

Bentley University Record Retention and Destruction Policy

- 1. Overview and Purpose**
- 2. Scope**
- 3. Policy**
- 4. Record and Document Destruction**
- 5. Suspension of Record and Document Destruction Schedule**
- 6. Enforcement**
- 7. Policy Support Contact**
- 8. Related Documentation**

1.0 Overview and Purpose

The purpose of this policy is to ensure that necessary records and documents of Bentley University are adequately protected and maintained and that records which are no longer needed for university purposes are discarded at the appropriate time. This policy is also to aid employees of Bentley University in understanding their obligations in retaining and destroying either physical (paper) or electronic documents.

2.0 Scope

This policy applies to university employees, faculty, staff, contractors, vendors, and other personnel who are responsible for owning and managing university records and documents in either paper or electronic formats.

3.0 Policy

This policy defines the university's record retention and destruction schedule for its records. The Record Retention Schedule (see Appendix A) is approved as the initial maintenance, retention and disposal schedule for the physical (paper) and electronic records of Bentley University. The Data Privacy Committee is responsible for the administration of this policy. University departments are responsible for the implementation of processes and procedures to ensure that the university Record Retention Schedule is implemented within university record and document handling processes. The Data Privacy Committee is also authorized to; make modifications to the Record Retention Schedule as needed to ensure that it complies with state and federal laws; ensure the appropriate categorization of documents and records on behalf of the university; annually review the policy and monitor the university's compliance with this policy. This policy applies to all physical (paper) and electronic records generated in the course of the university's operations, including both original documents and reproductions. University records must be retained and destroyed according to the defined schedule in either paper or electronic formats.

4.0 Record and Document Destruction

In accordance with applicable state and federal laws and the university's [Data Classification Policy](#), any documents containing personal or confidential information should be destroyed so that the information cannot be practically read or reconstructed. For physical (paper) documents, this means that personal or confidential data should be destroyed with a cross-cut shredder. For electronic documents, personal or confidential data should be destroyed with the appropriate software for overwriting electronic data, disk encryption technology or through other means of physical destruction where the information cannot be practically read or reconstructed. For complete details of what is considered personal or confidential data, please refer to the university's Data Classification Policy.

5.0 Suspension of Record and Document Destruction Schedule

In the event the university is served with a subpoena or request for documents or any employee becomes aware of a governmental investigation or audit concerning the university or the commencement of any litigation against or concerning Bentley University, such employee shall inform General Counsel and any further disposal of documents shall be suspended until such time as General Counsel determines otherwise. General Counsel shall take such steps as is necessary to promptly inform appropriate staff of any suspension in the further disposal of documents. Upon notice from General Counsel, the email data of the individual(s) in question will be made available for legal holds. Once the litigation is terminated or settled, General Counsel will notify the appropriate individuals so that backups tapes can be put back into general rotation, archiving can be turned back on and copies of email data stored for the legal hold can be deleted.

6.0 Enforcement

As described in the university's [Acceptable Use Policy](#) anyone found to have violated this policy may be subject to disciplinary action, up to and including immediate termination.

7.0 Policy Support Contact

General Counsel

Chief Information Security Officer (CISO)

8.0 Related Documentation

[Acceptable Use Policy](#)

[Data Classification Policy](#)

[Appendix A - Record Retention Schedule](#)