Bishop's University Computing Acceptable Use Policy

Approved by the Board of Governors on February 1st, 2019

1. Preamble

1.1 The purpose of this Acceptable Use Policy is to provide guidelines for the appropriate use of Bishop's IT Resources. The University maintains software, services, and systems to provide teaching & learning, research and administrative tasks with technological adjuncts to increase efficiency or expand possibilities. Through adherence to this policy document, Authorized Users will ensure maximum Availability of resources for the University community.

1.2 Scope: This policy covers all members of Bishop's University community: faculty, staff, students and managers who use any aspect of Bishop's Information Technology, Computing Resources and Computer Facilities in the broadest sense; hardware, software, networks, databases, Internet and associated equipment and licenses.

1.3 Bishop's University believes very strongly in the value of users' privacy. Attributes of this Policy which grant access to Data and/or monitoring of computers or other IT resources will be considered the exception, and will only be engaged with appropriate oversight from University Administration or legal responsibilities with regard to storage, protection, and transmission of data.

2. Definitions

For the purposes of this policy:

2.1 Authorized User

An Authorized User is a member of the Bishop's University community who is an employee, student, alumnus, appointee or other individual who has been granted permission, by virtue of the individual's role and responsibilities, to access certain data or systems that are part of Bishop's IT resources.

2.2 Availability

Means the accessibility of Bishop's IT Resources for their intended use.

2.3 Bishop's IT Resources
Refers to all Data, software, hardware, communications systems, storage systems, networks, and devices connected to or making use of the University Network, and being owned and/or managed by the University.

2.4 Confidential
Means that Credentials and/or Data are never revealed to unauthorized individuals or systems.

2.5 Credentials
Credentials refers to the combination of usernames, passwords, PINs and other forms of private information which, when combined, provide access to systems, sites, and services at or hosted-by the University.

2.6 Data
Data means information stored in or transmitted through Bishop's IT Resources, including documents, files, databases, emails, voice, and video.

2.7 Integrity
Integrity refers to the guarantee that data stored-in or transmitted-through Bishop's IT Resources has remained protected and unaltered by unintended means.

2.8 ITS
The Information Technology Services department at Bishop's University.

2.9 Security
Security means the protection of Data and systems from breaches to or of Availability, Confidentiality or Integrity of Bishop's IT Resources.

2.10 System Administrator
An individual responsible for the operation of systems and services offered by ITS to provide the Bishop's IT Resources and ensure their proper, effective delivery.

2.11 University
Refers to Bishop's University including the main and any and all satellite campuses.

2.12 University Email Address
Refers to the email address assigned to the individual (generally having the form flastnameXX@ubishops.ca where f is the first initial of the first name, lastname is the first seven characters of the last name and XX is, in the case of students, the year in which they registered) and not any generic and/or departmental addresses which the user may access as part of their job.

2.13 University Network

Means the wired and wireless network used for Data, voice, and video services operated by ITS.

3. Principles

3.1 Purpose of Use

Bishop's IT Resources exist to support the teaching & learning, research and administrative work of the University. Commercial activities (including but not limited to, selling for personal gain and advertising) are prohibited without express permission of the University. Activities involving the transfer or storage of illegal information are not permitted.

3.2 Who can Use

Authorized Users are permitted to use Bishop's IT Resources that are made available to them in their role. It is implied that in use, Authorized Users will take reasonable steps to ensure the Availability and Security of those resources. This will include, but is not limited to:

3.2.1 Authorized Users shall use Bishop's IT Resources in an ethical, responsible and lawful manner, in accordance with University policies.

3.2.2 Authorized Users shall take all reasonable steps to protect the Confidentiality, Integrity, and Availability of Bishop's IT Resources.

3.2.3 Authorized Users shall only access Bishop's IT Resources in accordance with Bishop's policies and procedures.

3.2.4 Authorized Users shall respect the intellectual property, including but not limited to, trademarks and copyrights, of owners of software and Data stored in or transmitted through Bishop's IT Resources, including library and archival resources.

3.2.5 Assuring the physical security of the device(s) in use, whether from foreign materials, physical theft or other damage.

3.2.6 Observing best Security practices as found on the ITS Virtual Helpdesk website, as they apply to Credentials.

3.2.7 Contacting the ITS Helpdesk immediately when issues relating to Security or malfunctioning equipment arise.

4. Credentials

4.1 Privacy

Authorized Users shall not knowingly divulge their personal Credentials to other individuals for any reason. Where it is essential that an account be shared between two or more people, clients should see ITS for the creation of a set of Credentials designed specifically for this task.

4.2 University's Role in Protection

In situations where ITS believes that an Authorized User's Credentials have been compromised, ITS may change passwords and PINs of the Authorized User's account to ensure the Integrity of our systems. Attempts will be made to contact the Authorized User at that time to inform them of the issue and begin a process to restore access.

5. Security

5.1 Authorized Users' Responsibilities

Authorized Users shall take the measures necessary to protect the Security of Bishop's IT Resources, including but not limited to:

5.1.1 Ensuring that other individuals are not watching the entering of Credentials on a device or website

5.1.2 "Locking" their computer workstation or other device(s) when leaving them unattended

5.1.3 Using their University Email Address as access credentials only for University-related matters, software and websites

5.1.4 Not using Bishop’s IT Resources for any purpose that puts the University at risk of compromising Security

5.1.5 Contacting the Helpdesk immediately when there is a possibility that Credentials or Bishop's IT Resources have been compromised

5.2 University's Role

The University is responsible for ensuring the effective and reliable operation of our systems and protection of our information technology resources. Therefore, the University will, in the attempt of a breach or other security compromise, monitor, audit, and log all information relating to the device(s) or Authorized User(s) in question. This may include live-monitoring of an Authorized User's activities by a System Administrator employed by the University or by a duly-appointed external partner.

6. Data

6.1 Confidentiality of Data

Confidential Data shall only be accessed by Authorized Users or by other individuals having a legitimate need and duly delegated by an Authorized User. The Confidentiality of Data accessed shall be preserved and the Data shall be used solely for the purposes for which it was accessed.

6.2 Access by Others

Notwithstanding section 6.1, access to Authorized User data may be provided to a University administrator with a legitimate interest in, and responsibility for, the matter in the following cases:

6.2.1 For continued operation of the University where the Authorized User whose Data are accessed is unavailable or no longer at Bishop's.

6.2.2 To investigate information security breaches where there exist reasonable grounds to believe that such a breach has occurred.

6.2.3 Where permitted and/or required by law.

6.3 Location of Data

Before entrusting storage, processing or transmission of Personal Information to any vendor owned by a company or service outside Québec, an Authorized User shall consult with the Vice Principal, Finance and Administration for guidance, who will then consult with senior administrators and/or legal counsel as required.

7. Email

7.1 Account

All Authorized Users are provided with a University Email Address with which to conduct University business.

7.2 Authorized Users' Responsibilities

It is the responsibility of each Authorized User to ensure that their email account is maintained with enough free space to ensure they are able to continue to receive emails. The University will not be held liable for a non-received email messages.

Additionally, while the technical capability exists for users to automatically forward or redirect all of their University email to an external email account, they should assure that the e-mail receives protections similar to those of University e-mail accounts and respects standards and laws concerning privacy and retention and destruction of documents.

7.3 Personal Use

The University understands that Authorized Users may occasionally utilize their University Email Address for personal use. Users must be aware that while they may do so, no additional protections will be available for personal email contained within the account. Should one of the provisions of this Policy allow System Administrators or others to access that account, all email in the account will be accessible.

8. Network

8.1 Access

ITS shall not normally use technology to prevent an Authorized User of Bishop's IT Resources from accessing an external site or service, where the computer has been configured to have access to Internet.

8.2 Exceptions

Notwithstanding section 8.1 the University shall moderate, filter, limit or block Internet traffic, where it exposes the University or Authorized Users to threats to Security or where it is necessary to ensure the Confidentiality, Integrity or Availability of Bishop's IT Resources.

8.3 Extending the Network

Authorized Users may not use software or hardware (including switches, routers, wireless access points, internet sharing devices, VPNs and/or firewalls) to extend or augment the University Network in any way without prior authorization from ITS.

9. Systems Administration

9.1 Role of ITS

Each Bishop's IT Resource has a duly appointed System Administrator that is responsible for maintaining the Availability and Integrity of that Resource. During the commission of normal work, Systems Administrators may monitor, log or otherwise access software or resources using hardware or software tools. Any Data obtained or witnessed during the commission of these duties shall only be used within their legitimate authority and will be treated as confidential.

10. Cybersecurity

10.1 Training

The University will engage in periodic cybersecurity training for Authorized Users.

10.2 Ongoing Dissemination

Periodically, or whenever contextually relevant, Information Technology Services may send out information regarding cybersecurity reminders, tips or warnings about current attacks, scams or other newsworthy cybersecurity events. It is expected that Authorized Users will read and apply an appropriate amount of attention to the information provided.

11. Compliance

11.1 Violations

Violations of this policy may lead to disciplinary action within the University and/or civil/criminal proceedings in cases which warrant such an escalation.

11.2 Investigations

When an abuse of the Acceptable Use Policy is suspected, the University and/or ITS may conduct a preliminary investigation, which may include the review of all subject Authorized User files, accesses, logs, emails, and/or other Data.

During, or as the result of, an investigation, Authorized User Credentials may be suspended or revoked.