Acceptable Use of Data and Technology Resources Policy

Policy Number: 1.11.1.1
Category: Information Technology
Responsible Unit: Information Technology Services
Effective: December 31, 2019
Last Revised Date: February 9, 2022
Revision History: Originally effective August 13, 2016; major revision March 27, 2017; major revision December 31, 2019; minor revision April 14, 2021; minor revision February 9, 2022
Review Date: December 30, 2022

Section 1:
PURPOSE AND SCOPE

1.1 The purpose of this Policy is to establish the rules that govern the use of the devices and information systems at West Virginia University, West Virginia Institute of Technology, and Potomac State College of West Virginia University ("University Technology Resources") to ensure both the protection of University Data and compliance with University policies and applicable laws and regulations.

1.2 This Policy applies to all individuals granted access to University Data and/or University Technology Resources ("Authorized Individuals"), including systems and services provided by third-parties, personally-owned, and publicly provided devices that connect to the Campus Network.

Section 2:
UNIVERSITY DATA AND UNIVERSITY TECHNOLOGY RESOURCES

2.1 University Data must be maintained pursuant to the Record Retention Policy and Schedule.

2.2 Pursuant to the Sensitive Data Policy, information the University considers Sensitive Data must only be retained within an approved University Technology Resource and must never be accessed or downloaded to a personal device.

2.3 Electronic University Data that does not require retention ("Incidental Records") must only be retained for as long is necessary to complete the action or resolve the issue that is the subject of the record.

2.4 The University will provide the use of University Technology Resources to Authorized Individuals as the primary means to create, store, send, or receive University Data.

2.5 Employees may not use University Technology Resources for political purposes in violation of the University and its affiliates' tax-exempt statuses; for their own private gain in violation of any state or federal ethics law; or to libel, slander, or harass another person.

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

2.7 Use of another person's WVU Login credentials to access University Technology Resources and/or University Data is strictly prohibited.

2.8 The University will monitor University Technology Resources and their use when necessary for operational needs and to ensure compliance with applicable laws and University policies and standards.

2.9 When the University receives a Freedom of Information Act request, subpoena, litigation, or other similar request for information or documents, it will take necessary measures to access University Technology Resources in order to obtain the requested University Data and comply with its legal obligations.

2.10 *De minimis* personal use of University Technology Resources is permitted provided the use does not:

2.10.1 Consume more than a trivial amount of resources that could be otherwise used for University academic, administrative, research, or outreach purposes;

2.10.2 Interfere with worker productivity;

2.10.3 Preempt any University activity; or,

2.10.4 Promote or result in a hostile work or academic environment.

2.11 Authorized Individuals who use University Technology Resources are advised that they should have no expectation of privacy or confidentiality in connection with anything they create, store, send, or receive on University Technology Resources, including de minimis personal use of these resources.

2.12 *De minimis* use of personally owned devices to create, store, send, or receive University Data is permitted pursuant to the requirements within the Bring Your Own Device Standard.

2.13 The University is bound by the contractual and licensing agreements it has entered; therefore, all members of the University utilizing such resources (e.g., software) are also expected to comply.

2.14 The University community must respect the rights of ownership of intellectual property and adhere to United States copyright laws.

2.15 The University Technology Resources provided by the University are shared widely and are limited. Any use of automated processes to gain technical advantage over others at the University is prohibited.

2.16 Frivolous, excessive, or inappropriate use of University Technology Resources by one person or a group of people that adversely affects the Campus Network and/or the ability of others to legitimately utilize such resources is strictly prohibited.

2.17 The University will limit use of resources through quotas, time limits, and other mechanisms should an individual and/or group of people exhibit a continued pattern of adversely affecting University Technology Resources.

Section 3:
EXPECTATIONS OF AUTHORIZED INDIVIDUALS

3.1 Individuals authorized to use University Technology Resources and/or access University Data are expected to:

3.1.1 Adhere to, and maintain all University Technology Resources according to, established University policies, standards, and procedures;

3.1.2 Adhere to all applicable international, federal, state, and local laws and regulations, including, but not limited to, those that pertain to the use, copy, and distribution of:

3.1.2.1 Protected health information;

3.1.2.2 Educational records;

3.1.2.3 Covered financial information; and,

3.1.2.4 Music, videos, games, images, texts, sound files, film clips, trademarks, logos, and other media.

3.1.3 Adhere to the contractual and licensing agreements to which the University has entered related to use of third-party resources (e.g., software) and require each individual using the resource to comply;

3.1.4 Use only University Technology Resources and/or accessing University Data for the purpose for which access has been granted;

3.1.5 Secure WVU Login credentials to prevent unauthorized access;

3.1.6 Be held accountable for all activities conducted under their Authentication;

3.1.7 Secure University Technology Resources and University Data appropriately;

3.1.8 Respect the rights and privacy of others;

3.1.9 Acknowledge the finite capabilities of University Technology Resources and limiting use to only consume the reasonable amount required to carry out activities;

3.1.10 Use the University's marks (e.g., trademark, logo) only as authorized; and,

3.1.11 Never represent personal comments as being those of the University.

Section 4:
UNACCEPTABLE USE OF TECHNOLOGY RESOURCES AND DATA AT THE UNIVERSITY

4.1 University Data and Technology Resources must never be subject to Unacceptable Use, which means the following:

4.1.1 Activities that may permit unauthorized access to University Technology Resources and University Data, including leaving Devices unsecured or sharing WVU Login credentials;

4.1.2 Storing University Data in an unsecure location;

4.1.3 Failing to destroy University Data when it is no longer needed (e.g., shredding printouts, erasing magnetic media);

4.1.4 Disrupting or endangering University Technology Resources and University Data by bypassing, subverting, or otherwise rendering ineffective the security controls implemented;

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

4.1.6 Unauthorized downloading or distribution of copyrighted materials;

4.1.7 Intentionally, recklessly, or negligently causing damage by any means to University Technology Resources and/or University Data;

4.1.8 Deliberate unauthorized altering, moving, or destruction of University Data or University Technology Resources;

4.1.9 Sending unsolicited, disruptive messages (e.g., spam, junk mail, chain letters);

4.1.10 Intercepting another individual's transmissions;

4.1.11 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,

4.1.12 Intentionally transmitting, receiving, accessing, printing, or storing any communication or content of a defamatory, discriminatory, harassing, obscene, or sexually explicit nature in violation of federal or state laws and regulations or Board of Governors Rule 1.6.

4.2 Additional examples of Unacceptable Use can be found within Exhibit A of this Policy.

Section 5:
DEFINITIONS

5.1 "Authorized Individuals" means faculty, staff, students, and others who have assigned WVU Login credentials which provides them access to University Data and Technology Resources such as retirees, consultants, presenters, camp attendees, or vendors.

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

5.3 "University Technology Resources" means the Campus Network, University-owned hardware, software, and communications equipment, technology facilities, and other relevant hardware and software items, as well as personnel tasked with the planning, implementation, and support of technology. University Technology Resources can be broken into the following categories:

5.3.1 **Campus Network** means the wired and wireless components and University Technology Resources connected to the network managed by the University. Excludes residence halls, University public/private partnerships, and other relationships the University may establish with

institutions, including the City of Morgantown and WVU Medicine, through which the University provides IP addresses but does not manage the network.

5.3.2 **Device** means a server, computer, laptop, tablet, or mobile device used to enter or access University Data from a University Information System.

5.3.3 **University Information System** means an application or software that is used to support the academic, administrative, research, and outreach activities of the University, whether operated and managed by the University or a third-party vendor.

5.4 "University Data" means anything that contains information regarding the University made or received in connection with its operations, regardless of whether it is a hard copy or electronic, and includes, but is not limited to, written and printed matter, books, drawings, maps, plans, photographs, microforms, motion picture films, sound and video recordings, e-mails, computerized or other electronic data on hard drives or network drives, or copies of these items. See Record Retention Policy and Schedule.

Section 6:
ENFORCEMENT AND INTERPRETATION

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

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

6.3 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.

6.4 The University's Chief Information Officer, supported by the Chief Information Security Officer, will coordinate with appropriate University entities on the implementation and enforcement of this Policy.

6.5 Responsibility for interpretation of this Policy rests with the Chief Information Officer.

Section 7:
AUTHORITY AND REFERENCES

7.1 BOG Rule 1.11 – Information Technology Resources and Governance

7.2 All other University policies are also applicable to the electronic environment. Relevant institutional policies include, but are not limited to:

7.2.1 Sensitive Data Policy

7.2.2 Sensitive Data Protection Standard

7.2.3 Electronic Mail Policy

7.2.4 Bring Your Own Device (BYOD) Standard

7.2.5 Record Retention Policy and Schedule

7.2.6 WVU FERPA Policies

7.2.7 Faculty Handbook

7.2.8 Code of Student Rights and Responsibilities (Code of Conduct)

CONNECT WITH US

Service Desk Hours

Monday – Thursday: 7:30 a.m. – 10 p.m.
Friday: 7:30 a.m. – 8 p.m.
Saturday: 10 a.m. – 5 p.m.
Sunday: 10 a.m. – 10 p.m.

Closed on official University holidays.

Contact Us

Information Technology Services
One Waterfront Place
Morgantown, WV 26506

(304) 293-4444 | 1 (877) 327-9260
ITSHelp@mail.wvu.edu

Get Help

Maintenance Schedule

To function effectively and securely, applications and the systems that support them must undergo regularly planned maintenance and updates.

See Schedule