Board of Trustees

Audit Committee

1:30 p.m.
February 17, 2022

Loughman Living Room, Scanlon Hall

A live stream of the meeting for public viewing will also take place on YouTube at the following link: https://www.westfield.ma.edu/live.

COVID-19 Procedures: Masks are required when indoors at Westfield State University, regardless of vaccination status. For more information about Westfield State's COVID-19 procedures, visit: https://www.westfield.ma.edu/spring-2022covid/faq.

---

1. Called to Order	Trustee Boudreau
2. Minutes	
a. December 16, 2021	Trustee Boudreau
3. President's Remarks	President Thompson
4. Items for Information	
a. Acceptable Use of Information Technology Resources Policy (0380)	Alan Blair
b. Public Safety Policy Overview	Tony Casciano
c. Uniform Guidance Audit Update	Lisa Freeman
5. Items for Discussion	
a. Risk Management/Internal Audit	Trustee Boudreau/Stephen Taksar
6. Items for Action	
a. Motion – Electronic Mail Policy (0550)	Alan Blair

Attachment(s):

a. Minutes 12-16-21 (Draft)
b. Acceptable Use of Information Technology Resources Policy (Track Changes)
c. Public Safety Policy Overview (Memo)

d. Motion – Electronic Mail Policy
e. Electronic Mail Policy (No Track Changes)
f. Electronic Mail Policy (Track Changes)
g. Electronic Mail Policy (Distribution List Guidelines)
h. Electronic Mail Policy (Social Media Guidelines)

Board of Trustees

Audit Committee

December 16, 2021

Minutes

Conference Room A (Garden Level), Horace Mann Center
A live stream of the meeting for public viewing also took place on YouTube.

MEMBERS PRESENT: Committee Chair Paul Boudreau, Vice Chair William Reichelt, and Secretary Dr. Gloria Williams

MEMBERS PARTICIPATING REMOTELY: Trustee Melissa Alvarado

TRUSTEE GUESTS PRESENT: Trustees Dr. Robert Martin, Kevin Queenin, and Ali Salehi

Dr. Linda Thompson, President of Westfield State University, was also present.

The meeting was called to order at 1:08 PM by Committee Chair Boudreau.

> **MOTION** made by Trustee Alvarado, seconded by Trustee Reichelt, to approve the minutes of the October 13, 2021 meeting.
>
> There being no discussion, **ROLL CALL VOTE** taken:
>
Trustee Alvarado	Yes
Trustee Reichelt	Yes
Trustee Williams	Yes
Trustee Boudreau	Yes

> **Motion passed unanimously.**

A roll call was taken of the committee members participating as listed above and announced that the meeting was being livestreamed and captured as recorded.

FY21 Payment Card Industry (PCI) Assessment. The University passed the assessment again this year, but it was challenging to do the assessment audit remotely because of securely providing information that is typically gathered in person. This year's audit will also be remote. There are significant changes in the environment for our payment cards. If we fail one of 200 areas, we can lose the right to accept credit and debit card payments.

Performance Audit: Post Audit Review. A letter has been received from the state auditor following up on action plans for the state audit. A form that was sent to them showing our implementation of the plan was shared. A new process has been developed with adding vendors to the system with signoffs from the people entering and reviewing the information. The KnowBe4 cybersecurity training completion is at 62%, with positive feedback from the campus. Monthly phishing campaigns will start soon. President Thompson

requested a harder push to obtain completion of the training by every person on the campus. It was suggested to provide a list of employees who have not completed security training be given to each vice president to send out reminders. Frequent clickers of scam material will automatically be enrolled in additional training.

Risk Management/Internal Audit. There has been some progress in this area by hiring Brittany Rende as the new Title IX Coordinator. Ms. Rende stated there is some work to do to be compliant with the 2,200 pages of regulations. She will be soon be providing training for the campus community and the Board, who are required reporters for Title IX violations.

There being no other business, **MOTION** made by Trustee Williams, seconded by Trustee Reichelt, to adjourn.

There being no discussion, **ROLL CALL VOTE** taken:

Trustee Alvarado	Yes
Trustee Reichelt	Yes
Trustee Williams	Yes
Trustee Boudreau	Yes

Motion passed unanimously.

Meeting adjourned at 1:26 PM.

Attachments presented at this meeting:

a. Minutes 10-13-21 (Draft)
b. FY21 PCI (Summary)
c. Performance Audit (Letter)
d. Performance Audit (Response)

Secretary's Certificate

I hereby certify that the foregoing is a true and correct copy of the approved minutes of the Westfield State University Board of Trustees Audit Committee meeting held on December 16, 2021.

_____ _____

Dr. Gloria Williams, Secretary Date

Westfield State University

Policy concerning:

APPROVED: March 2000

REVIEWED: December 2021~~December 2013~~

ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

PURPOSE

The purpose of this policy is to provide guidelines for the appropriate use of information technology resources at Westfield State University ("University") and establish sanctions for violations of this policy. This policy is intended to protect the users of the University's information technology resources by ensuring a reliable and secure technology environment that supports the educational mission of the University. These resources are provided as a privilege to all Westfield State University employees, students, and authorized guests. The University seeks to ensure the integrity of information technology resources made available to the community and to prevent disruption to academic and administrative needs. This policy is not intended to inhibit the culture of intellectual inquiry, discourse, and academic freedom.

In general, the same ethical conduct that applies to the use of all University resources and facilities applies to the use of the University's information technology resources.

SCOPE

This policy applies to all students, faculty, and staff of the University, and to all other users who are authorized by the University to access its information technology resources. This policy is supplemented by the policies of those networks to which the University is interconnected, including, but not limited to, the University of Massachusetts Information Technology Systems group, the Commonwealth of Massachusetts' Information Technology Division, Umass Online, etc.

For the purposes of this policy, "Information Technology Resources" means all computer and communication facilities, services, data, and equipment that are owned, managed, maintained, leased, or otherwise provided by the University.

USER OWNERSHIP AND RESPONSIBILITIES~~REPONSIBILITIES~~

It is the responsibility of any person using the University's information technology resources to read, understand, and follow this policy. In addition, all users are expected to exercise reasonable judgment in interpreting this policy, and in making decisions about the use of information technology resources. Any person with questions regarding the application or meaning of this policy should seek clarification from his or her supervisor, or from the Office of Information and Instructional Technology ~~Department~~.

The University owns and maintains the information stored in its information technology resources, and it limits access to its information technology resources to authorized users. Users of information technology resources have a responsibility to properly use and protect

these resources, respect the rights of other users, and behave in a manner consistent with any local, state, and federal laws and regulations, as well as all University policies. Information technology resources, including Internet bandwidth, are shared among the community, and users must utilize these resources with this understanding.

Users must respect all intellectual property rights, including any licensing agreements, applicable to information and resources made available by the University to its community.

Information technology resources are provided to support the mission of teaching and learning and to conduct official University business. Therefore, the University bears no responsibility for the loss of any personal data or files stored or located on any system.

The University does not systematically monitor communications or files. Users must be aware of, or responsible for, material which community members may post, send, or publish using its network, servers, and other resources including the Web.

UNACCEPTABLE USES OF UNIVERSITY INFORMATION TECHNOLOGY RESOURCES

The University permits limited, occasional, or incidental personal use of its information technology resources. Even when occasional usage is permitted, however, faculty, staff, students, and other authorized users should use discretion when using information technology resources for personal reasons.

The University prohibits the use of its information technology resources for the following purposes:

- in furtherance of any illegal act, including the violation of any criminal or civil laws or regulations, whether local, state, or federal.~~;~~
- for any political purpose.~~;~~
- for any commercial purpose.~~;~~
- to violate any University policy.~~;~~
- to discriminate against any person on the basis of any legally protected characteristic.~~;~~
- to harass any person based on ~~the basis of~~ any legally protected characteristic, including sex.~~;~~
- to access or share sexually explicit, obscene, or otherwise inappropriate materials.~~;~~
- to infringe any intellectual property rights.~~;~~
- to gain, or attempt to gain, unauthorized access to any computer or network.~~;~~
- for any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs.~~;~~
- to intercept communications intended for other persons.~~;~~

APPROVED: March 2000
2021~~December 2013~~

REVIEWED: December

- to misrepresent either the University or a person's role at the University.;
- to libel or otherwise defame any person.;
- to use e-mail or messaging services to threaten, harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted e-mail, or by using someone else's name or user-id.;
- to waste computing, network, or technology resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters, ~~or~~ unsolicited mass mailings or crypto mining.;
- to add, remove or modify equipment comprising the Information technology resources at the University unless they have been explicitly authorized to make such changes by the Chief Information Officer or his representative.;
- to install on the University's network for any purpose or use any peer-to-peer file sharing applications. In addition, any other network-based, non-academic application that consumes the University's bandwidth may be limited or restricted. The Chief Information Officer must approve the installation of any server or server-based application on the University's network.

This list is illustrative and not exhaustive, and the University reserves the right to determine other prohibited activities and/or unauthorized uses that are not specifically identified in this policy.

DATA CONFIDENTIALITY

While~~In the course of~~ performing their jobs, University employees and contractors often have access to confidential or proprietary information, such as personal data about identifiable individuals or commercial information about business organizations. Under no circumstances is it permissible for employees or contractors to acquire access to confidential data unless such access is required by their jobs. ~~-~~Under no circumstances may employees or contractors disseminate any confidential Information that they have rightful access to~~,~~ unless such dissemination is required by their jobs.~~-~~ Users of the University's information technology resources have a responsibility to protect the confidentiality of the information to which they have access.

COPYRIGHT PROTECTION

Computer programs are valuable intellectual property. Software publishers can be very aggressive in protecting their property rights from infringement. In addition to software, legal protections can also exist for any information published on the Internet, such as the text and graphics on a web site. ~~-~~As such, it is important that users respect the rights of intellectual property owners. Users should exercise care and judgment when copying or distributing computer programs or Information that could reasonably be expected to be copyrighted.

NETWORK SECURITY

APPROVED: March 2000
2021~~December 2013~~

REVIEWED: December

In compliance with state and federal data security laws, the University seeks to protect the security of its information technology resources and of users' accounts, and to prevent unauthorized access by others, both on and off campus.

It is critically important that users take particular care to avoid compromising the security of the network. ~~-~~Most importantly, users should never share their passwords with anyone else, and should promptly notify University personnel if they suspect their passwords have been compromised. ~~-~~In addition, users who will be leaving their PCs unattended for extended periods should log off the network.

The University reserves the right to make unannounced changes to the infrastructure or accessibility of any information technology resources. ~~in case of system instability or suspicion of possible criminal activity.~~

E-MAIL

In Massachusetts, e-mail is considered a public record and must be treated as such. E-mail is subject to production pursuant to a public record request, and it is subject to the Commonwealth's record retention policies in the same manner as paper records
When using e-mail, there are several points users should consider. First, because e-mail addresses identify the organization that sent the message (first.last@westfield.ma.edu), users should consider e-mail messages to be the equivalent of letters sent on official letterhead. Finally, although many users regard e-mail as being like a telephone in offering a quick, informal way to communicate, users should remember that e-mails can be stored, copied, printed, or forwarded by recipients. As such, users should not write anything in an e-mail message that they would not feel just as comfortable putting into a memorandum. ~~-~~Please refer to the Westfield State University Electronic Mail (E-mail policy).

PRIVACY/CONFIDENTALITY

The University is the owner of all information technology resources, including e-mail. ~~-~~As such, no student, faculty member, staff member or other authorized user has a reasonable expectation of privacy in their e-mail or any other use of the University's information technology resources.

To that end, the University cannot guarantee privacy or confidentiality in the use of its information technology resources. Under certain circumstances, the University may be legally obligated ~~-~~to disclose information in response to court orders or other legal actions, in response to public record requests, in disciplinary processes, in health and safety emergencies, or when necessary to protect the integrity or security of its information technology resources. The University retains full discretion in reviewing and disclosing records ~~in order~~ to comply with these requirements.

APPROVED: March 2000
2021~~December 2013~~

REVIEWED: December

Certain classes of data are also protected from disclosure by law or regulation. In compliance with those laws and regulations, the University seeks to protect any personally identifiable information managed on its information technology resources. All members of the University community with access to such data are required to maintain the confidentiality of such data in accordance with this policy.

Information technology resources at the University are the property of the University and the Commonwealth of Massachusetts. As such, the University retains, and when reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, the right to inspect any user's computer, any data contained in it, and any data sent or received by it. Any use of the University's information technology resources constitutes express consent for the University to monitor and/or inspect any data that users create or receive, any messages they send or receive, and any web sites that they access, in accordance with the requirements of the law and any relevant collective bargaining agreement.

MOBILE DEVICES

~~**PORTABLE COMPUTERS**~~

Employees using mobile devices~~portable computers~~ offsite are responsible for protecting the computer and any confidential files from theft or security breaches. This may include using a power-on password and encryption software. Any breaches of computer security or theft should be reported immediately to Public Safety and the Chief Information Officer.

ENFORCEMENT

Any behavior or activity that alters the normal functioning of the University's information technology resources, or which negatively impacts their use by any other member of the community, is strictly prohibited. The University retains the right to take any reasonable action necessary to protect the integrity and security of its information technology resources, to curtail illegal use of the resources, to ensure the resources are equitably shared, and to protect the rights and privacy of its users.

Users of information technology resources who violate this policy, gain unauthorized access, or violate any state, local or federal law will have their privileges to use information technology revoked and may be subject to the University's disciplinary processes and procedures. Violations of this policy may also result in disciplinary action, up to and including termination, expulsion and/or legal action. Illegal acts may also subject users to prosecution by law enforcement authorities.

APPROVED: March 2000
2021~~December 2013~~

REVIEWED: December

The use of the University's information technology resources constitutes an understanding of an~~and~~ agreement to abide by this policy.

REVIEW

This policy shall be reviewed annually by the Chief Information Officer ~~and the Vice President for Academic Affairs~~.

DEPARTMENT OF PUBLIC SAFETY

Westfield STATE UNIVERSITY

Memorandum

To: Stephen Taksar, Vice President, Administration and Finance

From: Tony Casciano, Director, Public Safety

Date: February 17, 2022

RE: Public Safety Policy/General Orders Overview

The International Association of Campus Law Enforcement Administrators (IACLEA) developed the following standards as a part of the IACLEA accreditation program. These standards are viewed as best practices and appropriate criteria for the effective and efficient operations of a campus public safety agency. They represent minimum requirements for an agency to achieve accreditation through the IACLEA program.

Additionally, we are required under a variety of Massachusetts General Laws and Code of Massachusetts Regulations (CMR's) to conform to those laws. An example would be the most recent changes in the Use of Force or Civil Disturbance.

The Westfield State University Department of Public Safety/University Police uses the term General Order to describe these standards. Other agencies use Standard Operating Procedures (SOP) or Department Policies.

The approval process for a General Order after it is written or updated is:

- Reviewed and approved by the Chief.
- Reviewed and approved by the Vice President who oversees Public Safety/ University Police.
- Reviewed by an AFSCME representative if the General Order has potential contractual implications.

Department of Public Safety
577 Western Avenue
P.O. Box 1630
Westfield, MA
01086-1630

(413) 572-5262
(413) 572-5496 (f)
westfield.ma.edu

Westfield STATE UNIVERSITY

Board of Trustees

February 17, 2022

MOTION

To approve the changes and accept the newly revised Electronic Mail Policy (0550), as presented.

_____ _____

Robert A. Martin, Ph. D., Chair Date

Westfield State University

Policy concerning

APPROVED: December 2013

REVIEWED: February 2022

ELECTRONIC MAIL (E-MAIL)

PURPOSE

The purpose of this policy is to establish a standardized, system-wide approach to managing the protection of information and Information Technology Resources to support core business needs and the provision of continuity and privacy at Westfield State University ("University") and establish accountability for violations of this policy. This policy is intended to protect the users of the University's Information Technology Resources by ensuring a reliable and secure technology environment that supports the educational mission of the University. These resources are provided as a privilege to all Westfield State University employees, students, and authorized guests. The University seeks to ensure the integrity of Information Technology Resources made available to the user community, as such, to ensure these resources are secure from unauthorized access for those that utilize them. This policy is not intended to inhibit the culture of intellectual inquiry, discourse, academic freedom, or pedagogy. In general, the same ethical conduct that applies to the use of all University resources and facilities applies to the use of the University's Information Technology Resources.

SCOPE

This policy applies to all students, faculty, staff, volunteers, vendors, consultants, contractors, or others (herein afterwards referred to as "constituents") who use or have authorized access to University Information Technology Resources. This policy is supplemented by the policies of those networks to which the University is interconnected, including, but not limited to, the University of Massachusetts Information Technology Systems group, the Commonwealth of Massachusetts' Information Technology Division, UMass Online, etc. It covers all University information whether in hardcopy or electronic form and any systems which access, process, or have custody of business data. This policy also applies to any and all information, in any form and in any medium, network, internet, intranet, computing environments, as well as the creation, communication, distribution, storage and disposal of information.

DEFINITIONS

Distribution List: A distribution list refers to a facility in the e-mail system to enable many subscribers mail addresses to be reached through a single (list) name. (i.e., departmental list, FACSTAFF, UniCom).

Westfield State University's e-mail system: The University's e-mail system is a communication resource to enhance and facilitate the academic and administrative operations of the University. This includes any originating e-mails containing @westfield.ma.edu. Use of the system shall be to support these purposes and this policy.

For the purposes of this policy, "Information Technology Resources" means all computer, applications and communication facilities, services, data and equipment that are owned, managed, maintained, leased or otherwise provided by the University.

PUBLIC RECORD

E-mail, whether created or stored on university-owned equipment may constitute a public record under Massachusetts' Public Records Law or be subjected to mandatory disclosure under other laws or regulations, including the rules compelling disclosure during litigation. Users of the University's e-mail services should be aware that Massachusetts' Public Records Law and statutory and regulatory provisions prevent the University from guaranteeing complete protection of email, including personal e-mail residing on the University's information technology resources.

The messages, information and data carried by the e-mail system are the sole property of the University and the Commonwealth of Massachusetts. The University reserves the right to monitor and access those systems and their contents as they deem necessary, in accordance with the law and relevant collective bargaining agreement. No user of the University's e-mail system shall have a reasonable expectation of privacy in any e-mail.

USER OWNERSHIP AND RESPONSIBILITY

I. SECURITY AND CONFIDENTIALITY

A. Individuals with approved access to the University's e-mail system have the responsibility to maintain a confidential password, as well as the responsibility to regularly change their password, to protect the system from unauthorized access. The University will never ask for your password, and users should not provide this information to anyone.

B. Individuals with approved access to the e-mail system have the responsibility to log off and lock their computer or mobile device. This will prevent others from tampering with an account or accessing confidential material.

C. All messages should be treated as confidential by other employees and accessed only by the intended recipient unless necessary as a normal function of their job. Employees are not authorized to intentionally retrieve or read any e-mail messages that are not sent to them.

D. Never assume that e-mail is confidential. A message can easily be forwarded to another e-mail user, and anyone has potential access to read an e-mail message once it has been printed. Technical problems or human error may result in the unintended distribution of e-mail.

E. Phishing attacks and cyber fraud incidents have significantly increased over the past few years. Your university provided email account helps identify you to

others and includes the security designed to help prevent these incidents. When conducting business as part of your employment at the university, you must utilize your university email address (ending in @westfield.ma.edu) to ensure proper identity and compliance.

II. USAGE

A. The University's e-mail system is the official method of communication for the University. Only mailboxes with westfield.ma.edu suffixes are supported. Anyone who utilizes another e-mail system, or forwards e-mail from their university account to another account does so at their own risk and is responsible for ensuring they are in receipt of all intended communications.

B. The University's e-mail system is intended to support the academic and administrative mission of the University. Users are expected to demonstrate a sense of responsibility in utilizing the email system to include maintaining professional etiquette in all e-mail communications.
.

Usage of the university e-mail system is also in accordance with the Social Media and Communication and the Distribution List guidelines.

III. RETENTION

Users are responsible for preserving their email in accordance with the Massachusetts Statewide Records Retention Schedule.
MA_Statewide_Records_Schedule_dec18.pdf (mma.org)

UNACCEPTABLE USES

It is unacceptable to use the University e-mail system as follows:

- for personal or private profit;
- In any way that violates University policy;
- In any way that violates local, state, or federal law;
- to send or receive, either across the University e-mail system or the Internet, any copyrighted materials, trade secrets, proprietary financial information, peer review committee reports and activities, or similar materials, or any information where exposure of that information to outside parties would have an adverse impact on the University or its employees, without prior approval;
- as a vehicle for unauthorized disclosure of confidential business or private facts concerning employees, students, or University-related business (authorized e-mail and e-mail attachments containing sensitive business information may be sent within the Westfield State University system on its secured network);
- for communications regarding commercial solicitations;

- for communications regarding political advertising, chain-letters, jokes, derogatory or inflammatory statements, and/or idle gossip.

ENFORCEMENT

Access to the e-mail system is a privilege and any misuse of the e-mail system may result in withdrawal of access to the system and disciplinary action up to and including termination. This policy will be reviewed annually by the Chief Information Security Officer.

Westfield State University

Policy concerning

APPROVED: December 2013

REVIEWED: August 2021

ELECTRONIC MAIL (E-MAIL)

PURPOSE

~~Westfield State University ("University") recognizes that principles of academic freedom and shared governance, freedom of speech and confidentiality hold important implications for electronic mail and electronic mail services ("e-mail"). E-mail is provided as a privilege to all University employees, students, and authorized guests. The same ethical conduct that applies to the use of all University resources and facilities applies to the use of university e-mail.~~

The purpose of this policy is to establish a standardized, system-wide approach to managing the protection of information and Information Technology Resources to support core business needs and the provision of continuity and privacy at Westfield State University ("University") and establish ~~sanctions~~accountability for violations of this policy. This policy is intended to protect the users of the University's Information Technology Resources by ensuring a reliable and secure technology environment that supports the educational mission of the University. These resources are provided as a privilege to all Westfield State University employees, students, and authorized guests. The University seeks to ensure the integrity of Information Technology Resources made available to the user community, as such, to ensure these resources are secure from unauthorized access for those that utilize them. This policy is not intended to inhibit the culture of intellectual inquiry, discourse, academic ~~freedom~~freedom, or pedagogy. In general, the same ethical conduct that applies to the use of all University resources and facilities applies to the use of the University's Information Technology Resources.

SCOPE

This policy applies to all students, faculty, staff, volunteers, vendors, consultants, contractors, or others (herein afterwards referred to as "constituents") who use or have authorized access to University Information Technology Resources. This policy is supplemented by the policies of those networks to which the University is interconnected, including, but not limited to, the University of Massachusetts Information Technology Systems group, the Commonwealth of Massachusetts' Information Technology Division, UMass Online, etc. It covers all University information whether in hardcopy or electronic form and any systems which access, process, or have custody of business data. This policy also applies to any and all information, in any form and in any medium, network, internet, intranet, computing environments, as well as the creation, communication, distribution, storage and disposal of information.~~This policy applies to all students, faculty, and staff of the University, and to all other users who are authorized by the University to access the University's e-mail system.~~

Formatted: Indent: Left: 0", First line: 0"

DEFINITIONS

Distribution List: A distribution list refers to a facility in the e-mail system to enable ~~a large number of~~many ~~subscriber~~subscribers mail addresses to be reached through a single (list) name. (~~Ex. i.e.~~i.e., ~~fac/staff,~~ departmental list, FACSTAFF, UniCom).

Westfield State University's e-mail system: The University's e-mail system is a communication resource to enhance and facilitate the academic and administrative

Westfield State University

Policy concerning

APPROVED: December 2013

REVIEWED: August 2021

operations of the University. This includes any originating e-mails containing @westfield.ma.edu. Use of the system shall be to support these purposes and this policy.

For the purposes of this policy, "Information Technology Resources" means all computer, applications and communication facilities, services, data and equipment that are owned, managed, maintained, leased or otherwise provided by the University.~~*Information Technology Resources*: Information technology resources refers to all computer and communication facilities, services, data, and equipment that are owned, managed, maintained, leased, or otherwise provided by the University.~~

Formatted: Font: 11 pt

PUBLIC RECORD

E-mail, ~~whether or not~~whether created or stored on university-owned equipment may constitute a public record under Massachusetts' Public Records Law or be subjected to mandatory disclosure under other laws or regulations, including the rules compelling disclosure ~~during the course of~~during litigation. Users of the University's e-mail services should be aware that Massachusetts' Public Records Law and statutory and regulatory provisions prevent the University from guaranteeing complete protection of email, including personal e-mail residing on the University's information technology resources.

The messages, information and data carried by the e-mail system are the sole property of the University and the Commonwealth of Massachusetts. The University reserves the right to monitor and access those systems and their contents as they deem necessary, in accordance with the law and relevant collective bargaining agreement. No user of the University's e-mail system shall have a reasonable expectation of privacy in any e-mail.

Formatted: Font: (Default) Arial, 11 pt

USER OWNERSHIP AND RESPONSIBILITY

I. SECURITY AND CONFIDENTIALITY

A. Individuals with approved access to the University's e-mail system have the responsibility to maintain a confidential password, as well as the responsibility to regularly change their password, to protect the system from unauthorized access. The University will never ask for your password, and users should not provide this information to anyone.

B. Individuals with approved access to the e-mail system have the responsibility to log off and lock their computer or mobile device. This will prevent others from tampering with an account or accessing confidential material.

C. All messages should be treated as confidential by other employees and accessed only by the intended recipient unless necessary as a normal

Westfield State University
Policy concerning

APPROVED: December 2013

REVIEWED: August 2021

function of their job. Employees are not authorized to intentionally retrieve or read any e-mail messages that are not sent to them.

D. Never assume that e-mail is confidential. A message can easily be forwarded to another e-mail user, and anyone has potential access to read an e-mail message once it has been printed. Technical problems or human error may result in the unintended distribution of e-mail.

~~D.~~E. Phishing attacks and cyber fraud incidents have significantly increased over the past few years. Your university provided email account helps identify you to others and includes the security designed to help prevent these incidents. When conducting business as part of your employment at the ~~univesrity~~university, you must utilize your university email address (ending in @westfield.ma.edu) to ensure proper identity and compliance.

Formatted: List Paragraph, No bullets or numbering, Allow hanging punctuation, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Font Alignment: Auto

II. USAGE

A. The University's e-mail system is the official method of communication for the University. Only mailboxes with westfield.ma.edu suffixes are supported. Anyone who utilizes another e-mail system, or forwards e-mail from their university account to another account does so at their own ~~risk, and~~risk and is responsible for ensuring they are in receipt of all intended communications.

B. The University's e-mail system is intended to support the academic and administrative mission of the University. Users are expected to demonstrate a sense of responsibility in utilizing the email system to include maintaining professional etiquette in all e-mail communications.~~,~~
~~the e-mail system to include maintaining professional etiquette in all e-mail messages~~.

~~C.~~ Usage of the university e-mail system is also in accordance with the Social Media and Communication ~~guideline~~and the Distribution List guidelines.~~Attached to this policy are guidelines regarding the use of the e-mail system.~~

III. RETENTION

~~E-mail is backed up on a daily basis. Tapes are retained in an alternate, locked fire-proof location for 14 days before they are overwritten. Deleted items are retained in the system for 14 days and then moved to tape. Mailbox space is allocated to users on a disk availability basis and space allocation is reviewed by the Associate Director~~

Formatted: Font: 11 pt

Westfield State University

Policy concerning

APPROVED: December 2013

REVIEWED: August 2021

~~for Infrastructure services on an annual basis. Even when e-mail messages are deleted from the user's mailbox, copies of the files and messages may be automatically retained on back-up systems for an extended period of time.~~ Users are responsible for preserving their email in accordance with the Massachusetts Statewide Records Retention Schedule. ~~archiving and retaining e-mails on their computer. For more information, please refer to the Executive Office E-mail Retention Policy and Procedure located on mass.gov website at http://www.mass.gov/eohhs/gov/laws-regs/dds/policies/r-e-mail-retention-policy-and-procedure.html~~MA_Statewide_Records_Schedule_dec18.pdf (mma.org)

Formatted: Font: (Default) Arial, 11 pt

Formatted: Font: (Default) Arial, 11 pt

UNACCEPTABLE USES

It is unacceptable to use the University e-mail system as follows:

- for personal or private profit;
- In any way that violates University policy;
- In any way that violates local, state, or federal law;
- to send or receive, either across the University e-mail system or the Internet, any copyrighted materials, trade secrets, proprietary financial information, peer review committee reports and activities, or similar materials, or any information where exposure of that information to outside parties would have an adverse impact on the University or its employees, without prior approval;
- as a vehicle for unauthorized disclosure of confidential business or private facts concerning employees, students, or University-related business (authorized e-mail and e-mail attachments containing sensitive business information may be sent within the Westfield State University system on its secured network);
- for communications regarding commercial solicitations;
- for communications regarding political advertising, chain-letters, jokes, derogatory or inflammatory statements, and/or idle gossip.

ENFORCEMENT

Access to the e-mail system is a privilege and any misuse of the e-mail system may result in withdrawal of access to the system and disciplinary action up to and including termination~~, suspension or expulsion.~~.

This policy will be reviewed ~~bi-~~annually by the Chief Information Security Officer.

Westfield State University

Policy concerning

APPROVED: December 2013

REVIEWED: August 2021

~~GUIDELINES FOR THE USE OF ELECTRONIC MAIL (move to social media/communication guideline)~~

Formatted: Centered

~~*Appropriateness*~~

- ~~E-mail is not intended to replace face-to-face interaction. E-mail is one of many communication methods available at the University. Be sure e-mail is the appropriate medium for your message before sending it. Do not use e-mail to write something you would not say face-to-face or include in a memo. Remember that e-mail is a public record, and your message may be subject to disclosure.~~

Formatted: Centered, Indent: Left: 0", Hanging: 0.25", Space After: 0 pt, No bullets or numbering

- ~~When using global distribution lists, remember that most groups include a mix of staff and employees. Know who is in the group you intend to send the message to and be sensitive to the intended recipients.~~
- ~~When responding to a message sent to you via a global distribution list, be careful not to use "Reply All" unless appropriate and necessary.~~

~~*E-mail Etiquette*~~

- ~~Treat e-mail messages as business correspondence. Be professional and careful about what you say about others. E-mail is easily (and often inadvertently) forwarded. Avoid using informal language and clearly separate opinion from non-opinion.~~
- ~~Be careful when using humor and sarcasm. Without face-to-face communication, your message may be misinterpreted.~~
- ~~Think before you write. Once sent, a message cannot be retracted. Identify yourself and your affiliations clearly and avoid responding when you are emotional.~~
- ~~Use mixed case. Do not write in all caps or all small letters. Writing in all upper-case letters is generally considered to be shouting in electronic correspondence.~~
- ~~Consider including your phone extension in the message. This allows the recipient to call you directly with a response if they prefer.~~
- ~~Limit each e-mail message to one topic and always use a clear identifier in the subject line of each message which reflects the content of the message. Use common abbreviations, when possible, but refrain from using acronyms that would be confusing or annoying to the reader.~~
- ~~E-mail messages should be brief and to the point, meant to be read off the screen in thirty seconds or less. Use attachments for long documents. However, do not create an attachment for brief correspondence; instead, create a brief e-mail (for example, do not create a Word document to communicate a meeting cancellation).~~
- ~~When sending an attachment, always include a one-line description of what the attachment contains, giving the addressee the option of opening it or not. If sending multiple attachments, identify the content of each attachment.~~
- ~~Be judicious with use of CC's.~~
- ~~You may also want to reference the University's Identity Guidelines Manual produced by the Marketing Department or the Writer's Style Guide.~~

Westfield State University

Policy concerning

APPROVED: December 2013

REVIEWED: August 2021

- When forwarding a message, remember that it is acceptable, and sometimes preferable, to delete any information that is irrelevant to the message you want to send or to cut and paste the pertinent information into a new e-mail.

Responsible E-mail Use

- Check your mailbox frequently. Respond to e-mail messages as soon as possible after receiving them. If you think the importance of the message justifies it, immediately acknowledge to the sender that you have received the message, even though you will send a longer reply later.
- ***Be cautious about sending time sensitive material to which you need an immediate answer. Do not expect an instant response to your messages.*** Not all users are "on-line" every day. Use the "return receipt" option to ensure critical messages have been received.
- E-mail is a transitory communication tool which should be kept current and up to date. Mail and working documents that have exceeded their practical life span should be deleted. Delete unwanted messages immediately and keep messages remaining in your mailbox to a minimum and archive messages regularly.
- When using e-mail as a decision-making tool, do not assume acceptance when a person does not respond.

Formatted: Font: (Default) Arial

Distribution List Guidelines

ROLES

1. Constituents - each constituent is responsible for understanding and complying with university policies, standards, and procedures.

2. The Office of Information and Instructional Technology (OIT)
    a. Responsible for the maintenance and/or setup of distribution lists unless otherwise noted.
    b. Ensuring no individual is authorized to approve their own access.
    c. Establish, modify, and terminate user accounts in accordance with Access Control Guidelines.

3. Chief Information Security Officer (CISO)
    a. Responsible for the oversight, management, coordination, update, and distribution of this guideline.
    b. Holds the authority to grant or remove access to any/all distribution lists
    c. Support the implementation and communication of the Passwords Policy and supporting guidelines and procedures.
    d. Ensure adherence to the E-Mail Policy (0550), supporting guidelines and procedures through education and controls.
    e. Establish, modify, and terminate access in accordance with the Information Security Policy and Access Control Guidelines.

PROCEDURES

1. Distribution List Creation
    a. Users may request a distribution list to be created by submitting a Support Desk ticket
    b. All lists will be visible in the global address list and have no restrictions on sending unless otherwise specifically stated
    c. All distribution lists requested by departments or individual will be assigned a distribution list manager who;
        1. Is responsible to manage the membership of the distribution list
        2. Should the distribution list manager role change, the department head/chair shall create a Support Desk ticket to change the distribution list manager ownership
        3. Failure to manage the list will result in removal of the distribution list

2. Specialized Distributions Lists
    a. UniCom
        1. Official business-related communication distribution list for the campus.
        2. Includes all faculty and staff (full time and part time) of the university
        3. Membership required
        4. This is a closed distribution list and requires the approval of the CISO to send to the list
        5. Anyone requesting send permissions to UniCom should open a Support Desk ticket

    b. FACSTAFF
        1. Unofficial communication distribution list for the campus.
        2. Includes all faculty and staff of the university
        3. Membership is automatic upon creation; however, users may opt out or in at any time by;
            i. Technology support site under DIY
            ii. Submitting a Support Desk ticket

    c. Students
        1. Official business-related communication distribution list for communicating with all students.
        2. Includes all students (day, CGCE, fulltime and parttime) of the University.
        3. Membership required
        4. This is a closed distribution list and requires the approval of the CISO to send to the list
        5. Anyone requesting send permissions to Students should open a Support Desk ticket

d. Union Distribution Lists
    1. Official communication distribution lists for the members of the unions on campus.
    2. These are closed distribution lists and requires the approval of the CISO and the union President, or designee, to send to the list. Anyone requesting send permissions to the Union Distribution lists email must either;
        i. Email the union President **AND** the CISO with their request
        ii. Open a Support Desk ticket requesting the send permissions which must be approved by both the union President and the CISO
    3. Includes all members of each as union upon hire
    4. Each union President shall designate a distribution list manager who;
        i. Is responsible to manage the membership of the distribution list
        ii. Should the distribution list manager role change, the union President shall create a Support Desk ticket to change the distribution list manager ownership

3. Any exceptions to these guidelines must be approved in writing by the Chief Information Security Officer.

4. Failure to comply with these guidelines and its supporting policies may be subject to disciplinary action up to an including termination.

REVIEW

These guidelines shall be reviewed annually by the Chief Information Security Officer

Date	Version	Updated by	Description of Changes
9-14-2021	1.0	Alan Blair	Draft
10-7-2021	1.1	Alan Blair	Updated Draft
11-10-2021	1.2	Alan Blair	Updated draft with CBU reps

SOCIAL MEDIA GUIDELINE FOR FACULTY, STAFF, AND STUDENTS

INTRODUCTION

Westfield State University embraces the use of social media as an effective means to communicate and build relationships with current and prospective students, alumni, faculty/staff, parents/families of students, and community members.

The following guideline outlines appropriate use of social media by faculty, staff, and students at Westfield State University. The University's social media accounts are official publications of the University.

GUIDELINE FOR USE OF SOCIAL MEDIA ON BEHALF OF WESTFIELD STATE UNIVERSITY

Use of the Westfield State University Name and Logo

- The Westfield State University logo may only be used to identify the University's identity, its programs, and its services.
- The development and use of any other logo, mark and/or symbol is prohibited. The University logo may not be combined with any other feature—including but not limited to other logos, words, graphics or symbols.
- The shape, proportion or color of the University logo may not be altered in any way, and the logo may not be redrawn or altered.
- Do not use the University's name, logos, or accounts to promote or endorse products, political parties/candidates, or personal work/opinions.
- If you have any questions regarding the Westfield State University graphic identity or need to obtain logo art, typefaces or print templates, contact the Marketing Department.

Utilize On-Campus Marketing Resources

- Consistency with branding and high-quality content influence how audiences perceive Westfield State, both on campus and in the public.
- Personal artwork or images must not be used for posts on University-related accounts.
- If you are seeking photography or graphic design for official University campaigns, file a Work Request Form with the Marketing Department.

Maintain Confidentiality

- Do not post or share information about the University or personal, medical, or financial information about students, alumni, faculty, or staff.
- Do not post or comment on legal matters or ongoing investigations.

Emergency Communications

- All social media communication related to an emergency or closing/cancellation will be generated by the Director of Campus Communication, and will be posted on the official University Facebook and Twitter accounts.
- University-related accounts may not make posts regarding an emergency or closing/cancellation, with the exception of sharing posts from the official University accounts.
- During an emergency, scheduled social media posts must be paused and administrators must monitor conversation regarding the situation.

Media Inquiries

- Any media inquiries must be directed to the Director of Campus Communication and/or the Communications Specialist in Public Affairs.

University Announcements

- All major announcements regarding Westfield State University must come from the official University accounts, unless the announcement pertains to a specific department or office. In such a case, the Director of Campus Communication will designate the release of news.
- Administrators of University-related accounts can share posts regarding announcements from official accounts.

Access of University Accounts

- All University-related social media accounts must be linked to a department email account.
- More than one employee must have administrative access to each account.
- Administrators of University-related accounts must provide the Social Media and Digital Content Coordinator with account login credentials. If changes to credentials are made, updates must be provided to the Social Media and Digital Content Coordinator
- Administrative access will be terminated upon an employee's separation from employment, reassignment to a different position, or for disciplinary reasons.
- If a University-related account is linked to an individual person, that person relinquishes all rights to the account, unless they work with the Social Media and Digital Content Coordinator to transfer ownership of the account.

Respect Copyright and Fair Use

- Use of third-party copyrighted or trademarked material or intellectual property rights of others is prohibited and can impact the University

Be Respectful

- Maintain a neutral, unbiased voice when making posts or comments.
- What you say in posts and share through photos should reflect the University brand in a positive light.

Do Not Create or Endorse Fundraising Campaigns

- Fundraising efforts of any kind must not be created, shared, or promoted through University-related accounts.

Respect University Time and Property

- Employees should use University computers/devices and their work time for only University-related business.

GUIDELINE FOR PERSONAL USE OF SOCIAL MEDIA BY FACULTY/STAFF AND STUDENTS

You are Responsible for What You Post

- Be mindful about the content that you post on social media – users are responsible for what they post on their own accounts and on accounts of others.
- Social media users can be held liable for comments and/or deemed to be copyright infringement, defamatory, or threatening.
- Do not share personal information about others unless you have their permission.

An Affiliation with Westfield State University on Your Account Can Impact the University

- If you identify your affiliation with the University in your account or in comments, users will naturally associate you with the University.
- All posts, comments, and actions made on social media can impact the reputation and brand of the University.
- Consider including a statement on your account that indicates that your views are personal and are not on behalf of the University.

BEST PRACTICES FOR MANAGING A UNIVERSITY-RELATED SOCIAL MEDIA ACCOUNT

Be Accurate

- Ensure that your content is an accurate representation of your department, organization, and the University as a whole.
- Always double check spelling and grammar and if you make an error, correct it quickly. If necessary, verify information with a source prior to posting.

Be Active

- A social media presence requires adequate planning and communication in order to be successful.
- University-related accounts must be updated at least weekly, if not daily, all year-round.
- Not every group or organization will generate enough content to sustain a page—using the main University channels to promote your program may be the best approach.
- It's not advisable to try to maintain a presence on every platform. A better approach is to start on one platform and focus on posting consistent, valuable content.
- If a University-related account is inactive for six months or more, the Social Media and Digital Content Coordinator will request deactivation of the account.

Monitor Comments

- Comments are an essential component of social media. Understand that not all comments will be positive, and respond to negative comments professionally and by providing information that may help resolve the issue.
- Monitor your accounts for inappropriate or offensive remarks, but avoid deleting comments.
- If you encounter issues or threats related to students, faculty/staff or the campus, direct them to Public Safety.

CREATING UNIVERSITY-RELATED SOCIAL MEDIA ACCOUNTS

1. Define your goals and scope of the account.
    a. Who is your audience?
    b. Can you devote at least an hour per day creating content and managing the account?
    c. What content will you create?
    d. What platform(s) will be used?
2. Arrange a meeting with the Social Media and Digital Content Coordinator to discuss your goals.
3. If you aim to create a Facebook page, the Social media and Digital Content Coordinator will create the page and provide administrative access to the designated faculty/staff member(s). For any other platforms, login information must be shared with the Social Media and Digital Content Coordinator.
    a. The Social Media and Digital Content Coordinator will not manage the account, but is simply a backup if login information is forgotten.
    b. Accounts can only be registered by faculty/staff using department university email accounts.
4. Submit a Marketing Request for help designing or selecting a profile photo, cover photo, or any other images for the account.
5. Register for the account and start posting content. Only follow University-related accounts and other appropriate users, nothing that reflects negatively on the University

6. Measure success using built-in insight tools. Contact the Social Media and Digital Content Coordinator with questions or assistance.

ENFORCEMENT AND REVIEW

The University reserves the right to review, remove, and deny content that is considered inappropriate or inconsistent with posting guidelines and practices.

Content that the University determines is offensive, threatening, libelous, defamatory, obscene, aligns with hate speech, or is otherwise objectionable or violates any party's intellectual property will not be tolerated and is subject to be removed.

Requests for exemption to this guideline should be directed to the Social Media and Digital Content Coordinator and accompanied by written justification for the exemption request.

This policy will be reviewed annually by the Social Media and Digital Content Coordinator, the Director of Marketing, and the Director of Campus Communications.