POLICY TITLE: Acceptable use of IST Resources

POLICY #: IT – 15

DATE DRAFTED: 10/16/06

DATE POSTED for Review:

APPROVED DATE:

REVISION DATE: **2/8/07 AB** 05/22/07 AB

BRIEF DESCRIPTION:

Access to communication systems and networks owned or operated by Bluefield College imply certain responsibilities and obligations. Access is granted subject to college 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 mechanism, and individual rights to privacy and to freedom from intimidation and harassment. This policy pertains to all members of the Bluefield College community; faculty, staff, and students.

Introduction | Policy Statement | Password Standards **|** Related Policies **|** IT Policy Index

Introduction:

This acceptable use policy applies to all users of College information systems and technology (IST) resources. This includes the resources under the management or control of the Information Systems and Technology Department (IST). A "user" is defined as any individual who uses, logs into, or attempts to use or log into, a system; or 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. The term "user" thus includes system sponsors and system managers, faculty, staff, students, and other customers. "Information systems 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, printers, modems, e-mail, fax transmissions, video, multi-media, instructional materials, and course management and administrative systems. Student owned personal equipment physically connected to the College network is also subject to this policy, along with the *Residence Hall Network Acceptable Use Policy (Resnet)* and the *Network Citizenship Policy.*

Policy Statement:

In making appropriate use of IST resources, you MUST:

- Use resources for authorized purposes;
- Protect your user ID and the system from unauthorized use. You are responsible for all activities taking place under your user ID or that originate from your system;
- 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, manuals, or other resources; and
- 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 computing lab facility on campus;
- Use another person's system, user ID, password, 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;
- Engage in any activity that might be harmful to systems or to any information stored therein, such as creating or propagating viruses, disrupting services, or damaging files;
- Use college systems for commercial or for partisan political purposes;
- Use college systems or networks to view or print pornographic material;
- Make or use illegal copies of copyrighted software, store such copies on college systems, or transmit them over college networks.
- Use email, messaging, or display services to harass or to intimidate another person, for example, by broadcasting unsolicited message, by sending unwanted mail, downloading, printing or displaying offensive material (e.g., screen savers), or by using someone else's name or user ID;
- 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 letters;
- Destroy or damage networking equipment, such as keyboards, mice, computer towers, printers and monitors;
- Consume beverages or food in any computing lab facility on campus;

- Use the college's systems or networks for personal gain, for example, by selling access to your user ID or performing work for profit with college resources in a manner not authorized by the college, or by selling/buying merchandise on-line; and
- Engage in activity that does not conform to the statements above.

Enforcement

Bluefield College 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 College and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. Bluefield College also reserves the right to protect its network from systems and events that threaten or degrade operations. Bluefield College also reserves the right to determine what is acceptable and not acceptable in the use of computer systems. 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 College Department of Information Systems 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 College policies concerning appropriate network use.

Related Policies, References and Attachments:

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