

# Data Privacy Principles

## WWU Ethics and Compliance Program

Principle	Application
 <p><b>Lawful, Legitimate, Ethical &amp; Responsible</b></p>	<p>Personal data is collected, used, disclosed, and destroyed in a lawful, ethical, and responsible manner and only for legitimate business purposes. Responsible use includes, but not limited to, using it in a non-discriminatory manner.</p>
 <p><b>Defined Purpose</b></p>	<p>The business need for personal data is narrowly tailored and determined prior to collection. Subsequent use is consistent with the original purpose unless consent is received or is reasonably necessary, compatible with the original purpose, and permitted or required by law.</p>
 <p><b>Minimization of Data</b></p>	<p>Only the minimum amount of data necessary to meet the determined purpose is collected. Disclosures are limited to what is requested or legally required or permitted. Retention is limited to legal requirements or period necessary to achieve original purpose if longer than legal requirement.</p>
 <p><b>Transparency</b></p>	<p>What personal data is collected, for what purposes, and with whom it may be shared is transparent including being subject to public records requests. Individuals may request to understand which of their personal data the University maintains.</p>
 <p><b>Individual Participation</b></p>	<p><sup>a</sup> Involve people in the collection and management of their personal information when appropriate or required by law. Participation may include accessible processes to provide or revoke consent, opt-out of collection or data, or obtain copies of or correct their records.</p>
 <p><b>Security &amp; Integrity</b></p>	<p>Reasonable cybersecurity and administrative controls are implemented and maintained based on the amount and type of data, risk, technology and ensure accuracy when collected, processed, retained, disclosed, and destroyed.</p>
 <p><b>Third Party Due Diligence</b></p>	<p>Taking reasonable steps and exercising care before and after entering into and while maintaining an agreement with a third party that includes sharing personal information to ensure adequate protection of personal data.</p>
 <p><b>Accountability</b></p>	<p>Effective oversight is maintained through appropriate governance and activities such as privacy impact assessments, implementing best practices for continuous improvement, and responding to and addressing reported concerns and issues.</p>