



Vermont College of Fine Arts
Information Technology Use Policy
Revised September 2010

Introduction:

This policy applies to all persons and equipment utilizing the information technology resources. This includes, but is not limited to, faculty, staff, students, conference services guests, and authorized individuals or organizations.

The information technology resources of Vermont College of Fine Arts (VCFA) support the instructional and administrative activities of the College. These resources include, but are not limited to, information technology assets, local area networks, wireless networks, servers, client workstations, electronic mail, Internet access, voice mail, video conferencing and other related services.

Users of the information technology resources have access to valuable University resources, to sensitive data, and external networks.

Authorization to use Information Technology Resources:

VCFA reserves the right to limit, restrict or extend computing privileges and access to information technology resources. If the use or access to an information technology resource is not explicitly given then it is unauthorized.

Privacy:

Users of information technology resources should be aware that administrative access to resources assigned to a user may occur. This access may be at the request of a user to correct a problem in their assigned resources, or in response to a system security, resource overload, or other event requiring administrative access. Access may also occur by law enforcement or judicial requirements.

All information stored on College systems is considered the property of the College and can be reviewed at the discretion of senior management.

Policies for use:

VCFA computers, networks and other information technology resources may not be used in any manner prohibited by law, licenses, contracts, or college regulations.



Organizations, faculty, staff, students and other individuals are accountable for the information they publish across VCFA information technology resources. They must be aware of and abide by existing policies regarding confidential information, intellectual property, harassment, and the acceptable use of information technology resources.

Users are individually responsible for their use of the information technology resources to which they have been granted access. Sharing of personal accounts is prohibited.

Pranks, practical jokes, use of accounts without authorization, cracking systems or accounts, and malicious or unauthorized hacking are prohibited. Physical damage to information technology resources is prohibited. Email, executable binary programs, software, recordable media and data files should be treated as possibly containing computer viruses, worms or other destructive programs unless there is reliable evidence to the contrary.

College resources are shared resources. Be considerate and refrain from monopolizing systems, overloading networks with excessive data or wasting computer time, disk space, printer paper, manuals or other resources. It is a violation of federal and state laws and College policy to use technology resources to intimidate or single out individuals or groups for degradation or harassment. Use of College resources for private financial gain or compensation is prohibited.

Upon separation of employment from the College all College owned resources must be returned by the final day of in-office work to the IT Administrator.

User Responsibility for Laptops:

All employees shall take all precautions necessary to avoid damage or loss of a laptop computer in their possession. Costs incurred from damages or total loss of a laptop may be the responsibility of the assigned department if the circumstances are caused by intentional damage, improper care or neglect. The user or department shall report a stolen computer to a senior staff member and the Information Technology department as soon as possible.

The user is responsible for backing up any files from the laptop computer. For those employees located on campus, the Information Technology department offers network storage for this purpose.



Sensitive information should never be stored permanently on a laptop computer. All sensitive information should be stored on a designated network drive where the data is secure and backed up on a nightly basis. In the event that a user's data has been compromised, the user shall contact the Information Technology Department and the CFO immediately.

Remediation of policy violations:

Abuse of information technology resources, unauthorized access, inappropriate use, or violation of these policies is cause for dismissal and may result in disciplinary action per College regulations and, if applicable, prosecution under federal or state laws.

Accidental abuse, including but not limited to run-away computer processes, sudden loss of disk space on a shared device, loss of network bandwidth and accidental virus infestations may be corrected by the resource owner or department network manager. Reasonable efforts will be made to notify and educate the user who is abusing a resource if time permits before the resource or access to it is removed. The IT department may take appropriate action to eliminate the resource abuse including but not limited to the removal of offending processes, accounts and or files. Users suspecting they may have propagated viruses or worms should notify the IT department immediately.

The IT department will make a good faith effort to maintain resource security by applying security patches and taking other security measures.