Email Policy

1. **Overview and Purpose**
2. **Scope**
3. **Email Data Ownership**
4. **Email Data Confidentiality**
5. **Inappropriate Uses of Email**
6. **Email Data Retention**
7. **Distribution Lists**
8. **Email Storage Quotas**
9. **Email Account Termination**
10. **Exceptions**
11. **Enforcement**
12. **Policy Support Contact**
13. **Approval and Revisions**
14. **Supporting Documentation**

1.0 Overview and Purpose

Bentley University provides electronic mail services to the campus community, at the university's expense, in support of academic and administrative pursuits. This policy applies to electronic mail sent, received or stored through the university’s email system or on University or personal devices (e.g. cellphones).

2.0 Scope

This policy applies to Bentley University employees, faculty, staff, students, contractors, vendors, and other personnel who are granted privileges to the Bentley University network and its computing systems.

3.0 Email Data Ownership

Electronic mail created or distributed by university resources is considered sole property of the university, regardless of content. Employees and students should be aware that email sent and received using the university's email

resources cannot be considered confidential or private. The university upon reasonable grounds may access email data at any time, and without prior notice. Access to an employee's or student's email data will require the approval from –General Counsel Office and the divisional Vice President responsible for the employee or student. The university will not read or make available the contents of any individual's electronic mail unless there are reasonable grounds to do so. Reasonable grounds for doing so may include but are not limited to the following.

- Ensuring system integrity (such as tracking viruses or corrupt messages) ;
- Complying with legal obligations (such as subpoenas);
- Maintaining the continuity of business operations (such as when employees are terminated or leave the university);
- Investigating complaints of possible violation of university policy;
- Resolving disputes or grievances between individuals at the university;
- Performing certain system-management functions (troubleshooting reported problems such as corrupted or compromised accounts);
- Conducting judicial review cases;
- Continuing business after a person is terminated from their position or leaves the university;

4.0 Email Data Security

O365 provides data security via encryption for emails within the university but cannot guarantee encryption of email data that is sent or forwarded from a university account to an external email account.

5.0 Inappropriate Use of Email

No person may use the university's electronic mail system to send harassing or threatening message(s), or a message that would be considered offensive. Individuals who engage in such behavior may be subject to disciplinary action. If a complaint of a harassing email message is received, the university reserves the right to fully investigate the matter by reviewing the logs and message data of both recipient and sender. The university may also pursue disciplinary actions including, but not limited to, termination or

expulsion. Prohibited uses of email may include but are not limited to the following.

- Employees may not send or forward level 1 data in email. Please see the university's Data Classification Policy for full details.
- Soliciting for fundraising, political, religious or business ventures not directly affiliated with official university activities
- Transmitting information that is false, derogatory, profane or sexually explicit manner
- Using email to publicly convey what would reasonably be interpreted as personal information regarding another employee or student.
- Sending harassing materials (i.e., threats or offensive remarks about race, ethnicity or sexual orientation)
- Attempting to disguise the identification or origin of the email
- Including copyrighted or trademarked materials without authorization from the person or business holding the copyright or trademark, with the exception of fair use.
- Sending email that contains malware, viruses or Trojan horses
- Using another user's email password and address
- Sending unwanted, uninvited spam or phishing emails to others inside or outside the university regardless of the origin of that email.

6.0 Email Data Retention

The University maintains limited backup copies of all email data. Please be aware that deleting email messages from a folder will remain in your deleted items for 30 days and then deleted permanently. The university is under no obligation to provide students or employees with archived copies of their email data upon graduation or termination of the relationship with the university.

7.0 Distribution Lists

Email distribution lists are considered sole property of the university. They may be furnished to an external third party only in conjunction with a legitimate academic or administrative purpose, approved in writing by the divisional Vice President. In such cases, contractual arrangements with any party wishing to use university distribution lists must include language that

prevents that party from furnishing, duplicating or selling the distribution list to another party.

- University distribution lists cannot be used for individual gain or to express unsolicited personal views and opinions;
- Creating and using self-constructed distribution lists comprised of faculty, staff and student email addresses for purposes of surveys, marketing a product, establishing or maintaining a service or conveying a grievance is strictly prohibited;
- Faculty and staff must exercise caution in using email distribution lists to conduct internal surveys, as most recipients find unsolicited surveys tantamount to spam;
- Employee use of distribution lists for surveying is allowed only for legitimate academic or administrative purpose and only when approved by the appropriate divisional Vice President;
- Student organizations and their members who wish to use university owned distribution lists must seek prior approval from the Office of Student Activities in order to use defined lists for surveys and announcements;

8.0 Email Storage Quotas

While O365 provides 100 Gb of storage, the university reserves the right to implement email storage quotas for both employee and student email accounts. Individuals are responsible for regularly deleting email that is no longer needed for university purposes.

9.0 Email Account Termination

Upon separation from the university, all staff email accounts will be terminated. Emeritus faculty and students who graduate from the University have the option of retaining an email account. In cases where there is an immediate need to terminate the access, the university will alert the appropriate support groups to immediately disable access to university systems for the affected account.

10.0 Exceptions

Any exceptions to this policy are to be reviewed and approved by the General Counsel and Chief Human Resource Officer.

11.0 Enforcement

As described in Bentley University's Acceptable Use Policy, anyone found to have violated this policy may be subject to disciplinary action, up to and including immediate termination or expulsion.

12.0 Policy Support Contact

- Information Security Officer
- Infosec@bentley.edu

13.0 Approval and Revisions

This policy is approved by the Information Privacy Committee. The policy is reviewed on an annual basis and updated as needed.

- Revision v1: Approved by the Information Privacy Committee on 8/8/2010
- Revision v2: Approved by the Information Privacy Committee on 9/30/2013
- Revision v3: Approved by General Counsel and CIO.

14.0 Supporting Documentation

This policy is supported by the following policies, procedures, and/or guidelines;

- Acceptable Use Policy
- Data Classification Policy