Data Security and International Travel: What K–12 Schools and Trip Chaperones Need to Know

Insights
4.29.25

As global learning experiences become more common in K–12 education, schools increasingly send staff and students abroad for cultural exchanges, academic competitions, service trips, and more. While these trips offer incredible educational value, they can also expose school staff – especially trip leaders and chaperones – to serious digital and data security risks. If your school staff or chaperones carry laptops, tablets, or mobile devices with student records, staff contact lists, donor databases, proprietary curriculum, or other sensitive information, international travel can create opportunities for unauthorized access, cyber theft, and even legal violations. Understanding these risks is key to protecting your school community and staying compliant with privacy regulations like FERPA.

Border Inspections: What Chaperones Should Expect

When traveling internationally, particularly upon entering or reentering countries like the United States, border agents have broad authority to inspect electronic devices – even without suspicion or a warrant. This applies not only to foreign nationals but also to US citizens and lawful permanent residents. (You can read more about how this could impact the workplace here.)

For example, a school chaperone returning from a trip to Europe with a school-issued laptop could be asked to unlock their device, provide passwords, or even have the data copied for further review. If that device contains student data, donor records, emails, or confidential school documents, it could inadvertently expose your institution to privacy or data security concerns.

Surveillance and Cyber Risks While Abroad

Once overseas, chaperones and staff may also face surveillance and cybersecurity threats, particularly in countries where digital monitoring is widespread. Common risks include:

- **Public Wi-Fi interception:** Using hotel, airport, or café networks can allow bad actors to monitor internet activity or steal information, including sensitive donor communications or fundraising details.
- **Malware and phishing threats:** Devices connected to unknown networks may be more vulnerable to malicious downloads or fake login pages.

- **Restricted encryption laws:** Some countries restrict or ban the use of encryption tools, making it harder to keep data secure.

Ethical and Legal Duties of School Staff

Educators, administrators, and school IT personnel have a legal and ethical responsibility to protect confidential student and staff information. Any third-party access to a chaperone's device could trigger mandatory reporting requirements under student privacy laws. It is important to prepare staff before travel so they understand what is at stake.

Smart Security Steps for Chaperones and School Staff

To help keep data safe during international school trips, consider implementing the following precautions:

- **Limit digital exposure:** Only bring essential devices and remove non-essential data.
- **Use school-approved cloud storage:** Avoid storing sensitive files directly on devices.
- **Use loaner devices when possible:** Clean, pre-configured devices reduce risk.
- **Avoid unsecured public Wi-Fi:** Use school-issued VPNs or virtual desktops (if allowed).
- **Update software:** Ensure devices have the latest security patches installed.
- **Use strong passwords:** Require chaperones to disable biometrics before crossing borders and use strong passwords instead.
- **Back up everything before travel.**
- **Train chaperones:** Develop data handling policies for international trips and train chaperones on best practices.
- **Notify IT support and compliance staff of travel plans:** This helps ensure the right support and risk assessments are in place.

Final Thoughts

International travel can be transformative for students and staff alike, but data security needs to be part of your school's travel preparation. By taking practical steps and building awareness among chaperones and other traveling staff, your district can uphold privacy standards, protect student and donor information, and minimize risk – making sure educational travel stays safe and inspiring.

Conclusion

We will continue to provide updates to assist your school in workplace compliance. Be sure to subscribe to Fisher Phillips' Insight System to keep up with the most up-to-date information. Please contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in

our Education Practice Group or our Data Protection and Cybersecurity Team if you have any questions.

Related People

Angelica M. Ochoa
Partner
303.218.3669
Email

Service Focus

Privacy and Cyber

Global Mobility

Industry Focus

Education

K-12 Institutions