ALBERTA COLLEGE OF ART + DESIGN

ACAD

ACCEPTABLE USE POLICY

Policy #:	600.01.01
SECTION:	Computing + Technical Services
ORIGINAL APPROVAL DATE:	April 24, 2018
LATEST APPROVAL DATE:	**April 24, 2018**
APPROVING AUTHORITY:	Original Signed by President + CEO

Purpose

This policy establishes, controls, and manages the appropriate use of Alberta College of Art + Design information assets.

Scope

This policy shall apply to all authorized users of ACAD information assets regardless of the location or mode of access.

Definitions

Authorized Users:	Include students, staff, faculty, employees and third party users such as contractors, consultants, temporary or guest users, suppliers and service providers that have agreed to the terms of this procedure.
Information Assets:	Include all business applications, infrastructure related applications, databases, networks, operating systems, technology infrastructure, intranet, email, and hand held devices, wireless devices, security devices, files, and data.

Policy

1 General Asset Provision and Use

1.1 ACAD will provide the equipment and information assets necessary for the satisfactory completion of the duties and/or responsibilities of authorized users.

1.2 ACAD information assets shall only be used for authorized activities and purposes related to Authorized Users' legitimate functions and in an appropriate and safe manner.

1.3 Eligible ACAD Community members are permitted use of ACAD information assets:

1.3.1 When registered in a program of study;

1.3.2 For the purpose of employment;

1.3.3 For the purpose of fulfilling a contract, or

1.3.4 As authorized guest users (e.g. retirees, alumni).

2 Authorized User Acknowledgement

2.1 Acknowledgement and acceptance of this policy and associated policies and procedures as identified under the references is a condition of employment or enrollment for authorized users. This policy must be read and acknowledged by all authorized users.

3 Conditions of use

3.1 All such provided equipment remains the property of ACAD and authorized users may be requested to either produce the equipment for inspection or return the equipment, at any time, without notice.

3.2 Unauthorized use of information assets and equipment is prohibited as it may increase ACAD's risk of exposure to loss, virus attacks, network disruptions, services interruptions, and legal or regulatory compliance issues.

4 Acceptable Use

4.1 Users shall:

4.1.1 Comply with ACAD policies, procedures and guidelines regarding the use of ACAD information assets as applied to user access, social media use and conduct, and appropriate website use.

4.1.2 Be aware that the files they create on ACAD information assets remains the property of ACAD and that the Intellectual Property of the data is subject to all ACAD policies, procedures and guidelines related to Intellectual Property.

4.1.3 Store data on the network where it can be backed up as part of the regular backup procedure.

4.1.4 Use Information Assets in the way they were intended to be used.

4.1.5 Not alter or modify any operating system, software, hardware and/or system set up or configuration component compromising its security or safety.

4.1.6 Ensure personal use does not compromise the business objectives of ACAD and exercise good judgment regarding the reasonableness of personal use. All personal use of ACAD's information assets, including programs, data, system access, or equipment, are subject to review.

4.1.7 ACAD reserves the right to monitor networks and systems on a periodic basis to ensure compliance with this policy as well as related policies and procedures.

5 Unacceptable Use

5.1 Users shall not use ACAD information assets to:

5.1.1 Create negative impact on ACAD.

5.1.2 Violate any laws or participate in a crime or other unlawful or improper purpose.

5.1.3 Cause intentional harm or disruption to ACAD information assets.

5.1.4 Gain unauthorized access to other systems or other organizations' systems.

5.1.5 Actively engage in procuring or transmitting material that is in violation of the sexual harassment or workplace laws in the user's local jurisdiction.

5.1.6 Intentionally interfere with, or disable, another user's connection (session), through any means e.g., locally or through the Internet.

5.1.7 Distribute to any external parties any product or information asset without an appropriate authorization.

5.1.8 Initiate actions that defeat or circumvent corporate security measures and restrictions put in place by ACAD Management.

5.1.9 Create or introduce computer-based materials which are intended to be harmful to the operation of any computing system (e.g. Viruses).

5.1.10 Violate the Respectful Workplace policy and related Procedure 400.02.: Respectful Workplace.

5.1.11 Copy information classified as Confidential or Internal Use - Protected without authorization.

5.1.12 Install or distribute unlicensed software products.

5.1.13 Install malicious programs such as viruses, worms, etc. On ACAD information assets.

5.1.14 Reveal your account password to others or allowing the use of your account by others.

5.1.15 Carry out fraudulent activities using any ACAD computer account.

5.1.16 Initiate actions to gain unauthorized access to ACAD information assets including, but not limited to accessing data for which you are not the intended recipient.

5.1.17 Execute any form of network monitoring that will intercept data not intended for you except when this is part of a technician's authorized monitoring/troubleshooting responsibilities.

5.1.18 Circumvent user's authentication or access security of any ACAD information assets.

5.1.19 Deliberately interfere with or denying service to any legitimate user.

Note: Unmodified personal phones, tablets and laptops are allowed guest Wi-Fi access. Devices infected with malware must be disconnected immediately upon notification.

6 Enforcement

6.1 Corporate Services shall communicate the acceptable use procedure to all authorized users of ACAD information assets.

6.2 If there is evidence to show that these provisions have been violated, progressive remedial action may be taken under the direction of C+TS. (See Appendix I)

Roles + Responsibilities

7 Authorized Users

7.1 Understand and acknowledge the Acceptable Use Policy and related documents

8 Computing and Technical Services (C+TS)

8.1 Maintain current records of all authorized users, their account information and access privileges

8.2 Grant access privileges only as required to fulfill their functions.

8.3 Monitor network performance, traffic flow and resource utilization

8.4 Investigate violations of acceptable use guidelines and take corrective actions

8.5 Maintain evidence of noncompliance with this procedure in order to implement remedial action as required

9 Information Technology Steering Committee (ITSC)

9.1 Review violations to the procedure and recommend corrective action

9.2 Regularly review the procedure and update as required

Related Documents

ACAD Information Security Policy

Information Technology Steering Committee (ITSC) – Terms of Reference Appendix I: Remedial Action Pathway

Procedure 500.14.: Student Code of Conduct

Procedure 600.26.: Information Technology User Access

Policy 500.01.01: Copyright

Procedure 500.11.: Copyright

Procedure 600.14.: Social Media

Procedure 600.15.: Website

Procedure 400.02.: Respectful Workplace

Remedial Action Pathway

In order to maintain an efficient and effective work environment, when it is necessary, C+TS will take progressive corrective action.

10 Remedial Actions

10.1 Clear expectations

10.1.1 Expectations of ACAD Community members utilizing CTS assets and equipment are documented in Information Technology Procedures. It is expected that all community members are aware of their responsibilities as documented in the current versions of these procedures. The ACAD helpdesk is available for consultation and clarification, as required.

10.2 Training

10.2.1 Where possible, ACAD Community members will be offered training on subjects that influence the Information Technology environment.

10.3 Coaching

10.3.1 ACAD Community members will receive coaching from members of the ACAD Helpdesk to discuss any unacceptable use or behaviours that persist. Coaching may include review of typical actions taken by the community member, identification of warning signs and/or flags, preventative or corrective actions that can be taken while completing daily work.

10.4 Corrective Action

10.4.1 Is action taken by the C+TS, in consultation with the employee supervisor and the next progression should Remedial Actions fail to resolve the risk to ACAD. Certain threats to the IT environment will prompt CTS to take corrective action up to and including suspension of account privileges. Notice of corrective action will be provided to supervisors (for staff) or Student Affairs (for students) as necessary.

10.5 Disciplinary Action

10.5.1 Is action taken by the supervisor, in consultation with Human Resources and the C+TS department. This action is necessary when Remedial and Corrective actions have failed to address the risk to ACAD.

Table 1

Remedial Action				
Clear expectations *Policies, Procedures, Guidelines* ↘ **Training** ↘ **Coaching** ↘				
Corrective taken by C+TS				
Least Severe	**Written Warning** →	**Suspension of Account** →	**Cancellation of Account**	*Most Severe*
Disciplinary Action				