This policy outlines the standards and expectations for responsible and acceptable use of college computing systems and information technology (IT) resources. The college provides access to technology resources in support of the mission of the college. The college’s IT department is committed to protecting authorized users, computing systems, data, electronic communications and information technology resources from intentional or negligent illegal or damaging use. All users of the college’s technology resources are expected to act responsibly, ethically and lawfully.

This policy applies to all employees, students, visitors and agents of the college who use and access the college’s information technology resources, whether on campus, off campus or via remote connection. This policy applies to all equipment either owned or leased by the college and governs activity on personal computing devices while utilizing and/or accessing any college computing system or information technology resource.

The granting of privileges to use college computing systems and IT resources is predicated on the authorized user’s acceptance of and adherence to the corresponding conditions and user responsibilities detailed in this policy. College resources should be used for business and academic purposes. Occasional, limited and appropriate use of college resources for personal use is permitted if that use does not interfere with the user’s work performance. Authorized users assume responsibility for all communications originating from equipment or accounts assigned to the user. Authorized users are solely responsible for the use and handling of data, computing systems and information technology resources. It is the responsibility of all users to know the guidelines stated in college policies and to conduct their activities accordingly.

Information security is the responsibility of all users and any inappropriate use or suspected security incident must be reported to the college’s IT department by calling (410) 334-2870 or by emailing it-info@worwic.edu. Authorized users agree to be good stewards when storing, accessing and transporting data.

The use of IT resources is a privilege and not a right. Under no circumstances are authorized users permitted to engage in any activity that is illegal. The following list of prohibited activities, by no
means exhaustive, is an attempt to provide a framework for actions that fall into the category of unacceptable use:

- Using a computer without authorization;
- Obstructing the operation of the college's computer resources, including, but not limited to, intentionally damaging equipment, tampering with cables, adding or deleting files or software without authorization, changing network settings;
- The intentional introduction or creation of invasive software, such as worms or viruses, Trojan horses and email bombs;
- Attaching a network device to the college's networks without approval of the IT department, including hubs, switches, wireless access points, routers or similar devices;
- Using computing systems, college networks or any other information technology resource to threaten or harass others or attempting to alter computer systems, hardware, software or account configurations;
- Monitoring another individual's account(s), data, communications, software, computing resources or email without prior consent;
- Sharing user account passwords with others;
- Allowing the use of an authorized user account by others, such as another family member or friend;
- Misrepresenting one's identity or role in any type of electronic communication;
- Using computing systems or information technology resources for commercial or profit-making purposes without written authorization from the college;
- Copying software found on college systems that is licensed by the college for personal use, transferring software to non-college equipment or modifying it in any unauthorized manner;
- Installing or operating computer games on college-owned computers for purposes other than academic instruction;
- Producing and broadcasting hate mail, discriminatory remarks or chain letters;
- Breaching or attempting to breach computer systems or information technology resources or security systems, whether with or without malicious intent;
- Engaging in any activity that can be harmful to systems or to any stored information, such as creating or propagating viruses or other types of malware;
- Violating copyright and/or software license agreements or downloading, installing or using illegal software;
- Installing or using any covert video/audio recording device;
- Displaying any material that is sexually-explicit or discriminatory in nature; and
- Accessing or disclosing sensitive information without authorization or any theft of college data or equipment.

Authorized IT employees reserve the right to monitor and access any computing system or resource connected or attached to the college’s networks. Monitoring can include, but is not limited to, reviewing, copying and accessing or archiving any information, logs, packets or other materials stored on, transmitted through or created with college technology resources. There is no expectation of privacy with regard to the college’s computing systems, information technology
resources and network infrastructure, while on or accessing resources remotely.

Violations of this policy are subject to college disciplinary procedures, state, local and federal laws and regulations. Based on the nature of the offense and/or the number of violations, employees and other agents of the college are subject to appropriate personnel action, up to and including dismissal. Students are subject to disciplinary action taken in accordance with procedures that govern student conduct, up to and including permanent suspension. If appropriate, the college can pursue criminal and civil prosecution.
Email Usage Standards and Procedures for Employees

Policy Ref
PPM00160

Policy Title
Email Usage Standards and Procedures for Employees

The purpose of this document is to set forth general standards and procedures related to electronic communications, including e-mail. E-mail is provided to college employees and other agents of the college for administrative and educational purposes.

E-mail messages created and transmitted via college computers and applications are the property of the institution. The college reserves the right to monitor all e-mail transmitted via our computer systems. Employees have no reasonable expectation of privacy when it comes to business and personal use of the college's mail system. E-mail is not a method of secure communications and e-mail users must exercise extreme caution when dealing with sensitive or confidential information.

The college reserves the right to monitor, inspect, copy, review and store any and all employee e-mail at any time and without prior notice. In addition, the college reserves the right to monitor, inspect, copy, review, and store any files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored through the college's e-mail system. The college reserves the right to disclose e-mail information and images to regulators, courts, law enforcement agencies, and other third parties without the employee's consent.

E-MAIL SYSTEM STANDARDS
The following e-mail system standards apply to all college employees or agents of the college.

Mailbox Size Limits
Support Staff/Administrators/Faculty mailboxes are limited to a 2 GB Limit. Selected user mailboxes can be granted with an unlimited mailbox size on a case-by-case basis.

Message Retention Policy
Mailbox items that are older than 1 year are automatically deleted from user's mailboxes.

E-mail Attachment Limit
Attachments are limited to 30 Mb in size. Note that attachment size limits will vary on e-mail messages being sent to other outside e-mail systems.
ACCEPTABLE USE
This list of acceptable use of college e-mail does not represent a complete list, but serves as general guidelines.

- Be polite and professional.
- College e-mail should be used for college-related administrative and educational purposes.
- E-mail usage is subject to college policies and local, state and federal laws and regulations.
- College e-mail should not be used for commercial purposes.
- Users are prohibited from using email to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.
- Do not e-mail sensitive or confidential information, such as social security numbers.
- Do not reveal your account name and password to others.

WEB MAIL
Users can access their e-mail accounts via the Internet by using a standard web browser.

OUTLOOK WEB ACCESS URL
http://www.worwic.edu/FacultyStaff/EmployeeEmail.aspx or via link below.

E-MAIL ON MOBILE DEVICES
Users can receive remote access to e-mail via a mobile device, such as a smartphone or a tablet computer, on a Microsoft Exchange ActiveSync compatible e-mail program. To receive college e-mail on a mobile device, a user must agree to allow IT to remotely wipe their college or personally owned device if the device is reported lost or stolen. See Email Synchronization Acknowledgment Form. Lost or stolen devices must be reported to IT’s central number at (410) 334-2870. Backups of personal or company owned devices should be performed on a regular basis. The college is not responsible for any incurred data or voice charges on personally owned devices.

ADDITIONAL ASSISTANCE WITH E-MAIL
For assistance or additional information about college e-mail accounts or usage, call the IT central number at (410) 334-2870.

LINKS
Outlook Web Access URL Link
Email Synchronization Acknowledgment Form
The purpose of this incident response plan is to outline the methods and actions that the college will follow in the event of a data breach. A data breach is defined as an unauthorized movement or disclosure of sensitive or confidential information to a party that is not authorized to have or see the information. Sensitive and confidential information includes personally identifiable information (PII) such as, but not limited to, social security numbers, credit card numbers, student grades, birth dates, driver’s license numbers and personal medical information.

The task of protecting sensitive information is the responsibility of all individuals of the college who have access to this type of information. In general, sensitive information should not be copied, accessed, stored, downloaded, transmitted or used unless it is essential to do so to conduct official business of the college. Individuals should not store sensitive and confidential information on laptops, tablets, smartphones or other mobile storage devices. Encryption technology should be used where needed to protect sensitive data. Further information about protecting PII is included in the college’s identity theft prevention policy along with additional guidance for detecting, preventing and mitigating risks of identity theft.

Violations of the college’s computer usage policy include accessing or disclosing sensitive information without authorization, and breaching or attempting to breach computer systems or information technology (IT) resource security systems. These violations are subject to disciplinary action as specified in the policy.

RESPONDING TO DATA BREACHES
If a breach occurs, it is important that the college take immediate action to respond to the security incident. Computer and mobile device thefts must be reported immediately to the IT department. The following steps will be taken in the event of a suspected security incident:

- **Determine the nature of the security incident**
  - Record the date, time, location and apparent cause of the security incident
  - Identify the affected system(s)
  - Identify the data at risk
  - Determine if there was a breach
- **Communicate the breach to the following authorized individuals depending on the nature of**
the breach
- Senior director of information technology
- President
- Vice presidents
- Director of public safety
- Director of finance
- Senior director of human resources
- Dean of Continuing Education and Workforce Development
- Legal counsel
- Law enforcement

Investigate the breach
- Inventory materials at risk
- Utilize forensic tools
- Disconnect affected system(s) from the network
- Determine the likelihood of recovering data or stolen equipment
- Utilize the assistance of outside resources, if needed
- Secure material that could be used as evidence

Assess the breach
- Identify individuals affected by the breach and notify them
- Determine if identity theft monitoring is appropriate, and if so, for how long?

Remediate
- Change passwords to all user and system accounts
- Restore data from backup, if necessary
- Contact insurance company
- Replace systems

Notify the public of the breach
The president and vice presidents will meet with IT employees to determine the need and methods of communicating information about a breach to affected individuals, the college community and/or the public.

Post-Incident follow-up
- Pursue all reasonable means to recover data
- Modify processes, procedures or policies that can assist in avoiding future incidents

CONTACT INFORMATION
Individuals can utilize the contact information provided below to report a suspected breach:

College Main Number: (410) 334-2800
IT Department Number: (410) 334-2870
IT Department E-mail: it-info@worwic.edu
IT Security E-mail: infosec@worwic.edu
Passwords

Policy Ref
PPM00159

Policy Title
Passwords

The purpose of this policy is to establish the creation of strong passwords, the protection of those passwords and the frequency that passwords are changed. This policy covers all students, employees and other agents of the college who are assigned user accounts. The information technology department (IT) is responsible for securing passwords associated with any system or local computer accounts. Student user accounts have the same password requirements but their passwords do not expire.

Strong passwords are an integral part of computer security. A poorly chosen password can result in unauthorized access and/or exploitation of the college’s network and computer resources. All users with user accounts are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

PASSWORD GUIDELINES
- Passwords must be at least 8 characters in length.
- Password must include at least one character from 3 of the following 4 classes: lowercase letters, uppercase letters, numbers, and punctuation/special characters (e.g. $, %, &, etc.).
- Employee passwords must be changed every 180 days.
- Never share your password with others.
- If an account or password is suspected to have been compromised, report the incident immediately to IT and change all passwords.
- Passwords should not contain any words found in the dictionary, or any part of your full name or account name, or other personal data.
- Passwords should never be written down or be viewable in open areas.
- Passwords should never be emailed.
- Never reuse passwords.
- An example of a secure password is "TmB1w2R!".

ACCOUNT LOCKOUT
If an individual fails to enter the correct password after three attempts, his or her user account is locked out for 15 minutes. After a period of 15 minutes the user account is automatically unlocked in which the account can be used again.
Reporting Problems

Policy Ref
PPM00157

Policy Title
Reporting Problems

Technology related problems that require immediate attention should be called in to (410) 334-2870. All other problems or projects must be reported by submitting an electronic work order in Track-It!.