SPOTLIGHT: Placer Union High School District Develops Data-Driven Digital Privacy Plans

Placer Union High School District (PUHSD) is a community of high schools nestled in the Northern California Sierra Foothills. PUHSD's mission is to drive student learning through teaching excellence in a supportive environment. Educators across the district are highly committed to using technology to support classroom instruction. This includes providing the most beneficial technology programs, reliable networks and devices, and highly-trained instructors. In fact, since 2016 over sixty faculty members have earned Google Educator certification.

District-wide technology integration has proven very successful for student learning, but educators realized that with increased technology adoption, digital privacy and security needs increased as well. Although the district had developed some digital citizenship programing, there was little movement in other areas of digital privacy. Recognizing both the legal and ethical responsibility to keep staff and students safe, PUHSD looked to the Digital Privacy, Safety & Security module for guidance.

RESULTS

In Spring 2016, a small group of tech staff representing each campus walked through the initial assessment with the assistance of BrightBytes staff. This self-evaluation demonstrated the need for more voices in the conversation and the value of an iterative design-thinking process. The team grew to include board members, faculty, administrators, instructional coaches, library staff, and IT staff. Each of these individuals provided a unique perspective on digital safety needs.

To ensure digital privacy and data security continued as a collective, integrated, and evolving practice, PUHSD linked the theme to its broader tech planning around IT infrastructure and edtech professional development. Steering clear of traditional action planning designs that may have a committee meeting monthly all year-round, PUHSD crafted a three-part, tightly scheduled, "quick win" series of tech think-tanks (The T3) that included focused agendas addressing three goals: Review; Revise; Revitalize.

The first session (Review) was very productive. The privacy team evaluated the results across the module, discussed roles and ownership of potential initiatives, and established a method to set goals and share plans with stakeholders. In sessions two and three (Revise and Revitalize), members pitched ideas in a round-robin format and prioritized key themes to begin articulating action steps. The list of focus areas for privacy and safety included:

- **Student Voice-** Revise and rework the current AUP (acceptable use policy) into an RUP (responsible use policy) that incorporates a student voice

PLACER UNION HIGH SCHOOL DISTRICT, CA

NEEDS

To use research and data to define digital privacy goals

CHALLENGES

Following a successful technology integration, Placer Union High School District leaders realized that their digital privacy plan was in need of attention. Without an established team to lead efforts, the district struggled to obtain insight into the current digital privacy landscape or plan future digital safety efforts.

RATIONALE

The BrightBytes Digital Privacy, Safety & Security module guides the development of critical digital safety policies, procedures, and systems across each organization.
The research-driven module allows districts to use digital privacy data to better inform safety and security needs.

RESULTS

The BrightBytes Digital Privacy, Safety & Security module helped Placer Union High School District leaders:

- Establish a comprehensive digital privacy team to collaborate on safety needs
- Tailor communication about digital privacy to multiple stakeholders
- Develop strategic digital safety goals, action items, and a roadmap for the 2017-18 school year

- **Code Switching-** Help students and staff understand the value of keeping school and personal usage separate
- **Messaging-** Inform students and staff about digital privacy plans in a voice tailored to the audience
- **Digital Citizenship-** Revise digital citizenship instruction and expectations to communicate that it is a life skill that includes awareness, balance, ethical choices
- **Aeries SIS-** Educate staff on individual and broad consequences of data breaches, best practices for browser privacy, password management, and device security

During this trio of meetings, the team was also able to identify their number one priority: to communicate digital privacy and safety awareness to stakeholders sourced from one foundational set of beliefs. The team agreed that tailored communication of these beliefs should follow the sequence of staff first, followed by students and community members. To frame up their work, the group developed a schema to organize goals and objectives. Borrowing language from the Clarity platform, the privacy and security team defined goals in two categories, Quick Wins (easy to implement changes) and Game Changers (long-term large changes), and included "Why this Matters" language for each goal. To ensure that the objective was best communicated, the goal schema also defined the appropriate stakeholder audience.

Placer Union High School District Digital Privacy Goals and Strategies

GOAL: Digital Citizenship	STRATEGY
Repackage digital citizenship skills as regular life skills for staff, students, and community members to educate everyone about risks and promote responsible, productive use of resources. **OBJECTIVE:** Define and promote safe, responsible, and ethical use of data and technology resources among staff, students, and community. **DATA WE HAVE:** • Widespread anecdotal evidence of unsafe password practices among staff and students • Parent concern with student use of Chromebooks at school and at home • Need for an easily accessible, frequently distributed, uniform privacy and safety message **WHY IT MATTERS:** The consequences are significant, at personal, professional, and organizational levels. It can have legal, community, and safety consequences.	Simplify the resource 10 Foundational Principles for Using and Safeguarding Students' Personal Information and share a new version for an outreach campaign: • Create a slide deck with a clear message • Package revised message for dedicated webpage • Develop survey, presentation, and questionnaire **OWNERS:** The Digital Safety & Data Security Team **TIMELINE:** August 2017 **CONNECTION TO LCAP:** 3.2 "Communicate, engage, and collaborate with the community to enhance the wellbeing of our students and staff." **EVALUATION:** Ready for distribution by 2017-18 school year **RESOURCES:** Student Data Principles- www.studentdataprinciples.org

"The Digital Privacy, Safety & Security module has helped us recognize the blind spots where we need to focus our efforts. With the data revealed in the assessment, we can better prioritize our goals, define our objectives, and plan a strategy. At the end of the day, Brightbytes tools and resources build confidence to move forward with the latest industry practices in securing the precious personal data of our families."

GREGG RAMSETH
Technology, Assessment & Data Privacy Liaison
Placer Union High School District
Auburn, CA

GOAL: Messaging for Staff	STRATEGY
Publish new data safety and privacy message to staff. Educate our colleagues on best practices to protect personal, professional, and district information. **OBJECTIVE:** Promote norms of ownership and care regarding student and staff data, including accountability to our community as custodians of sensitive family information. **DATA WE HAVE:** There is a lack of understanding of PII • We see widespread careless practices: password autofill, not locking desktop, logging out, data breaches, etc. **WHY IT MATTERS:** If an account is compromised or subpoenaed, it is important that current and future employee data is kept separate in the appropriate place.	Create a staff presentation on Mentimeter that discusses: • Self-assessment (Online Privacy Personality Profile - Note to Self podcast and weekly email reminders) • New PII and privacy messaging • Log in safety: It doesn't matter, until it does matter. • Data breach protocol: Don't be the leak. • Permission limits: discipline, health care plans, family demographics, etc. **OWNERS:** Site tech coordinators and C&I's **TIMELINE:** Site staff meetings during Fall 2017 **RESOURCES:** Staff meetings, Chromebooks, *US News* article "Officials' Emails on Private Accounts Are Public" **CONNECTION TO LCAP:** 3.2 "Communicate, engage, and collaborate with the community to enhance the wellbeing of our students and staff." 3.6 "Committed to student learning through teaching excellence in a supportive environment."

Empower Educators to Innovate Responsibly with the Digital Privacy, Safety & Security Module!

brightbytes.net/digitalprivacy

With the top priority being communication, the district has now outlined a timeline to share new information to teachers through professional development sessions, students by way of classroom activities, library orientations and pushed content to Chromebooks, and finally parents and community at back-to-school events and 1:1 family orientations.

A work in progress, Placer Union's digital privacy and data security efforts will continue into the fall of 2017-18 as it implements the Review, Revise, Revitalize action plans crafted the previous school year. Come spring of 2018, the teams representing digital privacy, IT infrastructure and edtech support will assess progress and then chart the 2018-19 course. Placer Union intends to meet in the same format: three tech think-tanks over an accelerated six weeks.