secure either the student or the school, but not both. This is a false perception that we've run into a surprising number of times as the topic of student privacy has become more prevalent. Identity Automation works with each customer to ensure proper compliance with COPPA (and other appropriate regulations) during the initial deployment and over time as IAM functions/needs change.

RESOURCES

Identity Automation Is a Proud Signatory of the Student Privacy Pledge
http://blog.identityautomation.com/education/2015/identity-automation-proud-signatory-student-privacy-pledge

Student Privacy in Education - Analyzing Student Privacy: Its History, Issues, and Implications

Privacy in education is a subject on the rise. Everyone involved in school technology treads a fine line, balancing the security issues that are vital to the operation of a school district with the individual privacy rights of the actual classroom users of technology. But where is that line, and how does IT staff know if it has been crossed?

http://info.identityautomation.com/student-privacy-in-education-ebook

1 COPPA information obtained from the Cornell University Law School: https://www.law.cornell.edu/uscode/text/15/chapter-91
2 http://blog.identityautomation.com/education/2015/identity-automation-proud-signatory-student-privacy-pledge
3 Note: Guidelines are not applicable to all customers and implementations of RapidIdentity

Contact Sales: sales@identityautomation.com
Contact Support: support@identityautomation.com
Other information: info@identityautomation.com

Toll Free: 877-221-8401
Voice: 281-220-0021
Fax: 281-817-5579

Corporate Headquarters:
8833 N. Sam Houston Pkwy. W.
Houston, TX 77064

IDENTITY AUTOMATION