Acceptable Use of IST Resources

Policy #: IT – 15
Date Drafted: 10/16/06
Revision Date: 06/27/24

Brief Description:

Access to technological systems and networks owned or operated by Bluefield University implies certain responsibilities and obligations. Access is subject to University policies and local, state, and federal laws. Acceptable use is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security, Christian values, and individual rights to privacy and to freedom from intimidation and harassment. This policy pertains to all members of the Bluefield University community, including faculty, staff, alumni, and students.

Contents

1. Introduction:

This acceptable use policy applies to all users of Bluefield University Information Services and Technology (IST) resources. This includes the resources under the management or control of the Information Services and Technology Department (IST). A 'user' is defined as any individual who uses, logs into, or attempts to use or log into, a system; who connects to, or attempts to connect to or traverse, a network, whether by hardware or software or both, whether on campus or from remote locations; or who physically handles any hardware. The term 'user' thus includes system sponsors and system managers, faculty, staff, students, and other customers. 'Information Services and Technology resources' are those facilities, technologies, and information resources required to accomplish information processing, storage, and communication, whether individually controlled or shared, stand-alone, or networked. Included in this definition are classroom technologies, electronic resources, and computing and electronic communication devices and services, such as, but not limited to, computers,

tablets, phones, printers, scanners, modems, switches, access points, e-mail, fax transmissions, social media information, video, multi-media, instructional materials, and course management and administrative systems. User-owned personal equipment connected to the University network is also subject to this policy.

2. Policy Statement:

In making appropriate use of IST resources, you MUST:

- Use resources for authorized purposes.
- Protect your personal information and the system from unauthorized use. Personal information includes personal data, such as your birth date, social security number, or banking information, as well as your University-provided credentials and information. You are responsible for all activities taking place under your University credentials or that originate from your user-owned personal equipment.
- Log off IST resources when they are not in use.
- Access only information that is your own, that is publicly available, or to which you have been given authorized access.
- Use only legal versions of copyrighted software in compliance with the vendor license requirements.
- Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks, degrading services, or wasting computer time, connect time, disk space, printer paper, printer toner, manuals, or other resources.
- Conform to instructions/warning signs given in all lab areas.

In making appropriate use of resources, you MUST NOT:

- Consume beverages or food in any computer lab on campus.
- Use another person’s system, personal equipment, login credentials, files, or data.
- Use computer programs to decode passwords, gain access to confidential information, control confidential information, or monitor network activities.
- Attempt to circumvent or to subvert security measures or University restrictions.
- Engage in any activity that might be harmful to systems or to any information stored therein, such as visiting suspicious websites, downloading suspicious files, creating, or propagating viruses, disrupting services, or damaging files. Suspicious is to be defined as any file, website, or application that is likely to cause damage or propagate malware.
- Use University systems for commercial or for partisan political purposes.

- Use college systems or networks to view, read, watch, or print illicit, illegal, or pornographic material.
- Make or use illegal copies of copyrighted software, store such copies on University systems, or transmit them over University networks.
- Use email, messaging, calling, video conferencing or display services to harass or to intimidate another person, for example, by broadcasting unsolicited messages, sending unwanted mail, downloading, printing, or displaying offensive material (e.g., desktop backgrounds or profile pictures), or by using someone else's name or credentials.
- Waste computing resources, for example, by intentionally placing a program in an endless loop, by using excessive amounts of paper through printing needlessly, for amusement, or by sending chain communication.
- Destroy or damage technical equipment or hardware, such as keyboards, mice, computers, tablets, printers, and monitors.
- Use the University's systems or networks for personal gain; for example, by selling access to your login credentials or performing work for profit with University resources, or by selling/buying merchandise online for profit.
- Engage in activity that does not conform to the statements above.

3. Enforcement:

Bluefield University considers any violation of the acceptable use principles or guidelines to be a serious offense. Any or all uses of these systems and all files on these systems may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to Bluefield University and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. Bluefield University also reserves the right to protect its network from systems and events that threaten or degrade operations. Bluefield University also reserves the right to determine what is acceptable and not acceptable in the use of Bluefield University Information Services and Technology Department resources, including University hardware, University network, and University files. Violators are subject to disciplinary action as prescribed in the honor codes, in the *Student Handbook*, in the *Faculty Handbook*, and in the *Staff Handbook*. Offenders may be prosecuted under the law to its fullest extent.

Bluefield University Department of Information Services and Technology may suspend or limit access to its resources for misuse of software, hardware, and/or network services. Other actions may be taken depending on the nature of any misuse including investigating any suspicious activity. Violations may result in loss of access privileges, disciplinary action by student judicial groups, and/or prosecution under civil or criminal laws. By using these systems, you are

consenting to follow and submit to all Bluefield University policies concerning appropriate network use.

4. Related Policies:

This collection of Bluefield University Information Services and Technology policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify Bluefield University policy.

5. Glossary:

- User: Any individual who uses, logs into, or attempts to use or log into a system; who connects to, or attempts to connect to or traverse, a network, whether by hardware or software or both, whether on campus or from remote locations; or who physically handles any hardware.
- Information Services and Technology (IST) resources: Facilities, technologies, and information resources required to accomplish information processing, storage, and communication, whether individually controlled or shared, stand-alone, or networked. Includes classroom technologies, electronic resources, and computing and electronic communication devices and services such as computers, tablets, phones, printers, scanners, modems, switches, access points, e-mail, fax transmissions, social media information, video, multi-media, instructional materials, and course management and administrative systems.
- Personal Information: Personal data such as birth date, social security number, banking information, University-provided credentials, and information.
- Authorized Access: Access to information that is your own, publicly available, or information to which you have been given authorized access.
- Suspicious Websites/Files: Any file, website, or application that is likely to cause damage or propagate malware.