ACCEPTABLE USE

UNIVERSITY POLICY #50

Authority: BOG Policy 60: Information Technology Governance
Approval Date: 05/07/21
Effective Date: 05/07/21
Revision History:
President's Signature: On File

SECTION 1: Purpose and Scope

1.1 The purpose of this Policy is to establish the rules that govern the use of University Information Technology and Digital Resources ("IT Resources").

1.2 This Policy applies to all active Authorized Users for whom University IT Resources and network access are made available by the University.

SECTION 2: Acceptable Use

2.1 University IT Resources must never be used to conduct activities that would jeopardize the University's tax-exempt status, for political purposes, personal economic gain, or to libel, slander, or harass another person.

2.2 **Access.** Access to University IT Resources and University Data will be based on Least Privilege or on a need-to-know basis depending on the individual's job responsibilities.

2.2.1 Use of another person's WLU Login credentials to access University IT Resources and/or University Data is strictly prohibited.

2.3 **Institutional Use**. Use of all University IT Resources should be for purposes that are consistent with the non-profit educational mission and the policies and legal requirements of the University, and not for commercial purposes.

2.4 **Personal Use.** Personal use of University IT Resources, except for students enrolled at the University, should be incidental and kept to a minimum.

2.5 **Political Use.** As a governmental entity, the University is prohibited from participating or intervening in any political campaign on behalf of or in opposition to a candidate for public office, and no substantial part of the University's activities may be directed to influencing legislation (i.e. lobbying). Individuals may not use University IT Resources for political purposes in a manner that suggests the University itself is participating in campaign or political activity or fundraising, or for influencing legislation. Any other use with respect to political activity must be permitted by applicable University policy and consistent with applicable laws.

2.6 **Prohibited Use.** Use of University IT Resources should not violate applicable federal, state, and local law, including U. S. copyright law, or applicable University policies. If travel is involved, use of University IT Resources should not violate the laws of the relevant nation or state. University IT Resources may not be used to transmit malicious,

harassing, or defamatory or unprofessional content. Prohibited use includes, but is not limited to, the following:

2.6.1 Activities that may permit unauthorized access to University IT Resources, including leaving devices unsecured or sharing WLU Login credentials;

2.6.2 Storing University data in an unsecure location;

2.6.3 Disrupting or endangering University IT Resources by bypassing, subverting, or otherwise rendering ineffective the security controls implemented;

2.6.4 Altering, moving, or removing software, system logs, configuration files, or other files needed for the operation of a University IT Resource;

2.6.5 Unauthorized downloading or distribution of copyrighted materials;

2.6.6 Intentionally, recklessly, or negligently causing damage by any means to University IT Resources;

2.6.7 Deliberate unauthorized altering, moving, or destruction of University IT Resources.

2.6.8 Sending frivolous or excessive messages (e.g., spam, junk mail, chain letters);

2.6.9 Intercepting another individual's transmissions;

2.6.10 Conducting unauthorized commercial or personal business activities including sending personal email that may be construed by the recipient to be from the University, operating a personal business, political lobbying, or endorsement of political candidates; and,

2.6.11 Transmitting, receiving, accessing, printing, or storing any communication or content of a defamatory, discriminatory, harassing, obscene, or sexually explicit nature or otherwise considered inappropriate workplace conduct and behavior.

2.6.12 Any personal or commercial solicitation not authorized by West Liberty University.

SECTION 3: Access and Privacy

3.1 The University has the legal right to access, preserve and review all information stored on or transmitted through its electronic services, equipment and systems (collectively, "IT Systems"). The University endeavors to afford reasonable privacy for individual users and does not access information created and/or stored by individual users on its IT Systems except when it determines that it has a legitimate operational need to do so.

SECTION 4: Protection of University Resources

4.1 Users of University IT Resources are responsible for protecting University data, including its confidentiality, integrity, access, retention and disposal, in accordance with the University's Information Privacy Policy and other applicable University policies. Individuals with University accounts or administrative responsibility over any University resources should take reasonable measures to protect these accounts and resources. Shared University IT Resources should be used for educational purposes and to carry out the legitimate business of the University and should not be used in a way that disrupts or otherwise interferes with any University activities or systems or that is inconsistent with the University's policies or goals.

4.2 This Policy is not intended to abridge academic freedom, constitutional guarantees of free speech, or freedom of expression. While the rights of academic freedom and intellectual creativity are recognized, the interests of the University, students, faculty, and staff must be protected. In addition to consideration of legal liability issues, the institutional image and reputation of WLU are valuable assets requiring protection.

SECTION 5: Violations and Penalties

5.1 Any employee who violates this Policy will be subject to appropriate disciplinary action.

5.2 Any student who violates this Policy will be subject to appropriate disciplinary action in accordance with the Student Code of Conduct.

5.3 Any individual affiliated with the University who violates this Policy will be subject to appropriate corrective action, including, but not limited to, termination of the individual's relationship with the University.

5.4 The University's Chief Information Officer will coordinate with appropriate University entities on the implementation and enforcement of this Policy.

5.5 Responsibility for interpretation of this Policy rests with the President and Chief Information Officer.

SECTION 6: Definitions

6.1 "Authorized Users" means faculty, adjuncts, staff, students, authorized visitors, guests, and others who have assigned WLU Login credentials which provides them access to University IT Resources.

6.2 "Information Technology and Digital Resources ("IT Resources")" means University-owned devices and systems; University-contracted systems and services; privately-owned or publicly provided devices using the University's networks and resources; technology administered within the University internet domain by individual departments or members of the faculty or staff or by campus organizations; information services hosted by dorm-resident students or by authorized resident visitors on their

own hardware connected to the campus network; resources administered by administrative departments such as University Libraries or IT; authorized collaborative devices connected to the campus network and using University internet addresses; personally-owned devices connected by wire or wireless service to the campus network from University-owned housing or via campus locations providing mobile wired access or wireless access; actions originating from computer systems or mobile devices maintained or used by members of the campus community off-campus including in student areas, but connecting remotely to the University's network services; and websites bearing the University credentials, even when hosted outside the University's internet domain.

6.3 "Least Privilege" means granting the minimum system resources and authorizations needed to perform its function or restricting access privileges of Authorized Users to the minimum functions necessary to perform their job.