Policy Name: Acceptable Use of Electronic Information Resources
Approving Authority: Academic Council

Policy # AA-003
Approval Date: 5/28/2024
Date Last Reviewed: 6/26/2023
Next Review Date: 5/2029

**Statement**

The Acceptable Use of Electronic Information Resources Policy of Beal University Canada ("BUC" or the "University") requires all members of the University to use electronic information resources appropriately while respecting the privacy, rights, and property of others. The Academic Council will review this policy every five (5) years.

**Purpose**

The purpose of the Acceptable Use of Electronic Information Resources Policy, in conjunction with other applicable policies, is to:

- set forth the acceptable use of all electronic information resources in custody or under the control of the University; and
- describe the rights and responsibilities of the University and the University members with respect to the use of these resources.

**Roles and Responsibilities**

This policy applies to all University members, including students, staff, and faculty. The Chief Privacy Officer has implementation responsibility for this policy. The Academic Council has oversight.

**Policy**

The University provides electronic information resources to University members primarily to serve the educational, research, and administrative purposes of the University.

Appropriate use of electronic information resources is governed by the following principles:

1. Each user of electronic information resources bears primary responsibility for their use of these services and for the information they transmit, receive, or store through use of these services.
2. Users are expected to respect the rights and property of others, including privacy, confidentiality, and intellectual property.
3. Users shall comply with all applicable laws, regulations, and contracts and behave in a manner consistent with the University's policies and mission.
4. Incidental use of electronic information resources for personal use is acceptable but is limited to responsible activities that minimize disruption to University business while attending to necessary personal affairs. The University is not responsible for any personal data stored on University electronic information resources.
5. Electronic information resources as a result of incidental personal use ("personal data"):
    a. While the University takes reasonable measures to back up information and protect it from loss, the University cannot guarantee that personal data will be retained in University information systems or remain confidential. To protect their personal data from inadvertent access, disclosure or destruction,

users are encouraged to store it separately from University information systems and back it up on a regular basis. Where users intermingle personal data with BUC electronic information resources, they increase the risk that the University will unintentionally access the personal data in the course of accessing BUC electronic information resources for University business purposes.

b. Users should understand that the University routinely monitors network patterns such as source/destination, address/port, flags, packet size, packet rate, and other indicia of traffic on BUC information systems. University system administrators and other technical transmission personnel also perform routine maintenance of BUC information systems. This routine monitoring and maintenance may unintentionally reveal personal data.

c. As part of the University's response to an information security incident, the University may temporarily expand the scope of routine monitoring activities to include computers, servers, and devices connected to the University network to look for the presence of malicious software and indications that unauthorized access to data has occurred or is occurring.

6. Use of electronic information resources for commercial purposes is limited by University policies governing commercial activities sponsored by the University for the purpose of enhancing the University's mission.
7. The connection of privately owned computer equipment to University communications services is permitted. Access to electronic information resources from these computers, or from computers attached to remote networks, is also permitted. All such usage is governed by this policy. Connection of privately owned communications equipment with the intention of extending communications capabilities to other computers or communications equipment requires specific authorization from the Chief Privacy Officer (or designee).
8. An email or other record created using electronic information resources or University information systems may be a University record for the purpose of the Right to Information and Protection of Privacy Act (RTIPPA) and the Personal Information Protection and Electronic Documents Act (PIPEDA).
9. University electronic information resources, such as a University email (e.g., a @bealuniversity.ca email address), are provided to employees in academic and administrative positions for the purposes of conducting University business.
    a. For emails of employees who are terminated, resign, or are on an extended absence, the IT department will:
        i. Deactivate the email account within twenty-four (24) hours of notification from the Human Resources Department.
10. As a condition of access to electronic information resources, a user agrees not to use these resources for inappropriate or unauthorized purposes. Some examples of inappropriate use include but are not limited to:
    - Compromising or attempting to compromise the integrity of any electronic information resources;
    - Using accounts or identification numbers without authorization from the service provider;
    - Revealing, sharing, or showing passwords, access codes, or passphrases for accounts associated with individual users;
    - Sending communications that attempt to hide the identity of the sender or represent the sender as someone else;
    - Seeking, by any means, copies of or information regarding passwords, data, or programs of another user unless explicitly authorized to do so by that user;
    - Sending communications, or using electronic information resources (including email and web pages) that discriminate against or harass, defame, offend, or threaten;
    - Using an electronic information resource for non-University projects;
    - Using an electronic information resource for commercial or other external purposes;

- Attempting to disrupt, degrade, or interfere with the regular operation of any electronic information resource;
- Making or using illegal copies of copyrighted materials or software, storing such copies on electronic information systems, or transmitting them over University networks;
- Displaying or transmitting information that violates laws (e.g., copyright, criminal code, privacy);
- Monitoring electronic information resources without authorization;
- Introducing or propagating any malicious or unwanted software designed to self-replicate, damage, infiltrate, or otherwise hinder the performance of any electronic information resource;
- Initiating mass email transmissions or other electronic mass communications, except as authorized by the University President; or
- Sending mass communications to listservs, forums, discussion boards, social media sites, or other venues (whether provided by the University or third parties) that segments of University members have knowingly joined.

11. Social Media
    - All students and employees using sponsored Beal University Canada social media sites, such as pages on Facebook and Instagram, are expected to conduct themselves in a manner that complies with the terms of the Student Code of Conduct Policy (SA-001) and the Employee Code of Conduct Policy (HR-002). The code of conduct also applies to those students and employees who identify themselves with BUC and/or use their Beal University Canada email address in social media platforms such as professional blogs, LinkedIn, Facebook, etc.
    - While Beal University Canada does not typically provide editorial review of the content of social media sites used by its students and/or employees, Beal University Canada does reserve the right to require students and/or employees to remove content that is deemed to violate the Student Code of Conduct Policy and the Employee Code of Conduct Policy, based on third-party complaints, applicable law or regulation, or computer and network management concerns.

Alleged Violations Process

Upon allegation of a student's violation of this policy, the University will follow the Student Corrective Action Policy (SA-004), under the principles of natural justice, which provides the required steps to be followed, including the complainant's appeal process. Upon allegation of an employee's violation of this policy, the University will follow the Employee Corrective Action Policy (HR-018), under the principles of natural justice.

**Related Policies and Documents**

AA-002 Academic Integrity and Honesty Policy
AA-004 Student Corrective Action Policy
HR-001 Conflict of Interest Policy
HR-002 Employee Code of Conduct Policy
HR-003 Harassment and Discrimination Policy
HR-004 Equity, Diversity, and Inclusion Policy
HR-018 Employee Corrective Action Policy
IT-001 Data Access Policy
RE-001 Ethical Research Policy
SA-001 Student Code of Conduct Policy