SIAST
SASKATCHEWAN INSTITUTE OF APPLIED SCIENCE AND TECHNOLOGY

Policy and Procedure Statement

SUBJECT:	CATEGORY:	NO.
Appropriate Use of Information Technology Resources	**Information Management**	**801**

PREAMBLE

In support of its mission in teaching, learning and services, SIAST makes computing, network and other information technology resources available to its employees and students.

POLICY

This policy applies to all employees and students within the SIAST community and to others who have been granted the use of SIAST's information technology resources. This policy refers to all information technology resources within SIAST whether individually controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated or contracted by SIAST including personal computers, smartphones, PDAs, networks and associated peripherals and software. All individuals having access to SIAST's computing systems are bound by Canadian and Saskatchewan laws and statutes relating to copyright, obscenity, harassment and security regarding electronic media.

1.0 Responsible and authorized use.

All students and employees are entitled to use SIAST computing facilities for which they have been authorized. As such, all users of SIAST-owned or SIAST-leased information technology resources must:

1.1 Take responsibility for the integrity of the resources under their control;

1.2 Respect the rights of others, including safe guarding the privacy of person-to-person communication and other personal and confidential information.

1.3 Respect and comply with all laws, SIAST policies, copyrights, software licenses, contractual agreements and intellectual property rights (reference SIAST copyright policy #117).

1.4 Use the computing system for bona fide educational purposes in support of SIAST's goals and objectives. Other uses not authorized by SIAST, such as conducting commerce, are not permitted (see SIAST conflict of interest policy #704). The computing system may be used for incidental personal use.

1.5 Abide by the security practices, measures and restrictions in place.

1.6 Have proper authorization for the technology resources used and accessed.

1.7 Provide proper and correct sender identification in all electronic correspondence.

1.8 Not monitor network transmissions and general network traffic on SIAST networks.

1.9 Not use computing and network resources to access, create, view, listen to, store or transmit material that is harassing, obscene, abusive, illegal, pornographic, discriminatory or that otherwise violates applicable laws, SIAST policies or community standards.

The foregoing is **not** intended as an **exhaustive** list of permissions and prohibitions governing the use of computing and network resources. Sections 342.1, 430 and other parts of the Criminal Code as well as parts of the Canadian Charter of Rights and Freedoms and other relevant legislation are also pertinent. Individuals must report violations of this policy and possible security lapses to the Information Technology Services department to ensure SIAST's information technology resources can be maintained.

2.0 Rights of authorized users.

All users of SIAST-owned or SIAST-leased information technology resources must be aware that access to technology resources is a privilege. However, having been granted the privilege, authorized users of SIAST's computing system have certain rights with respect to their studies or employment including:

2.1 Access shall not be denied or removed without just cause.

2.2 The resources and other devices or networks to which they are connected will not be violated by misrepresentation, tampering, destruction or theft.

2.3 A right to privacy but not absolute privacy of their files, data and electronic mail unless the integrity and availability of SIAST's computing system is jeopardized.

2.4 Authorized access to and use of the resources will be protected by SIAST as is technically and reasonably possible.

3.0 Maintenance of resources by SIAST Information Technology Services.

3.1 All files on SIAST computers are owned by SIAST and are the property of SIAST. SIAST reserves the right to inspect that property in appropriate circumstances and take measures to ensure the integrity and availability of SIAST's information technology resources.

3.2 Information Technology Services has the right to examine files, data and email to gather sufficient information to diagnose and correct system hardware and software problems or to determine is a user is acting in violation of the policies stated in this document.

3.3 Information Technology Services has the right to suspend an account or access to SIAST's networks without prior notification to users if they are deemed to be in violation of SIAST policies.

4.0 SIAST reserves the right to recover from its employees any direct or indirect costs incurred as a result of any violation of this policy, in addition to any other disciplinary sanctions which may be imposed.

PROCEDURES

1.0 All new students and employees will be made aware of this policy during the appropriate orientation process.

2.0 Inappropriate use by students:

2.1 Suspected violations of this policy by a student are to be reported to the student's program head.

2.2 If required, Information Technology Services will assist the program head to determine if a violation of this policy has occurred. A program head requesting assistance must specify the nature of the suspected violation prior to an investigation beginning.

2.3 Should a violation of this policy be confirmed, the program head will determine if the violation requires suspension of privileges and notify Information Technology Services accordingly.

2.4 Other penalties may be imposed in accordance with established SIAST policies. If the violation is determined or suspected to be of a criminal nature, the matter will be referred to appropriate law enforcement authorities.

3.0 Inappropriate use by employees.

3.1 Suspected violations of this policy by an employee are to be reported to the individual's supervisor.

3.2 The supervisor, in consultation with Human Resources, will determine if further investigation is required.

3.3 If required, Information Technology Services will assist the supervisor and Human Resources to determine if a violation of this policy has occurred. A supervisor requesting assistance must specify the nature of the suspected violation prior to an investigation beginning.

3.4 The supervisor, in consultation with Human Resources, may request immediate suspension of access privileges if warranted. The individual suspected of a violation will be informed of the access privilege suspension as soon as reasonably possible by their supervisor.

3.5 Information Technology Services will not begin their investigation until the individual under investigation has been notified of the investigation by the supervisor. At the time of notification, the individual's computer may be removed by Information Technology Services and replaced with a temporary device. If removed, the individual's computer will be stored with Human Resources to ensure the device is properly secured to prevent any tampering with the contents of the computer.

3.6 At the conclusion of the investigation, Information Technology Services will provide a report to the supervisor and Human Resources.

3.7 Any access privileges suspension will be lifted upon the authorization of the individual's supervisor.

3.8 Other penalties may be imposed in accordance with established SIAST policies. If the violation is determined or suspected to be of a criminal nature, the matter will be referred to appropriate law enforcement authorities.