Building Trust in a Computer Science Professional Development Passport for K-12 Teachers

Joseph C. Tise
joe@csedresearch.org
Institute for Advancing Computing Education
Winchester, Virginia, USA

Monica M. McGill
monica@csedresearch.org
Institute for Advancing Computing Education
Peoria, Illinois, USA

Robert Schwarzhaupt
rschwarzhaupt@air.org
American Institutes of Research
Arlington, Virginia, USA

Abstract

The Computer Science (CS) Professional Development (PD) Passport Alliance has created an addition to the Computer Science Teachers Association (CSTA) member platform that provides the capability for CSTA members to track their CS PD-related activities in one convenient place. As part of our research effort supporting the platform development, one of our research questions was: *Among teachers, what features or practices are associated with trusting in software that contains professional personally identifiable information (PII)?* We conducted an exploratory mixed methods study (teacher interviews $n = 17$, teacher survey $n = 495$, program evaluation survey $n = 494$) to determine what enables trust in software that stores professionally identifiable information and which features were most important to teachers future use of the platform. We provide recommendations for the project implementation team (such as adding multi-factor authentication to the platform) to mitigate risks of a data breach (which our survey indicated would impact 98% of the respondents' perceptions).

ACM Reference Format:
Joseph C. Tise, Monica M. McGill, and Robert Schwarzhaupt. 2026. Building Trust in a Computer Science Professional Development Passport for K-12 Teachers. In *Proceedings of the 57th ACM Technical Symposium on Computer Science Education V.2 (SIGCSE TS 2026), February 18–21, 2026, St. Louis, MO, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3770761.3777212

1 Introduction and Background

The Computer Science (CS) Professional Development (PD) Passport Alliance has developed an enhancement to the Computer Science Teachers Association (CSTA) member platform, enabling members to conveniently track all their CS PD activities in one place. While there is significant research on protecting student data, there is little research on teachers' perspectives on the privacy and security of their data, particularly for data related to their roles as teachers. Nevertheless, we are aware of the risks that may be present in such a system. For example, consider a teacher who lives in a state or district that has banned any training that may cover diversity, equity, or inclusion topics, or is related to culturally relevant pedagogy. If a teacher takes that course to meet the needs of their students, what risks may be present to them or their school/district if their PD completion data were somehow accessed and shared?

It has been recommended that organizations develop strategies that go beyond the "logic of privacy self-management that has been embedded in privacy law in the United States and Europe for decades" [2, p.930]. To ascertain what these strategies may be for educators, our research question for this study was: *Among teachers, what features or practices are associated with trusting in software that contains professional personally identifiable information (PII)?*

2 Methodology

We employed an exploratory mixed methods study [1] to determine what enhances trust in software that collects and stores PII. Based on our review of the very limited extant literature, we first developed an interview protocol and we determined sampling requirements to guide participant selection. We also obtained Institutional Review Board approval for the broader project, after which CSTA invited all teacher members to take part in the study. Virtual interviews with teachers ($n = 17$) lasted approximately 20 minutes each and were then transcribed and cleaned for accuracy. We then deductively coded the transcripts based on the answers to each question, using themes and categories to identify key patterns.

Building on the qualitative results, we created a survey instrument to capture a broader set of teacher perspectives and a program evaluation survey containing related items. CSTA again invited all teacher members to participate in both in June 2025. The first survey ($n = 495$) represented a wide spectrum of respondents, with 21% instructing grade PreK-5, 26% grade 6-8, and 45% grades 9-12. 21% were from rural communities and 68% were from Title I schools. In the program evaluation survey ($n = 494$), there was also variation in respondent characteristics with 25% instructing grade K-5, 22% grade 6-8, and 41% grades 9-12. 70% of the program evaluation survey respondents self-identified as White and 63% as female. Quantitative data were subsequently cleaned and analyzed. Finally, findings from the qualitative and quantitative phases were integrated to inform the overall study report and a set of recommendations were provided to CSTA team members for integration into the platform.

3 Findings

Supporting the claim that teachers' perspectives on privacy and security of their data is important, over 98% of Survey 1 respondents indicated that a data privacy breach would impact their relationship with the platform or organization, and 42% said that their overall trust in the organization would decrease. 24% said they would stop using the software/service if an alternative exists.

SIGCSE TS 2026, St. Louis, MO, USA

ACM ISBN 979-8-4007-2255-4/2026/02
https://doi.org/10.1145/3770761.3777212

Table 1: Descriptive Statistics of Security and Usability Items

Abbreviated Item	n	Mean	SD
Transparency about who has data access	379	6.59	0.79
Strict access controls (limiting data access)	384	6.49	0.91
Explicit consent required before my information is published or shared	379	6.44	0.99
Offers capability to control who data is shared with	379	6.43	1.00
Consistent, bug-free performance (e.g., no glitches, data tracks correctly)	375	6.43	0.90
Offers capability to control data sharing	379	6.38	1.05
Reliable login process	375	6.28	1.03
Absence of excessive advertising or spam	375	6.26	1.22
Multi-Factor Authentication (MFA) / Two-Step Verification (e.g., text/email codes)	384	6.20	1.11
Responsive and easy-to-access customer support (e.g., quick email/chat replies)	376	6.20	1.14
Offers capability to manage/change password securely	384	6.13	1.16
Intuitive (easy to navigate, easy to find information)	374	6.11	1.05
Stable user interface	375	6.11	1.07
Clear explanations for why information is requested	379	6.09	1.22

Further, we asked participants to rate a set of items related to privacy and security for general software/websites using a 7-point Likert scale (1 = strongly agree and 7 = strongly disagree) and 14 items rated above 6 (see Table 1). Overall, participants want to know who has access to their data, want strict access controls along with explicit consent before publishing or sharing their data, and want controls over who has access to and what data can be shared. They also want multi-factor authentication for their accounts and clear explanations of why information is requested in the platform.

In our program evaluation survey, we asked respondents if they knew where to access the platform's data privacy and sharing policies. Nearly 41% ($n = 52$) reported being unable to locate those policies. We also asked respondents about which platform features would be most important in their decisions to use the passport in the future (Table 2). Respondents rated features on a Likert scale (Not at All Important (0), Somewhat Important (1), Very Important (2), Critically Important (3)). Participants rated control over sharing personal information, the passport's data security and policy policies, and user-friendly exporting of passport data as the most important features influencing their decisions to use the passport.

4 Recommendations

Based on the results, our recommendations for the CSTA team related to data privacy and security are:

- Add multi-factor authentication.
- Clearly state which organizations have access to user data and whether it is shared or sold externally.
- Provide clear explanations for why each piece of information is requested (e.g., via tooltips).

Table 2: Descriptive Statistics of CS PD Passport Features

Abbreviated Item	n	Mean	SD
The Passport allows me to select what personal information is shared from the platform and who it is shared with	438	2.10	0.72
The Passport allows me to export my CS PD participation records in a user-friendly format	441	2.20	0.71
The Passport's data security and privacy policies are easy to locate	318	1.80	0.97
The Passport can track and verify participation in CS PD not hosted by CSTA	439	1.80	0.73
The CS PD Passport integrates Multi-factor authentication for access	439	1.80	0.72
The Passport allows me to affiliate my records with multiple email addresses	439	1.80	0.72

- Offer training for users on how to protect student and teacher data.
- Prepare a plan (easily accessible on the platform) for data breaches and conduct an annual data audit.
- Do not use user data in AI models without explicit consent.
- Obtain data sharing agreements with NSF PD providers to ensure secure and compliant data handling.

For user experience/platform features, our recommendations are:

- Have a UI expert conduct user interviews to assess perceptions and improve platform look and feel.
- Implement features allowing users to export their CS PD participation records in user-friendly formats (.pdf, .csv).
- Create multi-modal FAQ resources covering topics like record verification, navigation, term definitions, and error reporting, and link privacy and data security policies prominently within the platform.

For evaluation and continuous improvement, we recommend:

- Create a crosswalk of platform features with research and evaluation findings to guide ongoing development.
- Notify users proactively about platform changes (UI or data policies) before and after updates.

Acknowledgments

This material is based upon work supported by the U.S. National Science Foundation under Grant No. 2327863. This work has been performed in partnership with the Computer Science Teachers Association. We thank Jennifer Manly and Jake Baskin for their support of this effort.

References

[1] John W. Creswell and Vicki L. Plano Clark. 2018. *Designing and conducting mixed methods research.* Sage Publications, Los Angeles.

[2] Sara Vannini, Ricardo Gomez, and Bryce Clayton Newell. 2020. "Mind the five": Guidelines for data privacy and security in humanitarian work with undocumented migrants and other vulnerable populations. *Journal of the Association for Information Science and Technology* 71, 8 (Aug. 2020), 927–938. doi:10.1002/asi.24317