

Network, Computer, and Communications Device Acceptable Use Policy [Condensed]

1. Scope

For the purposes of this policy, the term “communication and computing services” includes all IAIA information and systems using hardware, software, and network services including computer resources entrusted to IAIA by other organizations. Computing services explicitly includes the use of network services by personally owned computer systems which have been granted access to IAIA-provided network services for authorized Users.

2. Rights and Responsibilities

Under this policy, all Users are required to act ethically and legally, to protect the integrity and security of the resources, and to comply with all applicable laws, contractual obligations and regulations. Users must also abide by all the prevailing policies, rules, guidelines and standards applicable to the use IAIA Information Technology (IT) facilities and services, as announced by the IT department or as promulgated on the IAIA website from time to time.

Users are responsible for all their activities using computing services and shall respect the intended use of such services. IAIA has specific rules and regulations that govern the use of equipment and Users shall comply with the rules and regulations governing the use of such computing facilities and equipment. Users must understand and keep up-to-date with this policy and other applicable IAIA policies and procedures.

Acceptable use of resources **REQUIRES** that Users:

- use resources only for authorized purposes;
- protect their userid and systems from unauthorized use. Each User is responsible for all activities on their userid or that originate from their systems;
- access only information that is their own, that is publicly available, or to which the User has been given authorized access;
- use only legal versions of copyrighted software in compliance with vendor license requirements;

It is **NOT ACCEPTABLE** to:

- use another User’s system, files, or data without permission;
- engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses,

- disrupting services, or damaging files or making unauthorized modifications to IAIA data;
- use programs that degrade the available bandwidth, including but not limited to music/radio programs, videos, peer-to-peer sharing services, and game playing from Internet sites, unless these programs are incorporated into instruction;
 - transfer any restricted personal data and / or student record data under the purview of the Family Educational Rights and Privacy Act (FERPA) to any non-IAIA personal mobile data storage media or any non-IAIA owned computers;

4. Misuse of Computing Services

IAIA reserves the right to sanction a User if it is determined, after an investigation by the appropriate office, that the User violated federal or state law or IAIA policy by misusing IAIA computing services.

5. Monitoring and Privacy

Users, including managers, supervisors, and systems administrators shall respect the privacy of other Users. Users must be aware, however, that computing systems can never be totally secure and the IAIA cannot guarantee privacy.

Users expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network..

6. Activity and Data Retrieval

IAIA may specifically access and examine the account of an individual User if necessary to comply with federal or state law or if there is reasonable suspicion that a law or IAIA policy has been violated and examination of the account is needed to investigate the apparent violation.

7. Failure to Comply

Use of IAIA computing services in violation of applicable laws or IAIA policy may result in sanctions, which may include, but are not limited to, one or more of the following:

1. temporary or permanent withdrawal of use privilege;
2. disciplinary action according to applicable IAIA policies, up to and including, expulsion from IAIA or discharge from a position; and/or
3. legal prosecution under applicable federal and/or state law.