



Ohio Administrative Code

Rule 3337-92-01 Privacy Protection Policy.

Effective: August 23, 2024

(A) Overview

Ohio university ("we" / "us" / "our") requires compliance with the privacy standards set forth in all applicable laws and regulations.

(B) Philosophy

Ohio university is committed to protecting the personal data of faculty, staff, applicants, students, alumni, donors, research participants, patients, community members, and other individuals whose data we manage. By recognizing the right to privacy in all aspects of our operations, we cultivate a culture of transparency and accountability, which are essential values for sustaining the trust of our academic community.

(C) Definitions

(1) Anonymization - the process in which elements of individually identifiable data are removed in such a way that the data no longer can be traced back to a given data subject.

(2) Confidentiality - preserving authorized restrictions to access or disclosure of information for protecting privacy and proprietary information.

(3) Transparency - except when prohibited by law and to the best of our knowledge, we are committed to being open and clear about our collection, use disclosure, and maintenance of consents, and other similar information as appropriate.

(4) Purpose specification and use limitation - personal data must only be collected, used, stored, and disclosed for specific law purposes such as:



- (a) To carry out legitimate business and operational purposes of the university
- (b) To comply with legal obligations
- (c) To protect the public interest
- (d) For research purposes
- (e) For archival purposes

Verifiable individual consent, where required by law, shall be obtained prior to collection of such data.

When processing personal data for specific purpose, state, federal, and institutionally required safeguards shall be applied to protect the privacy of data subjects.

(5) Data minimization and anonymization - data minimization must be prioritized by collecting only the necessary amount of personal data to accomplish a specified purpose(s), such as those listed in paragraph (E)(3) of this policy.

To promote efficiency and minimize unnecessary data in a manner that aligns with the principles outlined in this policy. Whenever possible, personal data must be anonymized, pseudonymized, masked, or otherwise modified to effectively reduce the risk to data subjects.

(6) Data quality - To the extent required by law, reasonable steps shall be taken to optimize the accuracy of data addressed in this policy, including providing data subjects (ex. students) with the opportunity to review and correct their information.

(7) Disclosure limitation - Personal data must only be accessed and disclosed in a manner that represents the minimum necessary to complete the specified purpose.

(8) Security - Personal data must be collected, used, stored, and transmitted in a secure manner and consistent with applicable privacy and data security laws and regulations. This means that steps must



be taken to protect personal data from unauthorized access, unlawful use, and accidental loss. For more information on data protection, please see the office of information technology (OIT) protect university data website, which is listed in the references section of this policy.

(9) Retention limitation - Personal data must only be retained for as long as it is necessary for the purpose for which it was collected and to comply with university retention policies, guidance, or legal requirements. Personal data may be kept for longer periods for archiving, research, statistical purposes, or as permitted by law.

(10) Accountability - We are responsible for how personal data is collected, used, stored, and disclosed. We must commit to having appropriate safeguards and records (ex. training and OIT vetted vendors) in place to demonstrate our compliance with the other principles of privacy protection.

(D) Questions

For questions about this policy or privacy in general, please contact the chief privacy officer within the office of audit, risk, and compliance at privacy@ohio.edu.

(E) Reporting violations of this policy

Reports of privacy concerns or problems are taken seriously at Ohio university. While initial reporting through standard channels, including department leadership, is strongly encouraged, violations of this policy may be reported in good faith using Ohio university's hotline, eithicspoint, which is operated by a third party. Reports may be submitted anonymously.

Violations of this policy will be addressed through the appropriate university disciplinary process based on an individual's classification. Disciplinary action may vary, up to and including termination of employment.