

**BOARD OF TRUSTEES
FINANCE AND FACILITIES COMMITTEE**

Leonard D. Schiavone, Chair

James B. Greene, Vice Chair

All Trustees are Members

James P. Tressel, *Ex-Officio*

**Tuesday, March 15, 2016
2:00 p.m. or immediately following
previous meeting**

**Tod Hall
Board Meeting Room**

AGENDA

A. Disposition of Minutes for Meetings Held December 3, 2015; and December 16, 2015

B. Old Business

C. Committee Items

1. Consent Agenda Items*

**a. Resolution to Modify Reduction/Refund of Tuition and Fees Policy, Tab 1
3356-3-02.1 (Previous Policy Number 3002.01)**

Neal McNally, Vice President for Finance and Business Operations, will report.

**b. Resolution to Modify Acceptable Use of University Technology Resources Tab 2
Policy, 3356-4-09 (Previous Policy Number 4009.01)**

Neal McNally, Vice President for Finance and Business Operations, will report.

**c. Resolution to Modify Cellular Equipment Usage Policy, 3356-4-12 Tab 3
(Previous Policy Number 4011.01)**

Neal McNally, Vice President for Finance and Business Operations, will report.

2. Finance and Facilities Action Item

**a. Resolution to Rescind the Previously Approved Room Rental Rates for the Tab 4
University Courtyard Apartments**

Eddie Howard, Associate Vice President for Student Experience, will report.

*Items listed under the Consent Agenda require Board approval; however they may be presented without discussion as these items include only non-substantive changes.

3. Finance and Facilities Discussion Items

- a. Quarterly Update on FY 2016 Operating Budget** **Tab 5**
Neal McNally, Vice President for Finance and Business Operations, will report.
- b. Planning and Construction Projects Update** **Tab 6**
John Hyden, Executive Director of Facilities and Support Services, and Rich White, Associate Director of Planning and Construction, will report.
- c. Report of Audit Subcommittee**
A verbal report of the Audit Subcommittee will be presented. Leonard D. Schiavone will report.
- d. Report of Investment Subcommittee**
A verbal report of the Investment Subcommittee will be presented. James B. Greene will report.

D. New Business

E. Adjournment



Explanation of Modifications to *University Policy*:

**3356-3-02.1 Reduction/Refund of Tuition and Fees
(Previous Policy Number 3002.01)**

This policy was reviewed as part of the regular 5-year cycle and was updated to clarify when a refund or reduction in student tuition or fees may be appropriate. The attached redline version illustrates the changes the policy has undergone based upon this review.

**Board of Trustees Meeting
March 16, 2016
YR 2016-**



**RESOLUTION TO MODIFY
REDUCTION/REFUND OF TUITION AND FEES POLICY, 3356-3-02.1
(PREVIOUS POLICY NUMBER 3002.01)**

WHEREAS, University Policies are reviewed and reconceptualized on an ongoing basis; and

WHEREAS, this process can result in the modification of existing policies, the creation of new policies, or the deletion of policies no longer needed; and

WHEREAS, action is required by the Board of Trustees prior to replacing and/or implementing modified or newly created policies, or to rescind existing policies; and

WHEREAS, the Reduction/Refund of Tuition and Fees policy has been reviewed pursuant to the five-year review cycle, and formatted in accordance with Policy 3356-1-09, Development and Issuance of University Policies.

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby approve the modification of the University Policy Reduction/Refund of Tuition and Fees Policy, policy number 3356-3-02.1 (Previous Policy Number 3002.01), shown as Exhibit __ attached hereto. A copy of the policy indicating changes to be made is also attached.

**Board of Trustees Meeting
March 16, 2016
YR 2016-**

3356-3-02.1 Reduction/refund of tuition and fees.

Previous Policy Number: 3002.01
Responsible Division/Office: ~~Financial Services~~ and Business Operations
Responsible Officer: Vice President for Finance and
~~Administration~~ Business Operations
Revision History: March 1998; March 2007; March 2011; March 2016
Board Committee: Finance and Facilities
Effective Date: ~~March 18, 2011~~ March 16, 2016
Next Review: 201521

- (A) Policy statement. The board of trustees of Youngstown state university shall review and approve the schedule of student tuition and fees. This schedule and the associated refund procedures will be published in university “Bulletins” and other official university documents.
- (B) Parameters.
- (1) A full or partial reduction of the instructional, general, information services, performance, music, college, lab and materials fees, and the nonresident surcharge will be provided for all withdrawals or reductions which take place during a specified period of time outlined in the current university “Undergraduate” and “Graduate Bulletins,” or as modified by action of the board of trustees.
 - (2) Students suspended or dismissed from the university for non-academic reasons are not entitled to any reduction of fees unless extenuating circumstances are demonstrably present, such as a medical condition as verified by a physician. †
- (C) Procedures.
- (1) To receive a reduction of fees, a student must officially withdraw or complete an official change of registration.
 - (2) Students who withdraw or reduce hours after the specified refund period, and who do so for reasons beyond their control (~~physician’s request~~ such as for a medical issue, induction into

- military service, change in work shifts or transfer of employment; ~~or other special circumstances~~), may request to have their fees reviewed in accordance with the fees and charges appeals board process. If approved, the fees may be revised on a prorated basis.
- (3) Students withdrawing from all classes as a result of being called to active military service are eligible for a full reduction of fees. Students must officially withdraw and must provide the fees and charges appeals board with supporting documentation validating the withdrawal.
 - (4) Individuals seeking additional information on the reduction/refund of fees and charges should refer to the current Youngstown state university "Undergraduate Bulletin," "Graduate Bulletin," ~~and the office of student accounts and university receivables website at~~ <http://www.yosu.edu/vpadmin/studaeets/> or by calling the office of the university bursar at 330-941-1311.

3356-3-02.1 Reduction/refund of tuition and fees.

Previous Policy Number: 3002.01
Responsible Division/Office: Finance and Business Operations
Responsible Officer: Vice President for Finance and
Business Operations
Revision History: March 1998; March 2007; March 2011; March
2016
Board Committee: Finance and Facilities
Effective Date: March 16, 2016
Next Review: 2021

- (A) Policy statement. The board of trustees of Youngstown state university shall review and approve the schedule of student tuition and fees. This schedule and the associated refund procedures will be published in university "Bulletins" and other official university documents.
- (B) Parameters.
- (1) A full or partial reduction of the instructional, general, information services, performance, music, college, lab and materials fees, and the nonresident surcharge will be provided for all withdrawals or reductions which take place during a specified period of time outlined in the current university "Undergraduate" and "Graduate Bulletins," or as modified by action of the board of trustees.
 - (2) Students suspended or dismissed from the university for non-academic reasons are not entitled to any reduction of fees unless extenuating circumstances are demonstrably present, such as a medical condition as verified by a physician.
- (C) Procedures.
- (1) To receive a reduction of fees, a student must officially withdraw or complete an official change of registration.
 - (2) Students who withdraw or reduce hours after the specified refund period, and who do so for reasons beyond their control (such as for a medical issue, induction into military service, change in

work shifts or transfer of employment), may request to have their fees reviewed in accordance with the fees and charges appeals board process. If approved, the fees may be revised on a prorated basis.

- (3) Students withdrawing from all classes as a result of being called to active military service are eligible for a full reduction of fees. Students must officially withdraw and must provide the fees and charges appeals board with supporting documentation validating the withdrawal.
- (4) Individuals seeking additional information on the reduction/refund of fees and charges should refer to the current Youngstown state university Undergraduate Bulletin, Graduate Bulletin, or by calling the office of the university bursar at 330-941-1311.



Explanation of Modifications to *University Policy*:

**3356-4-09 Acceptable Use of University Technology Resources
(Previous Policy Number 4009.01)**

This policy was reviewed and has been modified to:

1. Makes YSU email an official means of University communications
2. Streamlines file access procedure of former employees

The attached redline version illustrates the changes the policy has undergone based upon the review.

**Board of Trustees Meeting
March 16, 2016
YR 2016-**

**RESOLUTION TO MODIFY
ACCEPTABLE USE OF UNIVERSITY TECHNOLOGY
RESOURCES POLICY, 3356-4-09
(PREVIOUS POLICY NUMBER 4009.01)**

WHEREAS, University Policies are reviewed and reconceptualized on an ongoing basis; and

WHEREAS, this process can result in the modification of existing policies, the creation of new policies, or the deletion of policies no longer needed; and

WHEREAS, action is required by the Board of Trustees prior to replacing and/or implementing modified or newly created policies, or to rescind existing policies; and

WHEREAS, the Acceptable Use of University Technology Resources policy has been reviewed pursuant to the five-year review cycle, and formatted in accordance with Policy 3356-1-09, Development and Issuance of University Policies.

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby approve the modification of the University Policy Acceptable Use of University Technology Resources Policy, policy number 3356-4-09 (Previous Policy Number 4009.01), shown as Exhibit __ attached hereto. A copy of the policy indicating changes to be made is also attached.

3356-4-09 Acceptable use of university technology resources.

Previous Policy Number: 4009.01
Responsible Division/Office: Information Technology Services
Responsible Officer: [Vice President](#) for Finance and ~~Facilities~~ [Business Operations](#)
Revision History: August 1999; November 2010; December 2012; [March 2016](#)
Board Committee: Finance and Facilities
Effective Date: ~~December 14, 2012~~ [March 16, 2016](#)
Next Review: ~~2017~~ [21](#)

(A) Policy statement. University technology resources are provided to the university community to support its academic and administrative functions in accordance with its teaching, research, and service missions. These resources are intended to be used for the educational and business purposes of the university in compliance with this policy.

(B) Scope. This policy applies to all users and uses of university-owned technology resources (including those acquired through grant processes) as well as to any non-YSU and/or remote technology devices while connected to the YSU network.

(BC) ~~General Statement.~~ Parameters.

- (1) Technology resources (computing, networking, data and network services) are provided to the university community in order to fulfill the mission of the university.
- (2) While the university recognizes the importance of academic freedom and freedom of expression, as a public employer, the university also has a responsibility to comply with all federal and state laws and regulations, as well as the obligation to fulfill its mission.
- (3) Use of university-owned technology to access resources other than those supporting the academic, administrative, educational, research and services missions of the university or for more than limited, responsible personal use conforming to this policy is

prohibited.

- (4) Technology resources provided by the university are the property of the university. University-owned technology is not intended to supersede the need for technology purchases for personal purposes.
- (5) As the university is a public entity, information in an electronic form may also be subject to disclosure under the Ohio public records act to the same extent as if they existed on paper. All use is subject to the identification of each individual using technology resources (authentication).
- (6) Use of technology is subject to the requirements of legal and ethical behavior and is intended to promote a productive educational and work environment.

([GD](#)) ~~Policy:~~ [User Requirements](#). All users of the university-owned technology resources (computing, networking and data), regardless of affiliation with the university, must:

- (1) Use only those technology resources that they are authorized to use and use them only in the manner and to the extent authorized.
- (2) Protect the confidentiality, integrity and availability of technology resources.
- (3) Comply with all federal, Ohio, and other applicable law as well as applicable regulations, contracts, and licenses.
- (4) Comply with all applicable policies at Youngstown state university (~~YSU~~).
- (5) Respect the right of other technology users to be free from harassment or intimidation.
- (6) Respect copyrights, intellectual property rights, and ownership of files and passwords.
- (7) Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.

- (8) Respect the finite capacity of technology resources and limit use so as not to consume an unreasonable amount of or abuse those resources or to interfere unreasonably with the activity of other users or to disrupt the authorized activities of the university.
- (9) Limit personal use of university technology resources so that such use does not interfere with one's responsibilities to the university.
- (10) Not attempt to circumvent information technology security systems or the university "Information Technology Security Manual."
- (11) Not use any radio spectrum space on any YSU-owned or YSU-occupied property, unless it is part of an approved wireless services deployment by the university.
- (12) Not use technology resources for personal commercial purposes or for personal financial or other gain unless specifically approved by the university.
- (13) Not state or imply that they speak on behalf of the university without authorization to do so and not use university trademarks and logos without authorization to do so.

~~(D) — Scope. This policy applies to all users and uses of university-owned technology resources (including those acquired through grant processes) as well as to any non-YSU and/or remote technology devices while connected to the YSU network.~~

~~(E) User responsibilities.~~

- (1) By accepting employment, being admitted as a student, or asking for any guest technology resource privileges, users implicitly agree to adhere to this policy and agree to [adhere to](#) the university "Information Technology Security Manual."
- (2) Users are responsible for any activity performed using their usernames and passwords except when account security is compromised by actions beyond the user's control.

- (3) Users are responsible for any activity performed on university-owned technology devices assigned to them except when the device is compromised by actions beyond the user's control.
 - (4) There is no expectation of personal privacy when using university resources. (See paragraph F of this rule.)
 - (5) Potential violations regarding use of technology resources should be reported to the appropriate ~~supervisor(s) or manager(s) or~~ information [technology services manager\(s\) or information security officer](#).
 - (6) Users are responsible for ensuring that critical data are backed up and available to be restored for systems not administered by information systems technology. This includes critical information contained on technology devices oriented to individual use (e.g., desktops, laptops, smart phones, and similar such devices).
 - (7) Users are responsible for maintaining data in compliance with the university records retention plan.
 - (8) Users are responsible for ensuring that sensitive information to which they have access is guarded against theft. (See rule 3356-4-13 of the Administrative Code for more information.)
 - (9) Personal use of computing resources not otherwise addressed in this policy or these procedures will generally be permitted if such use does not consume a significant amount of resources, does not interfere with the performance of an individual's job or other university responsibilities, and is otherwise in compliance with university policies.
- (F) No expectation of privacy.
- (1) The university does not routinely monitor specific individual end-user usage of its technology resources. However, the university does routinely monitor technology resource usage in the normal operation and maintenance of the university's computing, network and data resources. This monitoring includes the caching and backing up of data and communications, the logging of activity,

the monitoring of general usage patterns, the scanning of systems and networks for anomalies and vulnerabilities, the filtering of malicious traffic, and other activities that are necessary for the rapid and efficient delivery of services. Technology users should be aware that there is no expectation of privacy associated with the use of university technology resources.

- (2) When authorized by the office of the general counsel, the university may also specifically monitor the activity and accounts of individual end-users of university technology resources, including login sessions, file systems, and communications.
- (3) When authorized by the appropriate university ~~executive~~ administrator (president, ~~or~~ vice president, or associate vice president reporting to the president), the university may access active end-user accounts, files, or communications used for university business when needed by a supervisor or assigned personnel for university business and the end-user is unavailable. For inactive end-users, such as retirees or terminated employees, the end-user's former supervisor or the individual currently holding the supervisor position may request access. For inactive student end-users the provost may authorize access. For all other inactive end-users, the general counsel may authorize access.
- (4) The university, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate university personnel, student conduct, or law enforcement agencies and may use those results in appropriate university disciplinary proceedings.
- (5) Personal computing devices:
 - (a) Personal computing devices (laptops, desktops, tablets, cellular phones) are restricted to the campus wireless network or the residence hall network.
 - (b) No personal computing devices will be allowed to connect to the wired campus network (excluding the residence hall network).
 - (c) Personal computing devices must comply with university

“Information Security Practice” when using the campus wireless network or other provided university technology resource.

- (d) Personal computing devices used to conduct university business are subject to public records requests.
- (e) Personal hubs, routers, switches, or wireless access points are prohibited from being connected to either the university’s wired or wireless network.

(G) Email.

- (1) Email is an official means for communication at the university. Students, faculty and staff are expected to check their official email address on a frequent and consistent basis in order to stay current with university communications.
- (2) Only email sent to the university email address of record will be supported.
- (3) Email may not be automatically forwarded to off-campus computer accounts from a university assigned email account.

- (GH) Security. The university employs various measures (i.e., the university’s “Information Security Practice”) to protect the security of information technology resources and user accounts; however, users should be aware that the university cannot provide good security without user participation. Users should increase their technology security awareness and fully employ access restrictions for their accounts, including using strong passwords, guarding passwords diligently and changing passwords regularly to help safeguard their use of technology.
- (HI) Additional policy ramifications. Users must abide by all applicable restrictions, whether or not they are built into the computing system, network or information resources and whether or not they can be circumvented by technical or other means. Individuals who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those states and countries and the rules and policies of those technology systems and information resources.

(H) Examples of unacceptable use:

- (1) As a further aid to policy compliance, the following non-exhaustive list is provided of activities that are prohibited.
 - (a) Using technology resources to engage in fraud, defamatory, abusive, unethical, indecent, obscene, pornographic and/or unlawful activities is prohibited.
 - (b) Using technology resources to procure, solicit, or transmit material that is in violation of sexual, racial or other harassment or hostile workplace laws is prohibited.
 - (c) Any form of harassment by electronic means (e.g., email, web access, phone, paging), whether through language, content, frequency or size of messages is prohibited.
 - (d) Making fraudulent offers of products, items or services using any university technology resource is prohibited.
 - (e) Using technology resources for unauthorized or inappropriate financial gain, unauthorized solicitation, or activities associated with a for-profit business, or engaging in an activity that involves a conflict of interest. (Refer to rules 3356-7-01 and 3356-7-19 of the Administrative Code.)
 - (f) Creating or forwarding chain letters, Ponzi, or other pyramid schemes is prohibited.
 - (g) Broadcasting of unsolicited mail or messages is prohibited. Examples include chain letters, virus hoaxes, spam mail, and other email schemes that may cause excessive network traffic. Sending large numbers of electronic mail messages for official university purposes necessitates following the university's procedures for the electronic distribution of information.
 - (h) Sending junk mail or advertising material to individuals who did not specifically request such material (email spam)

is prohibited.

- (i) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed is prohibited.
 - (j) Unauthorized copying and downloading of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and films and the installation of any copyrighted software for which an active license has not been procured is prohibited.
 - (k) Circumventing user authentication or security of any host, network or account is prohibited. This includes, but is not limited to, monitoring by use of keylogging or session logging.
 - (l) Revealing your account password to others or allowing use of your account by others is prohibited. This prohibition extends to family, other household members, friends and/or co-workers.
 - (m) Attempting to log onto another user's account (secured or otherwise) is prohibited.
 - (n) Sending electronic communications in such a way that masks the source or makes it appear to come from another source is prohibited.
 - (o) Personal use beyond limited responsible use is prohibited.
- (2) [Exemptions](#). Individual university staff may be exempted from these restrictions on a case-by-case basis (with written authorization according to the university "Information Security Practice") in the course of performing legitimate job responsibilities.

- (3) Passwords. Special procedures exist and must be followed to ensure that accounts for employees are secured with passwords known to only the account holder, ~~but~~ Passwords may be changed at the request of the area supervisor and approved by the supervisor's vice president or the president.
- (4) Under no circumstances is an employee of Youngstown state university authorized to engage in any activity that is unethical or illegal under local, state or federal law while utilizing university-owned resources.

(~~H~~K) Enforcement.

- (1) The office of the chief technology officer may suspend and/or restrict either an individual's or a device's access to the university network resource if:
 - (a) It is deemed necessary to maintain the security or functionality of the network resource.
 - (b) It is deemed necessary to protect the university from potential liability.
 - (c) The account, system, or device is believed to have been either compromised or is in violation of this policy.
- (2) The office of the chief technology officer must immediately report the enforcement action and the justification for the action to the associate vice president of student experience, vice president for finance and business operations, or provost (or their designee), as applicable. The university may permanently suspend all technology access of anyone using the university network resource until due process has been completed by student conduct, employee administrative discipline and/or law enforcement agencies.

3356-4-09 Acceptable use of university technology resources.

Previous Policy Number: 4009.01
Responsible Division/Office: Information Technology Services
Responsible Officer: Vice President for Finance and Business
Operations
Revision History: August 1999; November 2010; December 2012;
March 2016
Board Committee: Finance and Facilities
Effective Date: March 16, 2016
Next Review: 2021

- (A) Policy statement. University technology resources are provided to the university community to support its academic and administrative functions in accordance with its teaching, research, and service missions. These resources are intended to be used for the educational and business purposes of the university in compliance with this policy.
- (B) Scope. This policy applies to all users and uses of university-owned technology resources (including those acquired through grant processes) as well as to any non-YSU and/or remote technology devices while connected to the YSU network.
- (C) Parameters.
- (1) Technology resources (computing, networking, data and network services) are provided to the university community in order to fulfill the mission of the university.
 - (2) While the university recognizes the importance of academic freedom and freedom of expression, as a public employer, the university also has a responsibility to comply with all federal and state laws and regulations, as well as the obligation to fulfill its mission.
 - (3) Use of university-owned technology to access resources other than those supporting the academic, administrative, educational, research and services missions of the university or for more than limited, responsible personal use conforming to this policy is

prohibited.

- (4) Technology resources provided by the university are the property of the university. University-owned technology is not intended to supersede the need for technology purchases for personal purposes.
 - (5) As the university is a public entity, information in an electronic form may also be subject to disclosure under the Ohio public records act to the same extent as if they existed on paper. All use is subject to the identification of each individual using technology resources (authentication).
 - (6) Use of technology is subject to the requirements of legal and ethical behavior and is intended to promote a productive educational and work environment.
- (D) User Requirements. All users of the university-owned technology resources (computing, networking and data), regardless of affiliation with the university, must:
- (1) Use only those technology resources that they are authorized to use and use them only in the manner and to the extent authorized.
 - (2) Protect the confidentiality, integrity and availability of technology resources.
 - (3) Comply with all federal, Ohio, and other applicable law as well as applicable regulations, contracts, and licenses.
 - (4) Comply with all applicable policies at Youngstown state university (“YSU”).
 - (5) Respect the right of other technology users to be free from harassment or intimidation.
 - (6) Respect copyrights, intellectual property rights, and ownership of files and passwords.
 - (7) Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.
 - (8) Respect the finite capacity of technology resources and limit use so

as not to consume an unreasonable amount of or abuse those resources or to interfere unreasonably with the activity of other users or to disrupt the authorized activities of the university.

- (9) Limit personal use of university technology resources so that such use does not interfere with one's responsibilities to the university.
 - (10) Not attempt to circumvent information technology security systems or the university "Information Technology Security Manual."
 - (11) Not use any radio spectrum space on any YSU-owned or YSU-occupied property, unless it is part of an approved wireless services deployment by the university.
 - (12) Not use technology resources for personal commercial purposes or for personal financial or other gain unless specifically approved by the university.
 - (13) Not state or imply that they speak on behalf of the university without authorization to do so and not use university trademarks and logos without authorization to do so.
- (E) User responsibilities.
- (1) By accepting employment, being admitted as a student, or asking for any guest technology resource privileges, users implicitly agree to adhere to this policy and agree to the university Information Technology Security Manual.
 - (2) Users are responsible for any activity performed using their usernames and passwords except when account security is compromised by actions beyond the user's control.
 - (3) Users are responsible for any activity performed on university-owned technology devices assigned to them except when the device is compromised by actions beyond the user's control.
 - (4) There is no expectation of personal privacy when using university resources. (See paragraph F of this rule.)

- (5) Potential violations regarding use of technology resources should be reported to the appropriate information technology services manager(s) or information security officer.
 - (6) Users are responsible for ensuring that critical data are backed up and available to be restored for systems not administered by information systems technology. This includes critical information contained on technology devices oriented to individual use (e.g., desktops, laptops, smart phones, and similar such devices).
 - (7) Users are responsible for maintaining data in compliance with the university records retention plan.
 - (8) Users are responsible for ensuring that sensitive information to which they have access is guarded against theft. (See rule 3356-4-13 of the Administrative Code for more information.)
 - (9) Personal use of computing resources not otherwise addressed in this policy or these procedures will generally be permitted if such use does not consume a significant amount of resources, does not interfere with the performance of an individual's job or other university responsibilities, and is otherwise in compliance with university policies.
- (F) No expectation of privacy.
- (1) The university does not routinely monitor specific individual end-user usage of its technology resources. However, the university does routinely monitor technology resource usage in the normal operation and maintenance of the university's computing, network and data resources. This monitoring includes the caching and backing up of data and communications, the logging of activity, the monitoring of general usage patterns, the scanning of systems and networks for anomalies and vulnerabilities, the filtering of malicious traffic, and other activities that are necessary for the rapid and efficient delivery of services. Technology users should be aware that there is no expectation of privacy associated with the use of university technology resources.
 - (2) When authorized by the office of the general counsel, the

university may also specifically monitor the activity and accounts of individual end-users of university technology resources, including login sessions, file systems, and communications.

- (3) When authorized by the appropriate university administrator (president, vice president, or associate vice president reporting to the president), the university may access active end-user accounts, files, or communications used for university business when needed by a supervisor or assigned personnel for university business and the end-user is unavailable. For inactive end-users, such as retirees or terminated employees, the end-user's former supervisor or the individual currently holding the supervisor position may request access. For inactive student end-users the provost may authorize access. For all other inactive end-users, the general counsel may authorize access.
- (4) The university, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate university personnel, student conduct, or law enforcement agencies and may use those results in appropriate university disciplinary proceedings.
- (5) Personal computing devices:
 - (a) Personal computing devices (laptops, desktops, tablets, cellular phones) are restricted to the campus wireless network or the residence hall network.
 - (b) No personal computing devices will be allowed to connect to the wired campus network (excluding the residence hall network).
 - (c) Personal computing devices must comply with university Information Security Practice when using the campus wireless network or other provided university technology resource.
 - (d) Personal computing devices used to conduct university business are subject to public records requests.
 - (e) Personal hubs, routers, switches, or wireless access points

are prohibited from being connected to either the university's wired or wireless network.

- (G) Email.
- (1) Email is an official means for communication at the university. Students, faculty and staff are expected to check their official email address on a frequent and consistent basis in order to stay current with university communications.
 - (2) Only email sent to the university email address of record will be supported.
 - (3) Email may not be automatically forwarded to off-campus computer accounts from a university assigned email account.
- (H) Security. The university employs various measures (i.e., the university's Information Security Practice) to protect the security of information technology resources and user accounts; however, users should be aware that the university cannot provide good security without user participation. Users should increase their technology security awareness and fully employ access restrictions for their accounts, including using strong passwords, guarding passwords diligently and changing passwords regularly to help safeguard their use of technology.
- (I) Additional policy ramifications. Users must abide by all applicable restrictions, whether or not they are built into the computing system, network or information resources and whether or not they can be circumvented by technical or other means. Individuals who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those states and countries and the rules and policies of those technology systems and information resources.
- (J) Examples of unacceptable use:
- (1) As a further aid to policy compliance, the following non-exhaustive list is provided of activities that are prohibited.
 - (a) Using technology resources to engage in fraud, defamatory, abusive, unethical, indecent, obscene, pornographic and/or

unlawful activities is prohibited.

- (b) Using technology resources to procure, solicit, or transmit material that is in violation of sexual, racial or other harassment or hostile workplace laws is prohibited.
- (c) Any form of harassment by electronic means (e.g., email, web access, phone, paging), whether through language, content, frequency or size of messages is prohibited.
- (d) Making fraudulent offers of products, items or services using any university technology resource is prohibited.
- (e) Using technology resources for unauthorized or inappropriate financial gain, unauthorized solicitation, or activities associated with a for-profit business, or engaging in an activity that involves a conflict of interest. (Refer to rules 3356-7-01 and 3356-7-19 of the Administrative Code.)
- (f) Creating or forwarding chain letters, Ponzi, or other pyramid schemes is prohibited.
- (g) Broadcasting of unsolicited mail or messages is prohibited. Examples include chain letters, virus hoaxes, spam mail, and other email schemes that may cause excessive network traffic. Sending large numbers of electronic mail messages for official university purposes necessitates following the university's procedures for the electronic distribution of information.
- (h) Sending junk mail or advertising material to individuals who did not specifically request such material (email spam) is prohibited.
- (i) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed is prohibited.

- (j) Unauthorized copying and downloading of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and films and the installation of any copyrighted software for which an active license has not been procured is prohibited.
 - (k) Circumventing user authentication or security of any host, network or account is prohibited. This includes, but is not limited to, monitoring by use of keylogging or session logging.
 - (l) Revealing your account password to others or allowing use of your account by others is prohibited. This prohibition extends to family, other household members, friends and/or co-workers.
 - (m) Attempting to log onto another user's account (secured or otherwise) is prohibited.
 - (n) Sending electronic communications in such a way that masks the source or makes it appear to come from another source is prohibited.
 - (o) Personal use beyond limited responsible use is prohibited.
- (2) Exemptions. Individual university staff may be exempted from these restrictions on a case-by-case basis (with written authorization according to the university Information Security Practice) in the course of performing legitimate job responsibilities.
- (3) Passwords. Special procedures exist and must be followed to ensure that accounts for employees are secured with passwords known to only the account holder. Passwords may be changed at the request of the area supervisor and approved by the supervisor's vice president or the president.
- (4) Under no circumstances is an employee of Youngstown state university authorized to engage in any activity that is unethical or

illegal under local, state or federal law while utilizing university-owned resources.

(K) Enforcement.

- (1) The office of the chief technology officer may suspend and/or restrict either an individual's or a device's access to the university network resource if:
 - (a) It is deemed necessary to maintain the security or functionality of the network resource.
 - (b) It is deemed necessary to protect the university from potential liability.
 - (c) The account, system, or device is believed to have been either compromised or is in violation of this policy.
- (2) The office of the chief technology officer must immediately report the enforcement action and the justification for the action to the associate vice president of student experience, vice president for finance and business operations, or provost (or their designee), as applicable. The university may permanently suspend all technology access of anyone using the university network resource until due process has been completed by student conduct, employee administrative discipline and/or law enforcement agencies.



Explanation of Modifications to *University Policy*:

**3356-4-12 Cellular Equipment Usage
(Previous Policy Number 4011.01)**

This policy was reviewed and some sections listed under procedures have been modified to establish additional controls for purchasing cellular equipment, and to require justification to purchase nonstandard equipment with University funds. The attached redline version illustrates the changes the policy has undergone based upon this review.

**Board of Trustees Meeting
March 16, 2016
YR 2016-**

**RESOLUTION TO MODIFY
CELLULAR EQUIPMENT USAGE POLICY, 3356-4-12
(PREVIOUS POLICY NUMBER 4011.01)**

WHEREAS, University Policies are reviewed and reconceptualized on an ongoing basis; and

WHEREAS, this process can result in the modification of existing policies, the creation of new policies, or the deletion of policies no longer needed; and

WHEREAS, action is required by the Board of Trustees prior to replacing and/or implementing modified or newly created policies, or to rescind existing policies; and

WHEREAS, the Cellular Equipment Usage policy has been reviewed pursuant to the five-year review cycle, and formatted in accordance with Policy 3356-1-09, Development and Issuance of University Policies.

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby approve the modification of the University Policy Cellular Equipment Usage Policy, policy number 3356-4-12 (Previous Policy Number 4011.01), shown as Exhibit __ attached hereto. A copy of the policy indicating changes to be made is also attached.

**Board of Trustees Meeting
March 16, 2016
YR 2016-**

3356-4-12 Cellular equipment usage.

Previous Policy Number: 4011.01
Responsible Division/Office: [Information Technology](#) ~~Division~~ [Services](#)
Responsible Officer: [Vice President](#) for Finance and ~~Administration~~
[Business Operations](#)
Revision History: January 2005; June 2011; [March 2016](#)
Board Committee: Finance and Facilities
Effective Date: ~~June 17, 2011~~ [March 16, 2016](#)
Next Review: ~~2015~~ [21](#)

- (A) Policy statement. Youngstown state university (“YSU”) provides cellular capable equipment to employees who, by the nature of their work, are approved to use cellular phones and other devices to conduct university business. Technical support will only be provided for designated university-issued cellular equipment.
- (B) Purpose. This policy establishes guidelines to satisfy the need for university-owned cellular capable equipment. The provisions of this policy apply to all employees of YSU, including those who acquire cellular equipment and services through grants or contracts. This policy also allows the university to meet internal revenue services (“IRS”) regulations and its fiduciary responsibility to the taxpayers of the state of Ohio.
- (C) Procedures.
- (1) The university shall leverage strategic sourcing opportunities by maintaining a single carrier cellular solution in the delivery of its university-issued cellular equipment and services. University-issued cellular equipment shall be limited to standard offerings: a standard voice phone, a standard smartphone, and a standard cellular mobile data accessory (i.e., USB modem). The current standard offering in each category shall be based on the availability of current commercial models and all standard offerings will be provided technical support through YSU tech desk.

- (2) Cellular equipment not conforming to the standard offerings, university-owned or otherwise, does not qualify for technical support for device operation or connectivity to university systems.
- (3) Requests for a cellular-capable device may be made any time during the fiscal year ~~and must be procured centrally through the university's office of information technology services (ITS).~~ Cellular capable devices acquired with university funds may not be purchased with a departmental purchasing card or through any other means.
- (a) ~~Standard university-issued cellular-capable devices must be procured centrally through the network telecommunications office~~ Requests for non-standard devices, as determined by ITS, should be accompanied by written justification and the signature approval of the requestor's supervisor and appropriate executive level officer, as defined by rule 3356-7-35 of the Administrative Code. Any additional costs associated with non-standard devices will be borne by the requesting department.
- (b) Additional accessories for university-issued equipment should be procured locally through the originating department.
- (bc) University-issued cellular equipment and services may be used for incidental personal cellular purposes as defined by IRS tax law and in accordance with rule 3356-4-09 of the Administrative Code. Employees must reimburse the university for any liability incurred through the personal use of the issued cellular equipment. Amounts, if any, to be reported on an employee's W-2 form for non-incidental personal use will comply with IRS guidelines.
- (ed) University-issued cellular equipment and services shall be billed to the assigned department through a monthly chargeback process. The financial manager of the assigned budget must approve the initial requests for university-issued cellular equipment and/or services and for changes in equipment and/or services.

- (de) Use of the cellular devices in any manner contrary to local, state, or federal laws will constitute misuse and may result in the loss of use of university cellular equipment and/or other actions according to rule 3356-4-09 of the Administrative Code.
- (ef) Use of the university-issued cellular equipment must comply with rule 3356-4-13 of the Administrative Code with regard to the transmission and storage of sensitive information on the cellular equipment.
- (fg) Note that university-issued cellular devices are owned by the university. Business-related activity on a cellular-capable device is subject to public records and other applicable laws, regulations, policies, and procedures. Employees should refrain from the use of university-provided cellular equipment while driving.

3356-4-12 Cellular equipment usage.

Previous Policy Number: 4011.01
Responsible Division/Office: Information Technology Services
Responsible Officer: Vice President for Finance and Business
Operations
Revision History: January 2005; June 2011; March 2016
Board Committee: Finance and Facilities
Effective Date: March 16, 2016
Next Review: 2021

- (A) Policy statement. Youngstown state university (YSU) provides cellular capable equipment to employees who, by the nature of their work, are approved to use cellular phones and other devices to conduct university business. Technical support will only be provided for designated university-issued cellular equipment.
- (B) Purpose. This policy establishes guidelines to satisfy the need for university-owned cellular capable equipment. The provisions of this policy apply to all employees of YSU, including those who acquire cellular equipment and services through grants or contracts. This policy also allows the university to meet internal revenue services (IRS) regulations and its fiduciary responsibility to the taxpayers of the state of Ohio.
- (C) Procedures.
 - (1) The university shall leverage strategic sourcing opportunities by maintaining a single carrier cellular solution in the delivery of its university-issued cellular equipment and services. University-issued cellular equipment shall be limited to standard offerings: a standard voice phone, a standard smartphone, and a standard cellular mobile data accessory (i.e., USB modem). The current standard offering in each category shall be based on the availability of current commercial models and all standard offerings will be provided technical support through YSU tech desk.

- (2) Cellular equipment not conforming to the standard offerings, university-owned or otherwise, does not qualify for technical support for device operation or connectivity to university systems.
- (3) Requests for a cellular-capable device may be made any time during the fiscal year and must be procured centrally through the university's office of information technology services (ITS). Cellular capable devices acquired with university funds may not be purchased with a departmental purchasing card or through any other means.
 - (a) Requests for non-standard devices, as determined by ITS, should be accompanied by written justification and the signature approval of the requestor's supervisor and appropriate executive level officer, as defined by rule 3356-7-35 of the Administrative Code. Any additional costs associated with non-standard devices will be borne by the requesting department.
 - (b) Additional accessories for university-issued equipment should be procured locally through the originating department.
 - (c) University-issued cellular equipment and services may be used for incidental personal cellular purposes as defined by IRS tax law and in accordance with rule 3356-4-09 of the Administrative Code. Employees must reimburse the university for any liability incurred through the personal use of the issued cellular equipment. Amounts, if any, to be reported on an employee's W-2 form for non-incidental personal use will comply with IRS guidelines.
 - (d) University-issued cellular equipment and services shall be billed to the assigned department through a monthly chargeback process. The financial manager of the assigned budget must approve the initial requests for university-issued cellular equipment and/or services and for changes in equipment and/or services.
 - (e) Use of the cellular devices in any manner contrary to local, state, or federal laws will constitute misuse and may result

in the loss of use of university cellular equipment and/or other actions according to rule 3356-4-09 of the Administrative Code.

- (f) Use of the university-issued cellular equipment must comply with rule 3356-4-13 of the Administrative Code with regard to the transmission and storage of sensitive information on the cellular equipment.
- (g) Note that university-issued cellular devices are owned by the university. Business-related activity on a cellular-capable device is subject to public records and other applicable laws, regulations, policies, and procedures. Employees should refrain from the use of university-provided cellular equipment while driving.

**RESOLUTION TO RESCIND
THE PREVIOUSLY APPROVED ROOM RENTAL RATES
FOR THE UNIVERSITY COURTYARD APARTMENTS**

WHEREAS, Ohio law provides that each Board of Trustees of state-assisted institutions of higher education may establish special purpose fees, service charges, and fines and penalties; and

WHEREAS, the University Courtyard Apartments were acquired by the University in 2011; and

WHEREAS, on December 16, 2015, the Board of Trustees of Youngstown State University approved room rental rate increases for the University Courtyard Apartments, effective Fall semester 2016; and

WHEREAS, the Governor's Task Force on Affordability & Efficiency in Higher Education has recommended that Ohio's state-supported universities take steps to stem rising college costs and growing student debt; and

WHEREAS, after careful consideration, the University believes that the University housing rates should remain unchanged for Fall 2016 for all University owned housing and that any increases be deferred; and

WHEREAS, in addition to the room rental rates, the University has also carefully considered the University Meal Plan rates and has determined that these rates will also remain unchanged for Fall 2016.

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby rescind resolution YR 2016-____, canceling the previously approved increases in room rental rates for the University Courtyard Apartments.

**Board of Trustees Meeting
March 16, 2016
YR 2016-**

YOUNGSTOWN STATE UNIVERSITY
Budget to Actual
For the 6-month period of 7/1/15 - 12/31/15

FY2016 Revenue 2nd Quarter, 12/31/15	Fiscal Year 2016		Actual as a % of Budget	Business Indicator	FY16 actual compared to FY15 actual
	Budget	Actual			
Tuition and mandatory fees	\$95,098,715	\$83,567,596	87.9%	●	↓
Other tuition and fees	\$10,189,878	\$9,913,316	97.3%	●	↑
Student charges	\$1,311,000	\$870,718	66.4%	●	↑
State appropriations	\$42,471,742	\$20,859,552	49.1%	●	↑
Recovery of indirect costs	\$2,001,413	\$885,843	44.3%	●	↔
Investment income	\$1,530,000	\$1,217,445	79.6%	●	↑
Other income	\$897,252	\$372,393	41.5%	●	↓
Total	\$153,500,000	\$117,686,863	76.7%	●	↑

● On/Above target

● Caution

● Warning

FY2016 Expenses 2nd Quarter, 12/31/15	Fiscal Year 2016		Actual as a % of Budget	Business Indicator	FY16 actual compared to FY15 actual
	Budget	Actual			
Wages	\$74,739,881	\$36,817,576	49.3%	●	↓
Benefits	\$25,257,481	\$13,581,892	53.8%	●	↓
Scholarships	\$5,439,411	\$867,083	15.9%	●	↑
Operations	\$19,891,358	\$7,126,457	35.8%	●	↑
Plant & maintenance	\$9,842,345	\$4,554,358	46.3%	●	↔
Fixed asset purchases	\$390,327	\$129,398	33.2%	●	↑
Transfers	\$18,037,827	\$18,049,078	100.1%	●	↑
Total	\$153,598,630	\$81,125,842	52.8%	●	↑

● On/Below target

● Caution

● Warning

YSU Capital Projects Summary:

Board Projects Update 2/11/2016

Capital Projects Currently Underway:

Elevator Safety Repairs and Replacements
YSU 1516-35

\$1.6M (Capital C34531) Murphy Contracting, Contractor
Elevator cars and equipment in DeBartolo Hall, Tod Hall, Ward Beecher, and Maag Library will be replaced. Modifications to the freight elevators in Moser Hall and Bliss Hall will also be completed. **Update:** DeBartolo and Ward Beecher are complete. Maag Library will start in March for a fall completion and Tod Hall will start in May with an August completion.

Utility Distribution Upgrades and Expansion
YSU 1516-34

\$800k (Capital Funds C34541) C.L. Firestone, Penn Ohio EC
Upgrades and expansion of our electrical substation. **Update:** New sub-station components were installed. A section of high voltage cable needs to be replaced before power is switched over to the new components.

High Voltage Cable Replacement
YSU 1516-89

\$230k Penn Ohio EC
This project will replace electrical cables damaged during the power outage over winter break. The repairs were quickly bid, and a contractor is under contract with work scheduled over Spring Break (March 7 – 13).

Roof Repairs and Replacements
YSU 1516-36

\$1.2M (Capital Funds C34534) BSHM Architects, Boak and Sons
Sections of roofs on Tod Hall, Moser Hall, and Fedor Hall will be replaced. **Update:** Work is complete on Fedor Hall and Tod Hall. Work on Moser Hall was delayed because of the building exterior work and will start March/April 2016.

Moser Hall Advanced Manufacturing Lab
YSU 1516-50

\$700k (Capital Funds C34543) YSU Staff, United Contractors
Renovation of space in Moser Hall for lab space and for the relocation of associated faculty offices. **Update:** Controlling Board has released the funds for fume hoods and associated mechanical and electrical items. These will be delivered and installed over the next few weeks.

Building Exterior Repairs
YSU 1516-51

\$1.1M (Capital Funds C34535) GPD Group, Advanced Rest.
Repairs to the masonry exteriors on Moser Hall, Ward Beecher and Stambaugh Stadium. **Update:** This project is complete with only punch list items remaining.

Melnick Hall Renovations
YSU 1516-1

\$4.65 (Capital, Local C34530) Strollo Architects, Murphy Cont.
Renovations to Melnick Hall for the relocation of the YSU Foundation and WYSU. **Update:** University Development has moved in. WYSU is mostly moved in but radio operations will continue from Cushwa for a few more weeks.

Projects in development for Fall 2015 and Spring/Summer 2016:

Meshel Hall Renovations – 4th floor
YSU 1516-63

\$70k (Local Funds) YSU Staff w/JM Verostko

Relocation of sprinkler piping within the computer center. **Update:** Work will begin soon for this project. Shop drawings are being submitted to the State of Ohio this week.

Elevator Replacements in M1 Parking Deck
YSU 1516-61

\$600k (Capital C34531) Domokur Architects – Murphy Contracting

Complete replacement of two elevator cars in the M1 parking deck. Bids opened October 28th with Murphy Contracting the low bidder. **Update:** Controlling Board has released funds and we are under contract ready to start in May for an August completion.

M1 Parking Deck Lighting Upgrades
YSU 1516-79

\$1.4M (Parking Maintenance Funds) Walker Parking

Replacement of the lighting in the M1 parking deck with efficient LED fixtures. Also included will be painting of the ceilings and signage. Work scheduled to start in May 2016 with the entire deck being closed until August. **Update:** We are under contract and design for the M1 lighting project has begun.

Utility Distribution Upgrades – Steam Line Repair/Replacement
YSU 1516-34-2

\$700k (Capital C34541) CL Firestone

This project will be the replacement of deteriorated steam lines between Meshel Hall and Bliss Hall with new piping within new tunnel sections. **Update:** This project is out for bids with bids due Feb. 24th.

Campus Core Lighting Upgrades, Phase II
YSU 1516-49-2

\$800K (Capital C34537) YSU Staff/CL Firestone

This project will be a continuation of a previous project that will repair and upgrade lighting across campus core. New poles, conduits, and LED fixtures will be installed. **Update:** This project is scheduled to bid starting February 20th with bids opening March 16th. Work will begin Summer 2016.

Building System Upgrades
YSU 1516-73

\$1.5M (Capital C34542) JM Verostko

This project will be the repair and replacement of building systems (HVAC, building automation, mechanical) in several buildings across campus including Moser Hall and Ward Beecher. **Update:** This project is scheduled to bid starting March 12th with a bid opening on April 6th.

Storm Water Upgrades – Fedor Hall
YSU 1516-81

\$250k (Capital C34536) YSU Staff

This project will address water infiltration and flooding issues at Fedor Hall. Work is anticipated to start May/June 2016.

Edmund J. Salata Complex Renovations
YSU 1516-18

\$300k (Capital C34539) YSU Staff

This project will consist of replacing inefficient, single pane windows, replacing HVAC equipment, renovating the restrooms, and minor plumbing upgrades. This project will start early Fall 2016.

Instructional Space Upgrades

YSU 1516-82

\$1M (Capital C34524) YSU Staff

This project will renovate classrooms in Cushwa, DeBartolo, Ward Beecher, and Moser Hall. The project will consist of new flooring, ceilings, lighting, whiteboards, and other finishes. This project will tentatively begin in May 2016.

At Controlling Board

There are no projects currently at the controlling board.

Higher Education 2017-2018 Capital Request

Campus Name Youngstown State University

(highest
priority
first)

	UNIQUE PROJECT TITLE	STATE FUNDS	LOCAL FUNDS	OTHER FUNDS
Project 1	Ward Beecher Science Hall Renovations	2,500,000		
Project 2	Jones Hall Student Success Facility Upgrades	2,000,000		
Project 3	Academic Area Renovations and Upgrades	3,750,000		
Project 4	Meshel Hall Renovations	2,000,000		
Project 5	Campus Development	1,250,000		
Project 6	Emergency Generator Upgrades	1,000,000		
Project 7	Campus Stairwell Safety Upgrades	700,000		
Project 8	Restroom Renovations	750,000		
Project 9	Bliss Hall Renovations	750,000		
Project 10	Campus Wide Concrete Replacement	500,000		
Project 11				
Project 12				
Project 13				
Project 14				
Project 15				
FY17-18 Total		15,200,000	0	0