Youngstown
STATE UNIVERSITY

BOARD OF TRUSTEES
FINANCE AND FACILITIES COMMITTEE
John R. Jakubek, Chair
Scott R. Schulick, Vice Chair

Tuesday, September 18, 2012
3:00 p.m. or immediately following previous meeting

Tod Hall
Board Meeting Room

AGENDA

A. Disposition of Minutes for Meeting Held June 5, 2012

B. Old Business

C. Committee Items

1. Finance

a. Finance Action Items

1) Resolution to Approve Display of Posters and Other Printed Materials Policy **Tab 1**
John Hyden, Executive Director of Facilities will report.

2) Resolution to Modify Acceptable Use of University Technology Resources Policy **Tab 2**
Ken Schindler, Associate Vice President and Chief Technology Officer will report.

3) Resolution to Approve Interfund Transfers **Tab 3**
Katrena Davidson, Interim Controller, will report.

4) Resolution to Approve Transfers Related to Prior Year Ending Deficit Funds as of June 30, 2012 **Tab 4**
Neal McNally, Interim Associate Vice President, Budget Planning and Analysis/Treasurer, will report.

b. Finance Discussion Items

1) **First Quarter FY2013 Vacancy Savings Report** **Tab 5**
Neal McNally, Interim Associate Vice President, Budget Planning and Analysis/Treasurer, will report.

2) **Update on University Budget Fiscal Year 2012-2013**
Gene Grilli, Vice President for Finance and Administration, and Neal McNally, Interim Associate Vice President, Budget Planning and Analysis/ Treasurer, will report.

3) **Report of Audit Subcommittee**
A verbal report of the Audit Subcommittee will be presented. John Jakubek will report.

4) **Report of Investment Subcommittee**
A verbal report of the Investment Subcommittee will be presented. Scott R. Schulick will report.

2. Facilities

a. Facilities Action Item

1) **Resolution to Dissolve University Housing Corporation** **Tab 6**
Gene Grilli, Vice President for Finance and Administration, and Greg Morgione, Associate General Counsel, will report.

b. Facilities Discussion Items

1) **Planning and Construction Projects Update** **Tab 7**
An update of current and planned construction projects throughout campus. Gene Grilli, Vice President for Finance and Administration, will report.

2) **Presentations on Melnick Hall Rehabilitation**
Three architect firms will present, per Board Policy 4007.01 Selection of Architects/Engineers for University Capital Projects.

3) **Report on Pollock House Renovation**
Gene Grilli, Vice President for Finance and Administration, will report.

4) **Report on University Site for Veterans Center**
Gene Grilli, Vice President for Finance and Administration, will report.

D. New Business

E. Adjournment

Youngstown
STATE UNIVERSITY

Explanation of New *Guidebook Policy:*

4015.01 Display of Posters and Other Printed Materials

This is a new policy intended to reduce the random posting of printed materials throughout the campus, thereby enhancing the overall aesthetic appeal of the facilities. The policy does not limit the display of materials, but rather how and where materials are affixed to various building surfaces. This policy will also serve to reduce unintended damage to building surfaces caused by improperly affixed materials.

Board of Trustees Meeting
September 28, 2012
YR 2012-

Youngstown
STATE UNIVERSITY

RESOLUTION TO APPROVE
DISPLAY OF POSTERS AND
OTHER PRINTED MATERIALS POLICY

WHEREAS, the Institutional Policies are being 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;

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby approve the creation of an Institutional Policy governing Display of Posters and Other Printed Materials, policy number 4015.01 of the ***University Guidebook***, shown as Exhibit __ attached hereto.

Board of Trustees Meeting
September 28, 2012
YR 2012-

NEW POLICY

UNIVERSITY GUIDEBOOK

Title of Policy:	**Display of Posters and Other Printed Materials**
Responsible Division:	Finance and Administration
Approving Officer:	Vice President for Finance and Administration
Revision History:	
Resolution Number(s):	YR 2013-
Board Committee:	Finance and Facilities
EFFECTIVE DATE:	
Next review:	2017

Policy: Posters and other printed materials must be appropriate for public display, must be displayed in appropriate locations and must be affixed in an appropriate manner.

Procedures:

1) Printed materials must be appropriate for public display.

2) Students and employees may display printed materials only on designated public bulletin boards.

3) Materials must be displayed in appropriate places:

   a) On bulletin boards, message boards, or other locations specifically identified for the display of printed materials.

   b) Doors, windows, stairwells, elevators, or other locations where it interferes with safety, shall not have materials posted.

4) Printed Materials must be affixed in an appropriate manner:

   a) On surfaces specifically designed to display printed materials.

b) With methods of fixture that are appropriate to the surface being utilized.

c) In no case can printed materials be affixed to walls, windows, doors, elevators or other building surfaces when such surfaces have not been designated and properly prepared to affix printed materials.

5) Printed materials not meeting the above standards will be immediately removed.

6) Materials displayed for special occasions, for example, Red and White Day, must not damage surfaces and must be carefully removed in a timely manner.

7) Damage caused by improper posting and/or the cost of removal will be charged to the department or organization responsible for displaying the printed material.

8) All materials on public bulletin boards or other specific locations will be removed on a scheduled basis.

Youngstown
STATE UNIVERSITY

Explanation of Modifications to *Guidebook Policy:*

4009.01 Acceptable Use of University Technology Resources

This policy was revised to change the title to consist with other Higher Education Institutions, to add clarification to what is prohibited, to clarify language for "No Expectation of Privacy" section and to add an approval procedure prior to the University accessing an employee's email account or files. This policy also, addresses Personal Computing Devices, adds enforcement procedures and authorizes the "University Information Security Practices" guidelines for Information Technology Services (ITS) security related procedures.

Board of Trustees Meeting
September 28, 2012
YR 2012-

Youngstown
STATE UNIVERSITY

RESOLUTION TO MODIFY ACCEPTABLE USE OF UNIVERSITY TECHNOLOGY RESOURCES POLICY

WHEREAS, the Institutional Policies are being 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;

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby approve the modification of the Institutional Policy governing Responsible Use of University Technology Resources, policy number 4009.01 of the ***University Guidebook***, to be retitled as Acceptable Use of University Technology Resources, shown as Exhibit __ attached hereto. A copy of the policy indicating changes to be made is also attached.

Board of Trustees Meeting
September 28, 2012
YR 2012-

UNIVERSITY GUIDEBOOK

Title of Policy:	**Acceptable Use of University Technology Resources**
Responsible Division/Office:	Information Technology
Approving Officer:	Vice President for Finance and Administration
Revision History:	August 1999; November 2010; July 2012
Resolution Number(s):	YR 2000-56; YR 2011-45; YR 2013-
Board Committee:	Finance & Facilities
EFFECTIVE DATE:	
Next review:	2017

Policy: 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.

General Statement:
Technology resources (computing, networking, data and network services) are provided to the University community in order to fulfill the mission of the University.

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.

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.

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.

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).

Use of technology is subject to the requirements of legal and ethical behavior and is intended to promote a productive educational and work environment.

Policy:
All users of University owned technology resources (computing, networking and data), regardless of affiliation with the University, must:

- Use only those technology resources that they are authorized to use and use them only in the manner and to the extent authorized.
- Protect the confidentiality, integrity and availability of technology resources.
- Comply with all federal, Ohio, and other applicable law as well as applicable regulations, contracts, and licenses.
- Comply with all applicable policies at Youngstown State University.
- Respect the right of other technology users to be free from harassment or intimidation.
- Respect copyrights, intellectual-property rights, and ownership of files and passwords.
- Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.
- 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.
- Limit personal use of University technology resources so that such use does not interfere with one's responsibilities to the University.
- Not attempt to circumvent information technology security systems or the University Information Security Practices.
- 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.
- Not use technology resources for personal commercial purposes or for personal financial or other gain unless specifically approved by the University.
- Not state or imply that they speak on behalf of the University without authorization to do so.
- Not use University trademarks and logos without authorization to do so.

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.

User Responsibilities:
- 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 Security Practices.
- 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.

- 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 users control.
- There is no expectation of personal privacy when using University resources. (See section below regarding privacy)Potential violations regarding use of technology resources should be reported to the appropriate supervisor(s) or manager(s).
- 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).
- Users are responsible for maintaining data in compliance with the University records retention plan.
- Users are responsible for ensuring that sensitive information to which they have access is guarded against theft. (See the Sensitive Information Policy Guidebook Policy #4012.01 for more information.)
- 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.

No Expectation of Privacy:
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 operations 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.

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.

When authorized by the appropriate University Executive (President or Vice President), the University may access 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.

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.

Personal Computing Devices:

- Personal computing devices (laptops, desktops, tablets, cellular phones, etc.) are restricted to the campus wireless network or the Residence Hall network.
- No personal computing devices will be allowed to connect to the wired campus network (excluding the Residence Hall network).
- Personal computing devices must comply with University Information Security Practices when using the campus wireless network or other provided University technology resource.
- Personal computing devices used to conduct University business are subject to public records requests.
- Personal hubs, routers, switches, or wireless access points are prohibited from being connected to either the University's wired or wireless network.

Security:

The University employs various measures (i.e., the University's Information Security Practices) 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.

Additional Policy Ramifications:

Users must abide by all applicable restrictions whether or not they are built into the computing system, network, or information resource, 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.

Examples of Unacceptable Use:

As a further aid to policy compliance, the following non-exhaustive list is provided of activities that <u>are prohibited</u>:

- Using technology resources to engage in fraud, defamatory, abusive, unethical, indecent, obscene, pornographic and/or unlawful activities is prohibited.
- 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.
- 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.
- Making fraudulent offers of products, items, or services using any University technology resource is prohibited.
- 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 7001.01 – Conflicts of Interest, and 7005.01 – Solicitation and Distribution of Materials, Employees.)

- Creating or forwarding chain letters, Ponzi or other pyramid schemes is prohibited.
- 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.
- Sending junk mail or advertising material to individuals who did not specifically request such material (email spam) is prohibited.
- 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.
- 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.
- Circumventing user authentication or security of any host, network or account is prohibited.
- 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.
- Attempting to log on to another user's account (secured or otherwise) is prohibited.
- Sending electronic communications in such a way that masks the source or makes it appear to come from another source is prohibited.
- Personal use beyond limited responsible use is prohibited.

Individual University staff may be exempted from these restrictions on a case-by-case basis (with written authorization according to the University's Information Security Practices) in the course of performing legitimate job responsibilities.

Special procedures exist and must be followed to ensure that accounts for employees are secured with passwords known to only the account holder but may be changed at the request of the area supervisor and approved by the supervisor's Vice President or the President.

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.

Enforcement:
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:

1. It is deemed necessary to maintain the security or functionality of the network resource.
2. It is deemed necessary to protect the University from potential liability.
3. The account, system, or device is believed to have been either compromised or is in violation of this policy.

The Office of the Chief Technology Officer must immediately report the enforcement action and the justification for the action to the Vice President of Student Affairs, Vice President for Finance and Administration, 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.

UNIVERSITY GUIDEBOOK

Title of Policy: ~~Responsible~~ Acceptable Use of University Technology Resources

Responsible Division/Office:	Information Technology
Approving Officer:	Vice President for Finance and Administration
Revision History:	August 1999; November 2010; July 2012
Resolution Number(s):	YR 2000-56; YR 2011-45; YR 2013-
Board Committee:	Finance & Facilities
EFFECTIVE DATE:	
Next review:	2017

Policy: 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.

General Statement:
Technology resources (computing, networking, ~~and~~ data and network services) are provided to the University community in order to fulfill the mission of the University.

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.

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.

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.

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).

Use of technology is subject to the requirements of legal and ethical behavior and is intended to promote a productive educational and work environment.

Policy:
All users of University owned technology resources (computing, networking and data), regardless of affiliation with the University, must:

- Use only those technology resources that they are authorized to use and use them only in the manner and to the extent authorized.
- Protect the confidentiality, integrity and availability of technology resources.
- Comply with all federal, Ohio, and other applicable law as well as applicable regulations, contracts, and licenses.
- Comply with all applicable policies at Youngstown State University.
- Respect the right of other technology users to be free from harassment or intimidation.
- Respect copyrights, intellectual-property rights, and ownership of files and passwords.
- Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.
- 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.
- Limit personal use of University technology resources so that such use does not interfere with one's responsibilities to the University.
- ~~Refrain from any~~ Not attempt to circumvent information technology security systems or the University Information Security Practices.
- ~~Refrain from the~~ Not use ~~of~~ 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.
- ~~Refrain from using~~ Not use technology resources for personal commercial purposes or for personal financial or other gain unless specifically approved by the University.
- ~~Refrain from stating or implying~~ Not state or imply that they speak on behalf of the University without authorization to do so.
- ~~and from using~~ Not use University trademarks and logos without authorization to do so.

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.

User Responsibilities:
- By ~~using any YSU technology resources~~ accepting employment, being admitted as a student, or asking for any guest technology resource privileges, users implicitly ~~are agreeing~~ agree to adhere to this policy and agree to the University Information ~~s~~Security ~~p~~Practices ~~of the University~~.

- 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.
- 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 users control.
- There is no expectation of personal privacy when using University resources. (See section below regarding privacy)Potential violations regarding use of technology resources should be reported to the appropriate supervisor(s) or manager(s).
- 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).
- Users are responsible for maintaining data in compliance with the University records retention plan.
- Users are responsible for ensuring that sensitive information to which they have access is guarded against theft. (See the Sensitive Information Policy Guidebook Policy #4012.01 for more information.)
- 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.

No Expectation of Privacy:

~~While~~ ~~t~~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 operations and maintenance of the University's computing, network and data resources. This monitoring includes ~~require~~ the ~~backup and~~ caching and backing up of data and communications, the logging of activity, the monitoring of general usage patterns, the scanning of systems and networks ~~ports~~ for anomalies and vulnerabilities, the filtering of malicious traffic, and other ~~such~~ activities that are necessary for the rapid and efficient delivery of services. Technology users should be aware~~, however,~~ that ~~their~~ there ~~use of University technology resources~~ is ~~not completely private~~ no expectation of privacy associated with the use of University technology resources.

~~For uncommon situations,~~ ~~w~~When ~~specifically~~ authorized by ~~in conjunction with~~ 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 ~~individual~~ login sessions, file systems and communications~~, without notice, when:~~.

~~a. The user has given permission or has voluntarily made activity and accounts accessible to the public, for example by posting to a publicly accessible web page or providing publicly accessible network services.~~

~~b. Supervisors and assigned personnel need to access accounts, files or communications used for University business when an employee becomes unavailable.~~
~~c. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.~~
~~d. System managers initiate access to user accounts, files or communications when there is reason to believe that the user is interfering with the performance of a system.~~
~~e. It reasonably appears necessary to do so to protect the integrity, security or functionality of the University or other technology resources or to protect the University from liability.~~
~~f. There is reasonable cause to believe that the user has violated, or is violating, this policy.~~
~~g. It is otherwise required or permitted by law, University policy or work rules.~~

When authorized by the appropriate University Executive (President or Vice President), the University may access 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.

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.

Personal Computing Devices:

- Personal computing devices (laptops, desktops, tablets, cellular phones, etc.) are restricted to the campus wireless network or the Residence Hall network.
- No personal computing devices will be allowed to connect to the wired campus network (excluding the Residence Hall network).
- Personal computing devices must comply with University Information Security Practices when using the campus wireless network or other provided University technology resource.
- Personal computing devices used to conduct University business are subject to public records requests.
- Personal hubs, routers, switches, or wireless access points are prohibited from being connected to either the University's wired or wireless network.

Security:
The University employs various measures (i.e. the University's Information Security Practices) 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. **Additional Policy Ramifications:** Users must abide by all applicable restrictions whether or not they are built into the computing system, network, or information resource, 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.

Examples of Unacceptable Use:
As a further aid to policy compliance, the following non-exhaustive list is provided of activities that are prohibited:

- Using technology resources to engage in fraud, defamatory, abusive, unethical, indecent, obscene, pornographic and/or unlawful activities is prohibited.
- 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.
- 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.
- Making fraudulent offers of products, items, or services using any University technology resource is prohibited.
- 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 7001.01 – Conflicts of Interest, and 7005.01 – Solicitation and Distribution of Materials, Employees.)
- Creating or forwarding chain letters, Ponzi or other pyramid schemes is prohibited.
- 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 number of electronic mail messages for official University purposes necessitates following the University's procedures for the electronic distribution of information.
- Sending junk mail or advertising material to individuals who did not specifically request such material (email spam) is prohibited.
- 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.
- 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.
- Circumventing user authentication or security of any host, network or account is prohibited.
- 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.

- Attempting to log on to another user's account (secured or otherwise is prohibited)~~, remove or modify files, access protected files, or in any way alter another user's account are prohibited~~.
- Sending electronic communications in such a way that masks the source or makes it appear to come from another source is prohibited.
- Personal use beyond limited responsible use is prohibited.

Individual University staff may be exempted from these restrictions on a case-by-case basis (with written authorization ~~as identified above~~ according to the University's Information Security Practices) in the course of performing legitimate job responsibilities.

Special procedures exist and must be followed to ensure that accounts for employees are secured with passwords known to only the account holder but ~~accessible to the~~ may be changed at the request of the area supervisor ~~if needed as authorized by this policy~~ and approved by the supervisor's Vice President or the President.

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.

Enforcement:

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:

1. It is deemed necessary to maintain the security or functionality of the network resource.
2. It is deemed necessary to protect the University from potential liability.
3. The account, system, or device is believed to have been either compromised or is in violation of this policy.

The Office of the Chief Technology Officer must immediately report the enforcement action and the justification for the action to the Vice President of Student Affairs, Vice President for Finance and Administration, 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.

Youngstown
STATE UNIVERSITY

RESOLUTION TO APPROVE
INTERFUND TRANSFERS

WHEREAS, Policy Number 3010.01, Budget Transfers, of the ***University Guidebook,*** requires Board of Trustees approval for interfund transfers of $100,000 or more; and

WHEREAS, certain accounting adjustments and transfers outside the operating budget are necessary;

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby approve transfers outside the operating budget, as detailed in Exhibit ____.

Board of Trustees Meeting
September 28, 2012
YR 2012-

YOUNGSTOWN STATE UNIVERSITY
Interfund Transfers Requiring Board Approval
Transfers Outside of the Operating Budget
Requested Transfers for June 30, 2012

FROM	TO	AMOUNT	REASON
FY2012 Year End Transfers			
Housing & Residence Life (Auxiliary)	Housing & Residence Life Plant Reserve (Auxiliary Plant Fund)	$1,066,177	Year end excess of $1,071,177 less $5,000 to operating contingency reserve.
Parking Services (Auxiliary)	Parking Services Plant Reserve (Auxiliary Plant Fund)	$312,190	Year end excess of $327,190 less $15,000 to operating contingency reserve.
Kilcawley Center (Auxiliary)	Kilcawley Center Plant Reserve (Auxiliary Plant Fund)	$114,337	Year end excess.
Andrews Recreation & Wellness Center (Auxiliary)	Andrews Recreation & Wellness Center Plant Reserve (Auxiliary Plant Fund)	$184,578	Year end excess.
General Fund	Operating Carry Forward (Designated Fund)	($424,030)	Transfer net FY2012 year end deficit to Operating Carryforward Fund. Consists of General Fund deficit of ($1,610,345), Intercollegiate Athletic deficit of ($221,932) and unspent FY2012 technology and lab materials fees of $744,867, and unspent FY2012 college fees of $663,380.
ERIP OPERS Fund (Designated Fund)	General Fund	$2,338,082	Transfer ERIP Savings.
Bookstore Operating (Auxiliary)	Kilcawley Center Plant Reserve (Auxiliary Plant Fund)	$100,000	Payoff interfund loan.

YOUNGSTOWN STATE UNIVERSITY
Interfund Transfers Requiring Board Approval
Transfers Outside of the Operating Budget
Requested Transfers for First Quarter 2013

FROM	TO	AMOUNT	REASON
First quarter FY2013			
Debt Service Reserve - WCBA Gifts (Restricted Plant Fund)	Bond Fund - Series 2009 (Debt Service Fund)	$851,779	Transfer to fund portion of FY13 debt service attributed to the WCBA.
Kilcawley Center Plant Reserve (Auxiliary Plant Fund)	Kilcawley House Renovations - Phase 3 (Auxiliary Plant Fund)	$700,000	Transfer to fund third and final phase of a project to renovate the six resident floors during spring and summer semester 2013. Renovations include complete roof replacement for Kilcawley House, complete renovation of the sixth and seventh floors, and upgrades to the stairwells and basement lounges.
Debt Service Reserve - General Fund (Unrestricted Plant Fund)	Bond Fund - Series 2010 (Debt Service Fund)	$517,690	Transfer to fund portion of FY13 debt service.
Bond Fund - Series 2013 (Debt Service Fund)	Housing & Residence Life (Auxiliary)	$363,508	Transfer excess FY13 debt service funding back to original source.
Debt Service Reserve - WATTS Gifts (Restricted Plant Fund)	Bond Fund - Series 2010 (Debt Service Fund)	$299,547	Transfer to fund portion of FY13 debt service attributed to WATTS.
Debt Service Reserve - General Fund (Unrestricted Plant Fund)	Bond Fund - Series 2009 (Debt Service Fund)	$201,035	Transfer to fund portion of FY13 debt service.
Property Acquisition Fund (Unrestricted Plant Fund)	Church Deconstruction Fund (Unrestricted Plant Fund)	$119,000	Transfer to fund deconstruction of Pilgrim Collegiate Church.

Youngstown
STATE UNIVERSITY

RESOLUTION TO APPROVE TRANSFERS RELATED TO PRIOR YEAR ENDING FUND BALANCES

WHEREAS, certain accounting and budget adjustments and transfers outside the operating budget are necessary at the end of a fiscal year; and

WHEREAS, Youngstown State University completed the fiscal year ending June 30, 2012, with deficits in certain operating funds and excesses in other operating funds; and

WHEREAS, as part of the University's regular year-end closing procedures for the fiscal year ending June 30, 2012, a net deficit of $424,030 has been transferred to the University's operating carry-forward fund; and

WHEREAS, the University has adequate reserve funds with which to zero-out the said deficit in the operating carry-forward fund;

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby approve the budget transfers, as detailed in Exhibit___.

Board of Trustees Meeting
September 28, 2012
YR 2012-

YOUNGSTOWN STATE UNIVERSITY
FY 2012 Year-End Summary and Proposed FY 2013 Transfers
As of 8/27/12 (subject to audit adjustments)

FY 2012 Year-End Summary

General Fund (includes scholarships)	($1,610,345)
Intercollegiate Athletics	(221,932)
Subtotal	($1,832,277)
Technology & Lab Materials Fees	$744,867
College Fees	663,380
Subtotal	$1,408,247
Net Year-End Operating Deficit	($424,030)

Proposed FY 2013 Transfers to Cover Deficit

From Reserves:	
IT Equipment Replacement Reserve	$925,000
Technology Master Plan	293,913
Property Acquisition Reserve	150,000
Employee Wellness Program	63,213
Scholarship Reserve	140,179
Institutional Enhancement Reserve	100,000
Legal Contingency Reserve	115,903
Subtotal	$1,788,208
To Designated Funds:	
Tech & Lab Materials Fee Carry-Fwd. Fund	($590,182) *
College Fee Carry-Fwd. Fund	(649,573) *
Research Incentive Carry-Fwd. Fund	(124,423)
Subtotal	($1,364,178)
Net Total	$424,030

* Amounts adjusted for FY 2012 actual revenues and expenses.

FY 2013 Vacancy Savings Report
1st Quarter FY 2013 (as of August 15, 2015)

The following quarterly vacancy savings report is provided pursuant to the FY 2013 Operating Budget, adopted by the Board of Trustees on June 13, 2012, which states in part:

> *"Because the FY 2013 budget relies so heavily on vacancy savings, and because this use of position vacancies represents only temporary budgetary savings, the Administration will report quarterly to the Board of Trustees on the status of funds budgeted as vacancy savings."*

Note that the figures provided in this report reflect permanently budgeted staff positions; faculty vacancy savings are not included here.

YOUNGSTOWN STATE UNIVERSITY
FY 2013 Quarterly Vacancy Savings Report
Information as of 8/15/12

Original FY 2013 Budget	($4,944,484)
Budgeted FY 2013 Vacancies	4,944,484
Adjustments:	
Additional vacancy savings	324,614
Vacant positions filled	(283,056)
Vacancy Savings Balance	$41,558

Youngstown
STATE UNIVERSITY

RESOLUTION TO RECOMMEND THE DISSOLUTION OF THE UNIVERSITY HOUSING CORPORATION

WHEREAS, in 2001, the University Housing Corporation ("UHC") was formed as an Ohio non-profit corporation to develop housing for the students, faculty and staff of Youngstown State University (the "University"); and

WHEREAS, on May 8, 2002, the State of Ohio, through the Ohio Department of Administrative Services on behalf of the University, as Lessor, entered into a Lease with the UHC, as Lessee, pursuant to Ohio Revised Code 123.77 (the "Lease") for the real property described in the Lease for the development of student housing; and

WHEREAS, the UHC constructed the University Courtyard Apartments, a 408-bed student housing facility on the eastern edge of campus (the "Project"), which opened in the Fall of 2003; and

WHEREAS, in 2011, the University determined that it was in its best interest and consistent with the Centennial Campus Master Plan to acquire the Project from the UHC with the intent that the Project be self-supporting; and

WHEREAS, on June 17, 2011, this Board adopted Resolution YR 2011-108 authorizing the issuance and sale of not to exceed $20,500,000 of General Receipts Bond to pay the costs to acquire the Project from the UHC; and

WHEREAS, on July 20, 2011, the University acquired the Project from the UHC; and UHC assigned all its right, title and interest in the Lease to the University; and

WHEREAS, on June 5, 2012, the State of Ohio, through the Ohio Department of Administrative Services on behalf of the University, terminated the Lease which was unnecessary due to the purchase of the Project by the University; and

WHEREAS, this Board, finds that there is no University purpose for the continued existence of the UHC and that it would be in the best interests of the University and the UHC Board of Directors to take action to dissolve the UHC; and

WHEREAS, this Board recommends that upon dissolution of the UHC, the UHC Board of Directors distribute all residual assets of the UHC to the University in conformity with Article III(2)(b)(v) of the UHC Articles of Incorporation;

Youngstown
STATE UNIVERSITY

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby recommend to the University Housing Corporation Board of Directors that they take action to dissolve the University Housing Corporation and distribute all residual assets to Youngstown State University, and that a copy of this Resolution be delivered to the University Housing Corporation.

Board of Trustees Meeting
September 28, 2012
YR 2012-

YSU CONSTRUCTION PROJECTS UPDATE – AUGUST 15, 2012

Academic Building Renovations Project – The first phase of the Academic Building Project will be the renovation of three auditoriums found in Cushwa, DeBartolo and Ward Beecher. An additional auditorium in Beeghly Center will be renovated the following summer. Design work is by Facilities and Media and Academic Computing staff.

Bids were received on May 3rd and the following contractors were the lowest, best bidders: Murphy Contracting, SA Comunale, D&G Mechanical and BJ Electric. Construction is well underway and will be completed by August 22nd in time for fall classes.

Following this initial project will be several renovation projects in each of the buildings. The renovations will include but not be limited to flooring, lighting, wall finishes, major mechanical system upgrades and building exterior repairs.

M2 Parking Deck – Phase 2 of this project has been bid and is moving forward quickly. Contractors Suburban Maintenance and University Electric had the lowest, best bids and were accepted. Some minor repairs will be made in this phase along with all new interior lighting, painting and deck coatings. This project will be complete by the start of fall semester.

M1 Parking Deck Repairs – We will continue with preventative maintenance this summer on the M1 parking deck to ensure its long term viability. The contractors Suburban Maintenance and University Electric will also be working on this deck. Work started on time in May and will conclude in August prior to the start of fall semester.

Athletic Fields West of Fifth – Facilities, Athletics and our consultant GPD are reviewing bids that were open and read on August 8th. Initially it appears that this project will be to ready the site by leveling and installing necessary retaining walls then installing a synthetic soccer field and perimeter fencing. It was hoped that a softball field would also be included but at this time, project estimates and bid numbers indicate that funding may not be available. We hope to have the contractor on site working by early September.

Pollock House – Pollock House is winding down and as of now, we are on budget and working towards a final completion date of September 25th.

The first floor will be the main entertaining/gathering space of the mansion and will also include home office space for the president. The second level of the mansion will be the president's residence and consist of a kitchen, great room, master suite, in-law suite and two sleeping rooms. The upper level will not be renovated at this time. Exterior improvements include a new slate roof, repair/painting of the wood siding, new windows, and landscaping.

Campus Elevators Upgrades – This is a project that will start to bring our existing elevators, most of which are over 25 years old, up to modern day standards. This project was competitively bid with ThyssenKrupp being the low bidder. In this first phase, renovations to Kilcawley House and Cushwa Hall south elevators will take place.

This project began on time in May with Kilcawley House being already complete and Cushwa elevators heading toward a late September completion.

Lincoln Building Roof – The roof on the Lincoln Building has been in poor condition for some time. Facilities recently contracted with a roofing consultant, RoofTEC, and put together a project to replace the entire roof. The project was competitively bid and Industrial Energy Systems was the low bidder. All work except for punch-list items is complete.

Bliss Hall Music Practice Rooms – Originally constructed in the 1970's, the practice rooms in Bliss Hall are small spaces constructed of hard materials that reverberate sounds within the rooms and project the sounds into the surround spaces causing disruptions in the corridors and adjacent instructional spaces. This project will address the acoustics within the rooms and also reduce the sound infiltration into adjacent spaces. This project was competitively bid and Dick Building Co., Becdel Controls and Western Reserve Mechanical submitted the lowest, best bids. Construction started in late May 2012 and substantial completion will conclude prior to the start of fall classes. Some long lead items such as acoustic doors and rubber flooring will be installed in phases as they arrive but the space will be open for use by students.

Wind Turbine Project – Working with CJL Engineering and the department of Mechanical Engineering Technology with funding through a Department of Energy grant, Facilities is assisting with the installation of wind turbines behind Melnick Hall and along the East Bound Service Road. Three wind turbines will be installed on 80' towers and data from these turbines will be collected and studied by the Engineering Technology department.

This project was competitively bid with Zenith Systems being the low bidder. We are going through bid evaluations now, and should have Zenith under contract by mid September. This project will be complete by the end of December.

WATTS Solar Array – Facilities is working with Carbon Vision, the same company that installed the solar array on Moser Hall, to potentially install a solar array on the south facing roof of the WATTS Indoor Facility. Carbon Vision is currently working to determine the viability of the project and once confirmed, the project is anticipated to begin this fall.

This project will install solar panels over the entire south facing roof of the WATTS and the electricity generated by the panels will essentially make the WATTS facility energy self sufficient. Any additional energy created that is not used by the WATTS will loop back into the University power grid and be distributed throughout campus.

Cushwa/Debartolo Entryways – As part of the Academic Building renovations project, the main entryways into Cushwa and Debartolo will receive a makeover. The goal of this project is to enhance the overall appearance of the space and to create a more inviting entryway that welcomes people into the building as well as updating aged mechanical and electrical systems. Work for this project will begin at the start of winter break in December 2012 and be complete by mid January 2013 for the start of Spring Semester.

Melnick Hall Renovations – Preliminary work is beginning on renovation plans to Melnick Hall. Currently the Journalism program, WYSU, Jambar, Rookery Radio and parts of Telecommunications will potentially occupy the building. We have requested $2.5million in our capital request specifically earmarked for Melnick with additional funds coming from donations.

Planning and Construction has advertised for RFQ's and we received 21 submissions. A committee has been established to evaluate the submissions and choose three candidates for the board to review. Once a consultant is chosen, we can move forward with the design process.

Pilgrim Church – Work is underway to develop drawings and specifications for the demolition of this building. Some stained glass windows have already been removed and efforts are underway to find homes for the remaining windows. Demolition is anticipated for this summer.

Peck House Demolition – This project has started and will be complete by the end of August.

Building System Upgrades; 4160v Loop Repair – YSU has its own sub-station where power is brought on to campus and distributed out to our buildings. Most of our buildings are fed off of a "loop" from the sub-station which provides a redundant source of power so that in the event of one part of the loop failing, the other part of the loop can continue to supply power. As part of the Campus Wide Building System Upgrades project, major building systems such as voltage loops, steam lines and HVAC systems will be upgraded or replaced helping to ensure little to no disruption in service to our campus community.

In this project, a critical portion of a damaged power loop from our sub-station to our student dorms will be replaced. Replacing this line will ensure a redundant, reliable supply of power to our student housing.

This project was competitively bid and B&J Electric was the low bidder. The funding will be from State Capital and is scheduled for a September 10th hearing date and soon after we will enter into a contract with B&J and get the project started.