Illinois Valley Community College Board Policy			
Subject:	**Use of Campus and Network Computing Resources**	Effective Date:	10/19/10
		Last Reviewed:	04/14/16
Number:	**5.4**	Last Revised:	10/19/10

Illinois Valley Community College (IVCC) makes available computing and network resources for students, faculty, and staff, and community/guest users. The resources exist solely for educational purposes to carry out the legitimate business of the College, the Board of Trustees, and the IVCC Foundation. All users of Illinois Valley Community College campus and network computing resources are responsible for using these resources in an effective, ethical and lawful manner, and in accordance with IVCC Administrative Procedures (5.4 a, b, c, and d). The College's technology resources and the data entered, created, received, viewed, accessed, stored or transmitted by the College's technology resources are College property with the exception of student-created work stored on network drives or unless stipulated otherwise by the Intellectual Property Rights agreement between the College and IFT Local 1810 (Article VI, A) or IVCC Board Policy 4.18 Ownership of College Commissioned Works, or any applicable law. Acceptable and unacceptable uses of resources are outlined in related procedures. Users should:

- Exercise personal responsibility for understanding limits and privilege of computing resources.
- Use resources legally and ethically.
- Understand related privacy and ownership issues.
- Conserve and protect resources.

Enforcement:
Abuse of computing privileges and failure to observe this policy will result in disciplinary action. Computing privileges will be revoked and violators will be subject to the due process procedures of the College as outlined in the Student Code of Conduct, the Administrative Procedures, IVCC Employee Handbook, or the IVCC Board of Trustees Policy Manual. In case of conflict, local, state or federal laws and regulations will supersede this policy. Action taken by IVCC in accordance with this policy or related administrative procedures does not eliminate the possibility of legal action taken by the College or by others.

A copy of the Use of Campus Network and Computing Policy, as well as the accompanying Administrative Procedures will be made available to students, and will be available to all employees with a sign-off sheet acknowledging receipt and understanding.

Illinois Valley Community College Administrative Procedure

Subject:	**Acceptable Usage Guidelines for Computer and Internet Resources**	Effective Date:	10/19/10
		Last Reviewed:	04/14/16
		Last Revised:	04/14/16
Number:	**5.4 (a)**		

Computing and networked resources are available to students, College employees and community/guest users for the educational and administrative purposes of IVCC. General student access to computing and networked resources is provided in open lab areas and throughout the campus via wireless access. Other computers and computer labs are restricted to students in specific programs or courses. College staff members are available to help student users and new employees gain the computer access appropriate to their course of study or type of work. IVCC works with external partners to bring technology resources to campus, and has agreed to comply with the Acceptable Use policies of these entities.

Use of the campus computing resources is a privilege and not a right, and may be suspended during an investigation of alleged misconduct, and possibly terminated when improperly used. The following guidelines must be followed by all persons who use the College computing and networked resources, whether accessing them from on or off campus.

Guidelines and Prohibited Practices

Exercise personal responsibility

1. Users are required to learn, understand, and follow the guidelines for each type of computer, lab, or other electronic resource.
2. Users must only access those computing and information technology resources and data for which they have authorization and only in the manner and to the extent authorized.
3. Installing software or connecting any device to the College's network without prior consent from the IVCC Department of Information and Technology Services (ITS) is prohibited.
4. Persons to whom an individual account is issued are responsible at all times for its proper use. Passwords are assigned to approved users and may not be shared or transferred to someone else. Passwords should be changed frequently. Users are cautioned not to leave a computer logged in and unattended in a public area or classroom.

Use resources legally and ethically

5. Users should become aware of local, state, and federal laws governing certain aspects of computer and telecommunications use. Members of the College community are expected to respect these laws, as well as to observe and respect

College rules and regulations. Users may not engage in unauthorized copying or distribution of software, graphics, text files, music or video, including peer-to-peer and file sharing (see IVCC Board Policy 4.16 Copyright). Users are prohibited from transmitting fraudulent, harassing, or obscene messages and /or other materials over the Internet or any other directly connected network on or off campus. Users must exercise respect for others who may be offended by content displayed on a computer monitor or laptop, whether college-owned or otherwise. Some content is expressly prohibited [See Administrative Procedure 5.4(d)].

6. Prohibited unethical activities include, but not limited to, attempts to obscure the origin or content of a message or document; using College resources to promote personal financial gain of self or other individuals or entities; IVCC employee use of College resources to engage in political activities; activities that might damage the reputation of the College; and employee misrepresentation of personal opinion as the official position or viewpoints of the College.
7. Incidental personal use of computing and network resources by employees (e.g. redirecting email to personal account; unsubscribing to listservs or commercial messages, etc.) is acceptable.

Understand related privacy and ownership issues

8. Employees are expected to store work in network storage space. Files will be retained according to IVCC Record Retention Guidelines & Procedures.
9. All contents of files located anywhere on the computer or network equipment owned or maintained by the College may be reviewed by the College, its agents and designees, at any time for the purpose of investigating possible violations of Board Policy 5.4, or any alleged criminal violations. Users have no reasonable expectation of privacy with regard to any such search of contents of files located anywhere on the computer or network equipment owned or maintained by the College.
10. An employee may make a request to have the ITS department access, retrieve, or move his or her own files from their networked account. With the exception of faculty-owned files, this action may also be initiated by the individual's department head, provided the file is needed to carry out College business.

Conserve and protect resources

11. Game playing, use of chat rooms, social networking sites, music, video and other graphic-intensive Internet sites that are not course-related consume needed bandwidth. Their use may be limited or curtailed at peak times by ITS. Employees are prohibited from accessing such sites that are not job-related during scheduled work hours.
12. Users must not knowingly create, send or forward electronic chain letters, viruses, worms, or spam, or any other malicious software.
13. All users contribute to the protection of campus computing resources. Users are responsible for reporting any observed gaps in system or network security to the College's ITS Department.

Observed Violations and Enforcement

Observed violations of Board Policy 5.4 and/or its related administrative procedure [5.4(a), (b), (c), and (d)] should ultimately be reported to the Director of Information and Technology Services. Notification may originate from students, through computer lab employees, faculty members, or administrative staff. If the case is an alleged student violation, the matter will be referred to the Vice President for Student Services for consideration under the provisions of the Student Code of Conduct. If the case is an alleged IVCC employee violation, the matter will be referred to the Vice President for Business Services and Finance, and the Director of Human Resources, or the individual's immediate supervisor per the appropriate Administrative Procedure(s).

If, in the opinion of the Director of ITS, a violation is committed that is excessive or a blatant attempt to undermine the use of the Internet or IVCC computer resources, ITS reserves the right to disregard the warning process and immediately disable the user's account. The matter will then be turned over to the Vice President for Student Services (student violation) or the Vice President for Business Services and Finance (employee violation) for further action.

ITS will cooperate fully, upon the advice of College legal counsel, with any local, state, or federal officials investigating an alleged crime committed by an individual who has an account on the Illinois Valley Community College computer or networking system. The College will also cooperate with regulations enumerated in the Acceptable Use Policies of the Illinois Century Network (http:.//www.illinois.net/AUP.pdf).

Illinois Valley Community College Administrative Procedure

Subject:	**Bandwidth Shaping & White Listing Procedures**	Effective Date:	10/19/10
		Last Reviewed:	04/14/16
Number:	**5.4 (b)**	Last Revised:	04/14/16

IVCC is committed to student, faculty, and staff access to technology for educational, research, or community outreach purposes as top priorities. Some technology applications, such as social networking (Facebook and Twitter), streaming video, and other graphic-intensive, interactive sites consume high levels of bandwidth that may result in slowed or unsuccessful Internet access at peak times.

IVCC reserves the right to conserve the bandwidth of the College's access to the Internet in order to regulate technology resources, by:

1. Filtering out questionable email (SPAM) before it reaches the College;
2. Limiting or preventing high bandwidth Internet traffic to and from the College;
3. Blocking access to specific Internet sites.

Internet domains and addresses can be added to "White Lists" to insure that access to these websites or email from these addresses will not be blocked. Requests for adding domains or addresses to the White Lists, along with justification for the request, should be sent to the Help Desk at 555@ivcc.edu.

If a situation requires immediate action, the Director of Information and Technology Services will make the decision, and the Strategic Leadership and Planning Council or President's Council will review what was blocked, filtered or limited, and take official action at its next meeting.

Illinois Valley Community College Administrative Procedure

Subject:	**Email Retention and Release Guidelines**	Effective Date:	10/19/10
		Last Reviewed:	6/6/22s
Number:	**5.4 (c)**	Last Revised:	7/14/22

IVCC email is retained on active servers as required by applicable legal authority**.** Employees may utilize local archiving or other methods consistent with his/her work practices. Searchable content management applications are available for email retrieval for College business use, litigation, or Freedom of Information Act (FOIA) requests.

All e-mail which constitutes a public record shall be subject to this policy. Public record is defined as "all records, reports, forms, writings, letters, memoranda, books, papers, maps, photographs, microfilms, cards, tapes, recordings, electronic data processing records, recorded information and all other documentary materials, regardless of physical form or characteristics, having been prepared, or having been or being used, received, possessed or under the control of any public body" [5 ILCS 140/2(c)]. College email has been construed to meet this definition.

The Freedom of Information Act, Subsection 7 (1) a-z, Exemptions, provides guidance for situations, such as email, where portions of the documentation constitute public record and other portions do not.

If an email is not a public record, the employee responsible for the creation or receipt of the email should delete it as soon as practicable unless the email is subject to a litigation hold.

In addition, some information may be prohibited from disclosure or withheld from disclosure by the College due to state or federal law or regulations.

In an instance where a request is made to access one of the potentially exempt documents, the request will be reviewed and acted upon by the College President and FOIA Officer (Vice President for Business Services and Finance) based upon the requirements of the

Freedom of Information Act (5 ILCS 140/1(et seq.), the State of Illinois Local Records Act (50 ILCS 205/1 et. seq.), the State Records Act (5 ILCS 160/1 et. Seq.), IVCC Board Policies, and all other applicable state and federal statutes and regulations.

Illinois Valley Community College Administrative Procedure			
Subject:	**Discovery and Reporting Child Pornography and the Illinois Abused and Neglected Child Reporting Act (ANCRA)**	Effective Date:	10/19/10
		Last Reviewed:	04/14/16
Number:	**5.4 (d)**	Last Revised:	04/14/16

Under 325 ILCS 5/1 Abused and Neglected Child Reporting Act – Section 4.5, information technology workers and their employers are required to immediately report any child pornography images discovered on electronic and information technology equipment to local law enforcement. Compliance with this Act fulfills the concurrent obligation under Title 42 U.S. Code 13032, which offers the additional reporting option through the cyber tipline at the National Center for Missing and Exploited Children (http://www.cybertipline.com).

Any Information and Technology Services (ITS) staff member who discovers possible child pornography on a College computer must report the discovery immediately to the Director of Information and Technology Services. The Director of ITS is responsible for notifying the proper authorities. Other employees who have knowledge of possible child pornography on an employee's computer are required to inform the Director of Human Resources and/or appropriate Vice President or Associate Vice President. The Director of Human Resources will initiate an investigation, and if warranted, notify the proper authorities.

Any user whose computer is reported as a source of possible child pornography will have the user account immediately disabled and the matter will be turned over to the Director of ITS to secure the hard drive and/or history for further investigation.

Under 325 ILSC 5/4 Abused and Neglected Child Reporting Act (ANCRA) – Section 5.4, personnel of institutions of higher education having reasonable cause to believe a child known to them in their professional or official capacity may be an abused child or a neglected child shall immediately report or cause a report to be made to the Illinois Department of Children and Family Services.

Reports may be made to the DCFS hotline (1-800-25 ABUSE) or in person followed by a written report within 48 hours. IVCC's employee duty to report is absolute, and it rests with the individual identifying the suspected abuse or neglect. DCFS recommends that, if in doubt about whether to report, the reporter should report the suspected abuse.
Any person, who enters into employment with IVCC is mandated by virtue of that

employment to report under the ANCRA, shall sign a statement to the effect that the employee has knowledge and understanding of the reporting requirements of this Act. The statement shall be signed prior to commencement of the employment. The signed statement shall be retained by IVCC in the employee's personnel file.

All employees of IVCC are required to complete the DCFS on-line training. This on-line training could take 60-90 minutes and must be completed prior to employment. This on-line training is also required of any volunteer camp workers or volunteer coaches.

Faculty and Staff Acknowledgment
& Statement of Agreement

I acknowledge that I have received a copy of the Illinois Valley Community College Use of Computer and Network Computing Resources Policy 5.4 and associated Administrative Procedures and that I have read and understand these documents. I further understand that I must comply with all of the provisions of the Policy and the associated Administrative Procedures in order to have access to and use College technology resources as an employee of the College.

I understand that the College's technology resources and the data entered, created, received, viewed, accessed, stored or transmitted by the College's technology resources are College property, unless stipulated otherwise by the Intellectual Property Rights agreement between the College and IFT Local 1810 (Article VI, A) or through IVCC Board Policy 4.18 Ownership of College Commissioned Works, and as otherwise provided by law. I acknowledge my understanding that the College reserves the right to access, inspect, monitor, intercept, or review any and all information transmitted via College technology resources in accordance with Policy 5.4, its associated Administrative Procedures, and in accordance with state and federal law.

I also understand that if I do not comply with all provisions of the Policy, my access to College technology resources will be revoked, and I may face further disciplinary action.

Name (please print) _____

_____

Signature Date

_____

Witness Signature Date