Acceptable Use Policy

1.0 Purpose

The computing resources at PIEAS support the educational, instructional, research, and administrative activities of the Institute and the use of these resources is a privilege that is extended to members of the PIEAS community. As a user of these services and facilities, you have access to valuable Institute resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the Institute will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the Institute as deemed by the Disciplinary Committee. Individuals are also subject to federal, state and local laws, promulgated from time to time, governing many interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change.

An acceptable use policy (AUP) is a policy that a user must agree to follow in order to be provided with access to a network or to the Internet. This document establishes specific requirements for the use of all computing and network resources at PIEAS.

2.0 Scope

This policy applies to all users of computing resources owned or managed by PIEAS. Individuals covered by the policy include (but are not limited to) PIEAS faculty and visiting faculty, staff, students, alumni, guests or proxies, external individuals and organizations accessing network services via PIEAS' computing facilities.

Computing resources include all Institute owned, licensed, or managed hardware and software, and use of the Institute network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies apply to technology administered in individual departments, the resources administered by central administrative departments (such as the Institute Library and Computer and Internet Services Division), personally owned computers and devices connected by wire or wireless to the campus network, and to off-campus computers that connect remotely to the Institute's network services.

2.1 Your Rights and Responsibilities

As a member of the PIEAS community, the Institute provides you with the use of scholarly and/or work-related tools, including access to the Library, to certain computer systems, servers, software and databases, and to the Internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether you are a Institute employee or a student), and of protection from abuse and intrusion by others sharing these resources. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.

In turn, you are responsible for knowing the regulations and policies of the Institute that apply to appropriate use of the Institute's technologies and resources. You are responsible for exercising good judgment in the use of the Institute's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

As a representative of the PIEAS community, you are expected to respect the Institute's good name in your electronic dealings with those outside the Institute.

3.0 Policy

3.1 Acceptable Use

- You may use only the computers, computer accounts, and computer files for which you have authorization.
- You may not use another individual's account, or attempt to capture or guess other users' passwords.
- You are individually responsible for appropriate use of all resources assigned to you, including the computer, the network address or port, software and hardware. Therefore, you are accountable to the Institute for all use of such resources. As an authorized Institute user of resources, you may not enable unauthorized users to access the network by using a PIEAS computer or a personal computer that is connected to the PIEAS network.
- The Institute is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.
- You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing PIEAS's network and computing resources.
- You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- You must comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- You must not use PIEAS computing and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.
- On PIEAS network and/or computing systems, do not use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless you have been specifically authorized to do so.

3.2 Prohibited Use

CISD reserves the absolute right to define prohibited use of the Network, adopt rules and regulations applicable to Network use, determine whether an activity constitutes a prohibited

use of the Network, and determine the consequence of such inappropriate use. Prohibited use includes but is not limited to the following:

3.2.1 Violating any provincial or federal law and ordinance, such as:

- Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials;
- Criminal activities that can be punished under law;
- Altering system software or hardware settings that hamper the use of equipment.
- Users will not install software not previously approved by CISD.
- Selling or purchasing illegal items or substances;
- The unauthorized collection of email addresses ("harvesting") of e-mail addresses from the Global Address List and other directories;
- Obtaining and/or using anonymous email sites; spamming; spreading viruses;
- Circumvention of CISD protection measure/filter to access blocked sites;

3.2.2 Causing harm to others or damage to their property, such as:

- Using profane, abusive, or impolite language; threatening, harassing, bullying or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
- Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
- Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
- Using any PIEAS computer to pursue "hacking,", or attempting to access information protected by privacy laws; or
- Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes".

3.2.3 Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:

- Using another's account password(s) or identifier(s);
- Interfering with other users' ability to access their account(s); or
- Disclosing your own or anyone's password to others or allowing them to use your or another's account(s).

3.2.4 Using the network or Internet for Commercial purposes:

- Using the Internet for personal financial gain;
- Using the Internet for personal advertising, promotion, or financial gain; or

- Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes.

3.3 Fair Share of Resources

Computing and Information Services, and other Institute departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The campus network, computer clusters, mail servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use them. Therefore, the use of any automated processes to gain technical advantage over others in the PIEAS community is explicitly forbidden.

The Institute may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

3.4 Adherence with Federal, State, and Local Laws

As a user of PIEAS's computing and network resources you must:

- Abide by all federal, state, and local laws.
- Abide by all applicable copyright laws and licenses. PIEAS has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.
- Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.
- Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution. For example
    - Taking a CD you own, you make copies of songs onto your computer, and set up sharing to allow others to access those songs from your computer.
    - Playing a video in a classroom for entertainment purposes, or for its cultural or intellectual value unrelated to a teaching activity.

3.5 Other Inappropriate Activities

Use PIEAS' computing facilities and services for those activities that are consistent with the educational, research and public service mission of the Institute. Other prohibited activities include:

- Use of PIEAS' computing services and facilities for political purposes. While running for political office or campaigning for a political figure, you use your PIEAS email account

to send out email about your or other's candidacy to people, and promoting you or other's as a candidate.

- Use of PIEAS' computing services and facilities for personal economic gain. Using a computer connected to PIEAS's campus network, you establish a commercial business, selling products or services over the Internet.
- You download, store, print and/or display materials that could be perceived by others as contributing to an intimidating, hostile, or sexually offensive working environment.
- You send out unauthorized and unsolicited email messages to other PIEAS community members.
- While someone else is using a computer, you want to check your email. You ask them to log in, giving them your password to type in for you.
- While traveling on vacation, you ask a proxy to check your email for you by giving them your password.
- A colleague is out sick, and he/she was receiving responses for an event. Rather than calling them at home to ask them to check their email, you attempt to gain access to their account by guessing their password.
- After having your computer hacked, you decide to download and run hacking tools yourself to help your friends out by checking for vulnerabilities on their computers.

3.6 Privacy and Personal Rights

- All users of the Institute's network and computing resources are expected to respect the privacy and personal rights of others.
- Do not access or copy another user's email, data, programs, or other files without the written permission of the Mail Administrator.
- Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to Institute discipline as well as legal action by those who are the recipient of these actions.
- While the Institute does not generally monitor or limit content of information transmitted on the campus network, it reserves the right to access and review such information under certain conditions. These include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that PIEAS is not subject to claims of institutional misconduct.
- Access to files on Institute-owned equipment or information will only be approved by specific personnel when there is a valid reason to access those files. Authority to access user files can only come in conjunction with requests and/or approvals from senior members of the Institute. The Disciplinary Committee may request access to files through valid subpoenas and other legally binding requests. All such requests must be approved by the Disciplinary Committee. Information obtained in this manner can be admissible in legal proceedings or in a Institute hearing.

3.5.1 Privacy in Email

- While every effort is made to insure the privacy of PIEAS email users, this may not always be possible. In addition, since employees are granted use of electronic information systems and network services to conduct Institute business, there may be instances when the Institute, based on approval from authority (Inquiry Committee, Disciplinary Committee), reserves and retains the right to access and inspect stored information without the consent of the user.

3.6 User Compliance

When you use Institute computing services, and accept any Institute issued computing accounts, you agree to comply with this and all other computing related policies. You have the responsibility to keep up-to-date on changes in the computing environment, as published, using Institute electronic and print publication mechanisms, and to adapt to those changes as necessary.

Effective Date: June 16, 2013

Version Control No.	Section Changed/Modified	Document Control Authority	Effective Date
1.0	-	Head CISD	June 16, 2013

Change Control Board:

- Rector, PIEAS
- Pro-Rector, PIEAS
- Head CISD
- Network Administrator
- Mail Administrator
- WebMaster