

Avoiding Common Legal Issues at Coding Schools: Data Privacy and Security

April 27, 2017

If you are like most alternative education providers, whether a bootcamp, MOOC, coding academy or some other “nontraditional” model, you likely understand that your organization is to some degree subject to general privacy and data security requirements. But you also likely believe that you simply are not subject to the stringent rules governing the protection of student data and ensuring student privacy rights, and you probably think about privacy and cybersecurity as something to worry about later in your growth cycle.

In one important respect, this is not altogether incorrect. The federal Family Educational Rights and Privacy Act (commonly known as FERPA), the well-known federal law that provides strong protection of “personally identifiable” student data information and gives students certain special privacy rights, only applies to schools that receive federal funds, either directly or through their students receiving federal loans and grants. Since most “alternative education providers” typically do not receive any federal support, either directly or through student aid, they are not directly subject to FERPA.

That doesn’t mean you don’t have to worry about student data privacy. Many other federal and state data security and consumer protection laws still apply.

Data security needs to be a priority, even for startups. These laws apply to both large and small providers – and having limited resources will not usually be a successful argument if things go bad. And, in addition to the legal risks, often the most significant damage to a company from a data breach is reputational. Significant breaches can be a serious blow to otherwise healthy companies, and this risk can be compounded if the response is not handled properly. And increasingly, your partners and customers will want to know just how well you understand and practice good data security.

Organizations that build a strong culture around the importance of data security and privacy at an early stage are best positioned to mitigate the risk and use well-developed policies to competitive advantage. The key is to have the right policies and practices:

- Develop and implement a good privacy policy, but don’t just copy-and-paste. Having a privacy policy you don’t follow is far worse than not having one.
- Implement a comprehensive data security policy that addresses common technical, physical and administrative risks.
- Conduct regular risk assessments to identify weaknesses. Develop a plan for detecting and mitigating risks.
- Develop a data classification system so that you can determine and properly protect the sensitive (such as personally identifiable) data you collect.
- Employ appropriate encryption for both transmitting and storing sensitive data.
- Establish strong password protocols and enforce their consistent use.
- Develop and implement policies on data collection, retention and destruction. Limit access to sensitive data based on legitimate need.
- Remember the importance of physical security (such as “clean desk” policies and limitations on printing sensitive data), especially if you have an open or shared workspace.
- Invest in a Virtual Private Network (VPN) to ensure secure access to sensitive files while employees are on the go. Utilizing public WiFi is often a necessity, but without secure access protection, it exposes your systems to a variety of risks.
- Review and (if necessary and practicable) revise your terms of use and client contracts, particularly with regard to data privacy obligations and potential liabilities.
- Likewise, review and, if necessary, seek to revise your vendor contracts to ensure that you have adequate protections (such as indemnification and insurance provisions) if a subcontractor is the cause of a breach. And include specific obligations to reduce the likelihood of a breach. You should expect your vendors to follow best practices as you do.
- Find out if any of your clients are schools subject to FERPA or other federal or state student privacy requirements that may not apply directly to you, and determine to what extent you also need to comply. As an example, a

- coding academy that has a community college as a client may find itself with FERPA and/or state obligations.
- Secure a professional evaluation of the appropriateness and sufficiency of your insurance coverage.

And, above all, provide frequent training to everyone. Conduct regular training for all employees – not just the IT staff – who have access to data, particularly personal or financial data. Focus on both reducing the risk of a breach and how to respond properly (and promptly) if a breach occurs. Most hacks happen unintentionally by an employee unwittingly offering up a password or clicking on a malicious link. Proper training can significantly reduce that unwanted outcome.

Finally, accept that privacy and data security are facts of life in the 21st Century. Privacy and data security are not one-time boxes to check. Develop a plan, execute it, evaluate it and adjust it as needed.

While taking on privacy and data security may seem daunting – particularly for a new enterprise – understand that you don't have to start from scratch. At Cooley, we have seen what works (and what doesn't) and we have developed policies and procedures that can be easily customized to fit your needs. Ask your questions; we have answers.

Matt Johnson focuses on assisting higher education institutions and education technology companies regarding a variety of regulatory issues including state and federal privacy laws at the K-12 and postsecondary levels.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our [AI Principles](#), may be considered Attorney Advertising and is subject to our [legal notices](#). Copyright © 2026