Effective Date: July 1, 2021
Last Reviewed: July 1, 2021
Next Review: July 1, 2022

Privacy Policy

1. Purpose and Scope

Bentley University is committed to ensuring that the privacy of its students, faculty, and staff, alumin, parents and friends is respected. That commitment requires protecting the privacy of Prohibited, Restricted and Confidential Information within its control in a manner consistent with applicable laws, regulations, University policies and best practices.

2. Authority

Reviewed and approved by the Data Privacy Committee.

3. Applicability

This policy is applicable to all members of the Bentley community and visitors to the University, including but not limited to students, faculty, lecturers/instructors, staff, third-party vendors, and others with access to Bentley's campus and University Prohibited, Restricted and Confidential Information.

4. Definitions

a. **Disclosure:** "Disclosure" is the release of, transfer of, provision of access to, or other communication of Information outside of the Bentley community or within the Bentley community.

b. **Use:** "Use" is the examination, sharing, or other utilization of Information within the Bentley community.

c. **Information:** "Information" is all Bentley University Prohibited, Restricted and Confidential information, whether in electronic or paper format, as defined in Bentley's Data Classification Policy

d. **Guidelines:** "Guidelines" refer to the Information Security policy and Acceptable Use Policy.

5. Information Privacy

a. **General Policy**

Bentley must limit the collection, use, disclosure or storage of Information to that which reasonably serves the University's academic, research, or administrative functions, or other legally required purposes. Such collection, use, disclosure, storage, and retention must also comply with applicable Federal and state laws and regulations, and University policies.

b. **Legal and University Process**

Notwithstanding the General Policy contained in section 5.a, the University may disclose Information in the course of investigations and lawsuits, in response to subpoenas, for the proper functioning of the University, to protect the safety and well-being of individuals or the community, and as permitted by law.

c. **Policies That Apply to Special Categories of Information**

Bentley has adopted policies governing certain categories of Information. These policies are listed in this section, 5.c. To the extent that there is a conflict between this policy and any of these special policies, the special policy will control. For more information about Bentley's compliance with any of the laws and policies referenced below, please contact the cyber security & privacy team at infoprivacy@bentley.edu or the individual listed in section 7.a as responsible for compliance.

1. Prohibited Information, including Social Security Number ("SSN") and Driver's License Number ("DLN")

Bentley must not use an individual's SSN or DLN as a personal identifier unless required by law or approved by General Counsel or the Data Privacy Committee. Prohibited information, including SSNs and DLNs, may be stored electronically only in compliance with the Guidelines. If Prohibited Information must be stored on paper, the files must be stored securely with access provided only to authorized persons.

2. **Student Records**
   Students have rights with respect to access to their education records under the Family Educational Rights and Privacy Act of 1974 ("FERPA"). These rights are outlined in the Bentley FERPA Policy

3. **Health Information**
   Individuals have rights with respect to the privacy and security of their health information under Federal and state laws and regulations. The rights for faculty and staff are outlined in the University's health information privacy policy. The rights for student health information are protected under the FERPA guidelines.

4. **Human Subjects Research Information**
   In addition to the rights afforded by HIPAA and other laws related to health information, the Institutional Review Board outlines provisions specific to the privacy of research participants and the confidentiality of their information. Research compliance is maintained by the Institutional Review Board, which is responsible for the University policies related specifically to human subjects' research information.

5. **Financial Services Records**
   The Gramm-Leach Bliley Act requires that Bentley protect the privacy and security of information collected in the course of providing certain financial services, such as student financial aid. Bentley has adopted polices to protect this information. These protections are outlined in the Bentley GLBA Policy

d. Confidentiality Obligation

Members of the Bentely community are subject to the Confidentiality and Privacy provisions set forth in Section VI of the Code of Ethics for Faculty and Staff. As a reminder of Bentley's commitment to privacy, students, faculty, staff and other members of the workforce may be asked to sign a confidentiality statement based on the Code of Ethics and this privacy policy. Failure to sign such a statement in no way diminishes the obligation to uphold Bentley's policies.

e. Training

Departments within Bentley University are responsible for ensuring that all members of their workforce (including, among others, faculty, staff, students, consultants and volunteers) receive appropriate training on Bentley's privacy and security policies to the extent necessary and appropriate for them to carry out their required job functions. Departments will maintain adequate records of workforce training, which will be provided upon request by the Office of the General Counsel, Information Security Officer, Human Resources or other University official with a reasonable Bentley-related need for the information.

6. Expectation of Privacy

a. General Policy

Bentley respects and values the privacy of its faculty, students and staff and will not infringe on that expectationwithout cause, as required by law or as permitted by the policies and agreement referenced below:

1. **Computer and Network Usage.** Acceptable Use Policy. See section Access and Privacy. While we allow employees to use their computers for reasonable personal of use, all systems and the information on those systems belongs to Bentley. Generally, Bentley will not access an employee's email or computer without a

legitimate reason and only where there has been approval by two Vice Presidents. The only exception to this occurs when information is subpoenaed by a court or government agency pursuant to a confidential investigation.

2. **University Student Housing.** See Bentley's Housing Contract & Addendum circumstances in which student residences may be accessed.

b. Visitors on Campus

The University is private property; however, some areas of the campus typically are open to visitors. These areas include the conference center, library, public eating areas, retail establishments, outdoor and indoor guided touring areas, roads, walkways, designated parking areas and locations to which the public has been invited by advertised notice (such as for public educational, cultural, or athletic events). Even in these locations, visitors must not interfere with the privacy of students, faculty, lecturers/instructors, and staff, or with educational, research, and residential activities. The University may revoke at any time permission to be present in these, or any other areas. Visitors should not be inside academic or residential areas unless they have been invited for appropriate business or social purposes by the responsible student, faculty member, lecturer/instructor, or staff member.

7. Responsibilities

a. University Privacy Committee

1. Interpreting this Policy;
2. Providing advice with a view to encouraging compliance with all privacy laws and regulations, improving privacy practices, and resolving problems;
3. Establishing privacy policies and procedures in areas not covered by section 5.c above.
4. Recommending privacy policy and policy changes in all areas related to privacy at Bentley;
5. Facilitating special privacy-related situations.

b. Establishing Privacy Policies and Procedures

The University has designated certain officials with primary responsibility for establishing policies and procedures governing University compliance with certain specific privacy laws and regulations:

1. **FERPA.** The University Registrar has primary responsibility for establishing policies and procedures related to compliance with the Family Educational Rights and Privacy Act.
2. **GLBA.** VP Enrollement Management and ISO has responsibility for establishing policies and procedures related to compliance with the Gramm-Leach-Bliley Act.

c. Information Custodians and System Owners

Each individual who retains custody of Information, and each system owner, is responsible for the application of this policy and all related University policies to the systems and Information under their care or control.

8. Violations of this Policy

a. Failure to follow proper policies and procedures concerning access, storage and transmission of Information may result in sanctions and disciplinary action up to and including termination of employment, referral to the applicable administrative process.

b. Members of the Bentely community who believe that these policies have been violated should report such violations to This committee, Office of the General Counsel, and CIO and in the case of students the VP of Student Affairs. Complaints or concerns may also be reported anonymously by calling at (866) 384-4277 or reporting it online at bentleyuniversity.ethicspoint.com.

c. Any Department found to have violated this policy may be held accountable for the financial penalties and remediation costs that are a direct result of this failure.

9. Relevant Laws

a. MGL c.93H: Security breaches
b. MGL c.149, § 52C: Personnel records: inspection by employee
c. The Family Educational Rights and Privacy Act of 1974 (FERPA) (also known as the Buckley Amendment) 20 U.S.C. § 1232g; 34 C.F.R. § 99.1 et seq.
d. The Gramm-Leach-Bliley Act 15 U.S.C. § 6801 et seq., 16 CFR § 313.1 et seq.(privacy)16 CFR § 314.1 et seq. (safeguarding)
e. 201 CMR 17: Standards for the protection of personal information of residents of the Commonwealth
f. 940 CMR 27.00: Safeguard of personal information

10. Related Documentation

a. Faculty & Staff: Code of Ethics for Faculty and Staff
b. Student: Student Handbook
c. Technology: IT & Security Policies

11. Revisions

Version	Date	Author	Reviewers	Approvers	Notes
1.0	-	Michael Gioia	-	-	Original document
1.5	5/13/ 2021		Judy Malone – General Counsel Michael Gioia (ISO)	Data Privacy Committee	Made multiple revisions to finalization