Best Practices for Ed Tech Companies

Future of Privacy Forum Data Privacy Bootcamp
February 18, 2015
David Deschryver, Co-Director, Whiteboard Advisors
Chip Slaven, Alliance for Excellent Education, Counsel to the
President and Senior Advocacy Advisor
Amelia Vance, National Association of State Boards of Education, Director of Education Data & Technology
Problematic Trends

- Interpreting Legislation: Words Matter
  - Ambiguous Terms
    - Psychometric
    - Biometric
  - Interpretation Changes
- Accidental Consequences
- Implementation Difficulties
Problematic Trends Cont.

- Opt Out Proposals
- Automatic destruction policies that prevent data from traveling with the student
- Unclear definitions
- Commercial restrictions that go too far and limit necessary research to improve products
- Lack of Privacy Training
  - Poor professional training for teachers and staff
  - No or poor breach prevention and response plans
  - No designated chief privacy officer and/or state and district privacy expert

www.all4ed.org
www.nasbe.org
http://www.whiteboardadvisors.com/
What we advise policymakers to do:

- Review Your Resources
- Identify and Seek Input from Stakeholders
- Questions To Ask
- Best Practices
Start With Questions: What Data Do We Want Collected, and Why?

- Education data should only be collected for articulated purposes
- What is education data?
- What questions do you want answered?
- When the information needed to answer the question is sensitive, you must balance privacy with educational innovation

www.all4ed.org
www.nasbe.org
http://www.whiteboardadvisors.com/
Fundamental Questions to Consider in Crafting Privacy Policies

- What sensitive information do I want teachers, principals, and other educational officials (such as school counselors) in my state to know about children in their classroom?
- Of that information, which individual student information, if any, should be accessible to the district or the state education departments?
- How can information help parents?
Fundamental Questions, cont.

- What sensitive information, in the aggregate, do I want to share with the state education department?
- What sensitive information do I not want stored in a child’s school record?
- What restrictions, if any, do I want to place on how information is shared more broadly?
- When should a student record be deleted?
Foundational Elements of a State Data Privacy and Security Policy

1. Statement of the policy/law's purposes
2. Select the person(s) in charge
3. Encourage Transparency
4. Have Prevention and breach plans
5. Limiting Vendor Use of Data
6. Statewide data security plan
7. Ongoing Staff Training
Best Practices

- Make language simple
- Provide short explanation videos
- Explain what is being collected and why
- Do an inventory
- Be helpful to schools and policymakers
- Be very transparent!

www.all4ed.org
www.nasbe.org
http://www.whiteboardadvisors.com/
Best Practices (con’t)

- Put on an Orwellian mindset before framing your product
- Privacy by design, for both your product and your staff
- Have an emergency response plan in case you have a breach
- Handout being sent out after session

www.all4ed.org
www.nasbe.org
http://www.whiteboardadvisors.com/
Move the Debate

From here:

“I don’t want schools to collect data on my daughter.”

To here:

“I want my daughter’s school to collect learning information on her so I know she is on a path to success.”

www.all4ed.org
www.nasbe.org
http://www.whiteboardadvisors.com/
Questions?

David Deschryver
Co-Director, Whiteboard Advisors
David@whiteboardadvisors.com

Chip Slaven
Counsel to the President and Senior Advocacy Advisor, Alliance for Excellent Education
cslaven@all4ed.org

Amelia Vance
Director of Education Data & Technology, NASBE
AmeliaV@nasbe.org
@ameliaivance