Office of Information Resources Management

The American College of Greece

Acceptable Use of IT Resources Policy

Introduction and purpose

The American College of Greece (ACG) technological resources is for official use only. Use other than for College business, education, or research is prohibited. This policy familiarizes users with the purposes for which technological resources are provided, and the types of activities that are prohibited. The policy also informs users on their responsibilities toward ensuring acceptable use, and, provides other important information pertaining to the administration and operation of technology resources performed by the Office of Information Resources Management (IRM). Technological resources are provided by the College to support its primary role of education, research and associated functions related to this role. The College complies with, and adheres to, all its current legal responsibilities including under Data Protection, Electronic Communication and Intellectual Property legislation.

Responsible College Office & Officer

The Office of Information Resources Management (IRM) and its InfoSec Operations Team are responsible for the maintenance of this policy, and for responding to questions regarding this policy.

Who is governed by this policy?

This policy applies to all individuals who are granted access to ACG Technological Resources. Those individuals covered include, but are not limited to, faculty, staff, students, alumni, those who are working on behalf of the College, and/or individuals authorized by affiliated institutions and organizations. Exercising access to any ACG technological resource automatically signifies acceptance of this policy.

Definitions

Computer Network: Two or more computers that can share information, typically connected by cable, data line, or satellite link.

Intellectual Property: any product of the human intellect that is unique, novel, and unobvious and that fits, but is not limited to, one or more of the following categories: an idea, an invention, an expression of literary creation, a business method, an industrial process, a chemical formula, an issued patent, a copyrighted work, or a legal right inherent in a patent, copyright, trademark, or know-how or trade secret.

Internet: An international network of independent computer systems. The World Wide Web is one of the most recognized means of using the Internet.

Internet Services: include, but are not limited to, electronic mail, file transfer protocol, Telnet, news, and the World Wide Web

Sensitive System: A system that processes any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on ACG interests, the conduct of ACG programs, or the privacy to which individuals are entitled (e.g., Student Information System, Course Evaluation System, etc.)

Technological Resources: Technological resources include but are not limited to: computers and terminals, software, printers, networks and equipment, telecommunication equipment and services such as telephones, facsimile machines, modems, basic and long distance calling service, and voicemail; television and radio systems and equipment; computer information systems; and, data files and/or documents managed or maintained by the College which reside on disk, tape or other media. Technology resources also include multimedia equipped classrooms, computer classrooms, computer laboratories, computer offices, technologies equipped college residencies and computer furnishings operated or maintained by ACG.

Users: Faculty, staff and students as well as others who have been authorized to use The American College of Greece technological resources, i.e. contractors, interns, volunteers, etc.

General

ACG technological resources are the property of the College and they are provided to support the conduct of College business. Technological resources include but are not limited to information systems; computer hardware and software; network and telecommunications systems and services; and Internet access.

Procedures

I. Computer Network Accounts

Users are responsible for maintaining the privacy and security of their computer network account user logon names and passwords and for the computer information systems accessed through the network. Users are also responsible for the activities carried out under their user accounts. Users are granted access to computing, networks, telecommunications and electronically stored information contingent upon their prudent and responsible use. Access is granted to the individual only. Individuals are not authorized to transfer or share access with another.

II. No Privacy Expectation

Users should have no expectation of privacy in any message, file, image or data created, sent, retrieved, or received through the use of ACG’s systems and equipment. Electronic communication should never be considered private, confidential, or secure. For example, once sent, copies of e-mail can be forwarded to other parties and unintended recipients without the sender’s knowledge or permission. Messages transmitted should be prepared with the same level of care and discretion as paper-based correspondence. However, users should be aware that the College will make reasonable attempts to maintain the confidentiality and security of electronic communication.

ACG does not constantly monitor or access the content of data transmitted over the network or whether stored on College equipment or in transit on the College network. The content of electronic communications will not be accessed during the execution of systems support, network performance, and related security functions; but system administrators may by way of exception access and disclose such contents when required or permitted by law, including, without limitation when access and disclosure are necessary to protect the integrity of information technology resources, to ensure that these resources are equitably shared, to respond to health and safety emergencies, or to respond to subpoenas, court orders, or other valid forms of legal process or following prior written consent of the user. In any case, the access to, and disclosure of, the contents of electronic communications is subject at all times to the applicable Greek and European Community Data Protection Legislation. Where there is evidence of a criminal offense, the matter will be reported to ACG's judicial systems and/or law enforcement. The College will cooperate with the justice system in the investigation of the alleged offense.

In addition, with appropriate authorization, the College will investigate complaints received from both internal and external sources about unacceptable use of ACG's technological resources. Cases that involve unacceptable use should be immediately reported. Requests to access, investigate or disclose the content of user data will be handled within the following guidelines:

If the account belongs to a:	Then written permission must be obtained from:
Faculty Member, Student	Provost or Chief Academic Officer or the President (in cooperation with the Vice President of Administration and the Academic Deans).
Staff Member (incl. student employees)	Vice President of Administration.

All requests to access or disclose the content of a user account, including detailed information on why the request is being made, should be sent from the appropriate person authorized above to the Executive Director for IRM, for processing. If the request is the result of a court order, then written permission from the above authorized person is not required.

With the exception of content covered by the College's intellectual property policy, all electronic information residing on College owned systems and all Internet traffic generated through or within these systems, is the property of the College. They are not the private property of any College employee, faculty, staff, contractor, student, or other person.

III. User Responsibilities

When using University technological resources, users must:

1. Use the systems only for approved purposes and in accordance with College policies.
2. Maintain the conditions of security under which they have been granted access.
3. Make every effort to ensure that downloading of network and/or Internet-based material is performed in as safe a manner as possible.
4. Check with IT Services or IT Helpdesk (helpdesk@acg.edu) prior to downloading material that may have potential to affect network security and/or integrity (e.g. a virus-infected file).
5. Respect intellectual property rights, including but not limited to applicable software copyright laws.
6. Observe the applicable policies of external networks when they are accessed.
7. Show valid College identification when requested by authorized personnel.
8. Promptly report any policy violations, destruction of data/information or equipment, and other problems to the Office of Information Resources Management.
9. Closely observe the acceptable use of e-mail as it is explained by the College E-Mail policy.
10. Never engage in any of the prohibited activities specified below.

Users are to take precautions to prevent the unauthorized use of their ACG user accounts and account passwords. Account passwords must follow the college's Password Policy.

IV. Prohibited Activities

Within reason, freedom of speech and access to information for college business and academic purposes will be honored. However, users must never act in an improper, inappropriate, indecent, or injurious manner when using the technological resources of the College. Prohibited activities include, but are not limited to:

1. Using College technological resources for personal gain or to further personal views, religious or political causes, soliciting or marketing of commercial ventures, or performing other non-job related solicitations;

2. Intentionally accessing, downloading, printing or storing information with sexually explicit content which is prohibited by law.
3. Intentionally downloading and/or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful or inappropriate messages or images.
4. Intentionally installing and/or downloading unauthorized or personal computer software/programs and executable files, without proper approval; the only authority for performing installations or modifications of software on ACG owned hardware is the Office of Information Resources Management staff only.
5. Uploading, downloading, storing, or transmitting copyrighted materials or proprietary information without proper approval.
6. Uploading, downloading, storing, or transmitting access-restricted College information in violation of College policy or without proper approval.
7. Installing or using proprietary encryption hardware/software.
8. Intentionally permitting unauthorized individuals to use University technological resources in any manner.
9. Adding, removing, or modifying ACG owned or administered equipment, data, or documents without specific authorization by the owner or designated administrator.
10. Intentionally downloading video, audio, data, or any other files that cause excessive network and/or computing system traffic or load.
11. Providing information about or lists of ACG users to external organization or individuals without proper authorization or approval.
12. Tampering, defeating or attempting to defeat security systems (locks, surveillance cameras, alarms, firewalls, networks, etc.), attempting or gaining unauthorized access to College information, information technology, facilities, systems and/or other IT-based resources, and/or using proxies, info gathering, encryption, covert channels or other software and measures to bypass information and physical security controls.
13. Knowingly introducing computer viruses, worms, or similar types of programs into computer systems.
14. Denying/attempting to deny or to interfere with College services.
15. Although not strictly prohibited, users must be cautious when attaching the following internal or external devices (external drives, USB sticks, interface cards, or video systems, etc.,) to ACG equipment because this can cause internal conflicts as well as damage to systems and might result in service disruptions.
16. Any other activities prohibited by College, and Greek regulations.

The following additional security precautions apply to College employees, faculty, contractors, temporary employees, student workers, external parties, and others accessing College sensitive systems and data:

17. Accessing websites which are not directly related to the conduct of College business while accessing a sensitive College system.
18. Installing, using online chat applications, computer games, peer-to-peer file sharing software or other software which is not directly related to the conduct of College business.
19. Installing non ACG authorized online storage applications, such as Google Drive, or storing College data on online storage without written permission.

20. Copying or storing, sensitive College data on personal storage, personal computing devices, mobile devices, or any other unapproved media.
21. Transmitting, uploading, downloading, or emailing, sensitive College data to non-College or unapproved systems.

V. Personal Use

The College permits the use of its IT facilities by students, staff and other authorized users for a reasonable level of personal use. Personal use of College equipment is a privilege, which the College reserves the right to withdraw without notice. Reasonable and proportionate use of the College for personal use is permitted, subject to regulations that may be set out from time to time by the College administration. The use of ACG IT resources for personal business purposes is strictly prohibited. The following criteria will be used in determining whether personal use is acceptable:

- It does not interfere with College business or educational operations.
- It does not bring the College into disrepute.
- It does not breach staff employment contracts.
- It does not breach student regulations.
- It does not interfere with proper use of College resources.
- It is not a disproportionate use of College resources.
- It does not offend another member of staff or student.
- Priority must be given to use of resources for the main purpose for which they are provided.
- Not being of a commercial or profit-making nature, or for any other form of personal financial gain.
- Not be connected with any use or application that conflicts with an employee's obligations to the College as their employer.
- Not be against the College's rules, regulations, policies and procedures and in particular this acceptable use of technological resources policy.

VI. College Monitoring

IRM specialists frequently monitor network and computer systems access and utilization. This is done for various purposes which include: assessing systems availability and performance; identifying and resolving technical problems; to detect computer viruses, spyware, file-sharing software, etc. and/or to detect prohibited activities; to enforce College administration's directives and/or orders properly issued by law enforcement and legal authorities.

In any investigation of misuse, the College may inspect, without prior notice, the contents of files, voice mail, logs, and any related computer-generated or stored material, such as document output;

Account holder's computer files may be inspected occasionally when assuring system integrity or performing related authorized resource management duties.

VII. Worldwide Web Site Access

The Worldwide Web is rich with information that can be of significant benefit when used properly by education and supporting personnel. ACG users accessing the Internet/Worldwide Web must understand:

1. The College is not responsible for material viewed or downloaded by individual users of the Internet. For example, even though the College does try to eliminate access to offensive websites, a situation may occur whereby an Internet search request inadvertently leads a user to an offensive website. This does not mean the College condones sexual harassment and offensive information. Users should exercise caution since even innocuous searches may lead to sites with offensive content.

2. The Greek law specifies that certain activities are prohibited. Among these include accessing, downloading, printing, or storing information with sexually explicit content.

3. Mindful of the guidance specified above, the College has implemented a widely used website scanning and blocking system. When users attempt to connect to websites that are on the list of blocked sites, access to the website is denied and a webpage is returned which informs the user that the site has been blocked. This webpage also provides information on how to contact a College representative if additional information or clarification is needed.

4. Users can request that access to blocked websites be permitted by submitting a request to helpdesk@acg.edu. Requests are referred and reviewed by the Executive Director for IRM or a designated representative, who then determines if the block should be removed or if additional review is required. Users are then advised of the follow-on action.

5. Special care should be taken when downloading files to protect computer systems from viruses, spyware, and other harmful software and computer code.

Contact

For questions or comments: acgirm@acg.edu

The American College of Greece
Information Resources Management Department
Web: https://www.acg.edu/current-students/it-acg/
Email: acgirm@acg.edu
Telephone: +30 210 600 9800 ext. 1356

Policy Changes

The InfoSec Operations Team is charged with the responsibility to periodically review the policy and propose changes as needed.

Date of Creation: Nov. 30, 2012
Date of Last Update: Nov. 1, 2023