# FERPA Compliance

The Sail() Platform enables data-driven evidence-based instruction and research. To that end, the Sail() Platform collects profile (name, email), clickstream (navigation), submissions, and score information. The data is critical to enable faculty to monitor student progress, identify when to pursue an intervention, and to reflect on student performance to enhance learning. Also, the data enables the faculty to pursue research questions that are relevant to their context. We aspire for all Sail() Platform instructors to be data-driven instructors and researchers so that we can continue to enhance the effectiveness of our method and platform.

The Sail() Platform enables the faculty to get insight and answer research questions by capturing user logs. The Sail() Platform is hosted on MSFT Azure which provides [FERPA Compliance](https://aka.ms/ferpa-compliance) as outlined in [Microsoft’s compliance offerings](https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-ferpa?view=o365-worldwide).

The Sail() Platform complies with FERPA regulations by fulfilling all 17 requirements of the data security checklist and all applicable requirements of the data governance checklist, provided by the Privacy Technical Assistance Center, established by the U.S. Department of Education.

With its entire microservice-based infrastructure hosted on Microsoft Azure’s virtual resources (and its “Inventory of assets” constantly monitored through Azure Portal), the Sail() Platform delegates not only its “Physical security”, but also its many other security and privacy-related obligations to Microsoft Azure in a [shared responsibility model](https://gallery.technet.microsoft.com/Azure-FERPA-Implementation-441b6b71). Specifically, Azure Security Center (ASC) is responsible for offering “Provide a layered defense”, “Secure configurations”, “Firewalls and intrusion detection/prevention systems”, “Automated vulnerability scanning”, “Patch management”, and “Shut down unnecessary services”, while Azure Active Directory is responsible for “Authentication” and “Access control”. As of February 1, 2020, the Sail() Platform adopts 51 of the 73 [default security policies](https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy) in ASC, which meet the Azure CIS 1.1.0, PCI DSS 3.2.1, ISO 27001, SOC TSP standards out of the box.

The Sail() Platform also adopts the [Acceptable Use Agreements and Policies](https://docs.google.com/document/d/1vgIJ2M9d7GnuEtuPm_CCvLN2k2JddzQ_JD2VuxLLBAk/edit?usp=sharing) provided by the [National Center for Education Statistics](https://nces.ed.gov/pubs2005/tech_suite/app_A.asp#H1) established by the U.S. Department of Education. It covers policies for “Personnel security” and best practices for “Emailing confidential data”.