INFORMATION TECHNOLOGY SERVICES POLICIES

International House Information Technology Services
Computing Resources and Intellectual Property Acceptable Use Policy for Resident Members and Guests

This Acceptable Use Policy (this "Policy") provides standards for the use of International House ("I-House") computing resources, including any computer equipment, computing facilities, Internet access, and systems and networks made available by I-House for the use of Resident Members and guests (collectively, the "I-House Computing Resources"). Resident Members and I-House guests (the "Community Members") are expected to read and understand this Policy, and to follow this Policy in accessing or using any I-House Computing Resources.

In adopting this Policy, I-House recognizes that all Community Members are bound not only by the Policy, but also by local, state, and federal laws relating to electronic media, copyrights, privacy, and security. Each Community Member is expected to be familiar with and abide by this Policy and all other relevant policies.

1. Misconduct and Use Restrictions

A. Except as otherwise permitted in this Policy, Community Members may use I-House Computing Resources for educational use only.

B. Community Members must only use I-House Computing Resources in accordance with this Policy, and must not, under any circumstances:

1. use I-House Computing Resources in a way that violates, or promotes or encourages the violation of, any applicable federal, state, local or international law or regulation, or for any unlawful purpose or to promote illegal activities;

2. post, knowingly receive, send, upload, download or use any material or information that is unlawful, abusive, threatening, harassing, obscene, defamatory, libelous, fraudulent, infringing, or racially, sexually, religiously offensive, relates to child pornography, or is otherwise objectionable;

3. use I-House Computing Resources for mass and unsolicited communications (except official I- House activities authorized by the Office of the President) or for political campaigns;

4. use I-House Computing Resources for the commercial gain of any Community Member or any third party that is not expressly permitted under applicable I-House policies;

5. use another user's login or account for use of I-House Computing Resources without the prior written consent of I-House Information Technology Services.

6. provide false or inaccurate information when registering for a user account, or

when otherwise providing information, to access any I-House Computing Resources;

7. use a false name or email address, impersonate I-House, an I-House employee or representative, another user or any other person or entity, or otherwise mislead as to the origin of content, materials, or information.

8. add personal software or hardware to I-House workstations. Prior authorization from the IT office must be given before attempting to install any software or if the workstation prompts for an update.

2. Privacy and Information Practices

A. Users of I-House Computing Resources ("Users") must respect the rights of others to privacy and intellectual property rights and refrain from unauthorized access or copying. State and federal law and I-House policy prohibits unauthorized access to computer and telephone systems. No one may use aliases, nicknames, pointers, or other electronic means to capture information intended for others without permission of the intended recipient. Attempts to gain unauthorized access to machines or computer records, to decrypt encrypted materials, to monitor other individuals' computer or network use, to attempt to obtain their passwords, or to obtain privileges or information to which the user is not entitled are prohibited.

B. Passwords are private, personal information, which should not be written down, posted, or otherwise shared with others. Attempts to use another person's password or hack another person's password are prohibited. Any attempt to make use of another person's password or to access another person's account or information may result in immediate termination of access to I-House Computing Resources and as well as judicial or criminal prosecution as defined by the appropriate existing law or policy.

C. If an account holder allows public access to files via file sharing, it is presumed that the account holder does not intend to keep those files private from other users.

D. Information Technology systems support staff, systems operators, supervisors, and designated I- House officials may access information resources to locate and protect business information, maintain system and network resources, ensure system and network security, provide technical support, comply with legal requirements, or administer I-House policies. Information Technology personnel are not authorized to access or make use of any user's password, protected data without specific authorization from the user or direction from I-House's Legal Counsel, Internal Audit, Human Resources, or Public Safety.

E. Local area networks and local resources, including personal computers, workstations, file servers, printers, and similar devices shall be subject to the same rights to privacy and confidentiality afforded centralized computer systems regardless of whether those local resources are connected to any of I-House's central information technology networks.

3. Intellectual Property

A. No Community Member shall use another's content or property in a way that violates copyright law or infringes upon the rights held by others. The unauthorized duplication or use of any electronic material that is licensed or protected by copyright may constitute violations of civil and criminal law and is prohibited by this Policy. Community Members should assume that works communicated through the network are subject to copyright unless there is a specific disclaimer to the contrary.

B. Community Members should recognize that placing individual work in the electronic public domain may result in widespread distribution of that work and could jeopardize their rights to that work.

C. I-House retains ownership of all intellectual property rights in materials relating to I-House, including applicable copyrights, trademarks, and other proprietary rights. Community Members must not reproduce, distribute, modify, create derivative works of, publicly display, publicly perform, republish, download, store, or transmit any I-House intellectual property without permission from I-House.

4. Copyright Infringement

A. I-House strictly prohibits any form of copyright infringement including the illegal uploading and downloading of copyrighted works through peer-to-peer (P2P) file sharing or other peer to peer software. Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

B. Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504 and 505. Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information, please see the Web site of the U. S. Copyright Office at www.copyright.gov, especially the FAQ's at www.copyright.gov/help/faq.

C. In addition to the civil and criminal penalties outlined above, Community Members who engage in illegal downloading or unauthorized distribution of copyrighted materials using I-House Computing Resources will be referred to the appropriate authority and may face disciplinary action including the cancellation of their I-House membership.

5. Internet Access

A. I-House maintains computer facilities and Internet access for its primary missions of teaching, education, research, and public service. Excessive use of the Internet for other purposes places an unreasonable burden on the I-House network and interferes with access for legitimate use. Using I-House Computing Resources for occasional access to the Internet for personal purposes is not specifically prohibited. However, the Department of Information Technology Services is charged with the responsibility of ensuring recreational use does not interfere with legitimate educational and administrative access. When necessary, Information Technology staff will restrict activities as required to ensure all Users have adequate access to the Internet.

B. Violations of Internet use include, but are not limited to, accessing, downloading, uploading, saving, receiving, or sending material that includes sexually explicit content or other material using vulgar, sexist, racist, threatening, violent, or defamatory language.

C. Users should make economical and wise use of computer and network resources. Users should report suspected unauthorized use of resources to the Department of Information Technology Services. Theft,

failure to observe copyright laws, and/or tampering with any computer system or network device will place violators in jeopardy of losing privileges as well as possible criminal prosecution.

6. Monitoring and Enforcement

A. I-House reserves the right to:

1. Take any action with respect to any User conduct that I-House deems necessary or appropriate in its sole discretion, including if I-House believes that such User conduct (i) violates this Policy, including those prohibited uses described herein; (ii) infringes any intellectual property right or other right of any person or entity, or may result in criminal or civil action under applicable law or regulation; (iii) threatens the personal safety of Community Members, Users or the public; (iv) could create liability for I-House; or (v) is unlawful, offensive, abusive, harmful, malicious or otherwise constitute a misuse of I- House Computing Resources;

2. Disclose the identity of a Community Member to any third party who claims that the Community Member's use of I-House Computing Resources violates his or her rights, including their intellectual property rights or their right to privacy;

3. Take appropriate legal action, including referral to law enforcement, for any illegal or unauthorized use of I-House Computing Resources;

4. Terminate or suspend a Community Member's access to all or part of the I-House Computing Resources for any or no reason, including, without limitation, any violation of this Policy; or

5. Fully cooperate with any law enforcement authorities or court order requesting or directing disclosure of the identity of any users of I-House Computing Resources or other information of anyone posting any materials on or through I-House Computing Resources.

B. If Community Members become aware of any misuse of I-House Computing Resources, Community Members agree that they shall promptly contact Department of Information Technology Services to report such misuse.

C. In addition to the above action, I-House maintains the right to bring disciplinary action against those violating any provision of this Policy in accordance with the I-House Code of Conduct and Disciplinary Review Process. Such disciplinary action can include placement on probationary status and/or cancellation of Resident Membership.

7. Rights and Privileges

A. The names of Resident Members and staff are entered into an electronic database of names along with associated items of information. An entry in the I-House database, administered by Information Technology Services, grants access to network services that originate at I-House and requires user authentication. Resident Members have the right to request, through the Admission's Office, that their information is not made available to anyone outside the organization.

B. Having an account is a privilege, not a right or entitlement. An individual is assigned an account for use while conducting activities related to the mission of I-House.

C. The holder of an account is entirely responsible for the security and confidentiality of their account and password, and they are entirely responsible for any and all activities that occur under their account. An account holder may not share access information that would enable use of an account with any third party, including colleagues at I-House, family members, or any other individual. Community Members agree that they will immediately notify I-House of any unauthorized use of their account or any other breach of security of I-House Computing Resources of which they become aware. Any account may be revoked temporarily or permanently if a User violates public law or I-House policy.

8. Security

A. Personal computers and workstations are intended for use as "clients" that request computing services rather than "servers" that provide computing services. Providing services to other users, such as other I-House network users or the Internet at large, potentially consumes excessive amounts of network bandwidth and compromises network security. Without explicit, written authorization from the Department of Information Technology Services, computers shall not be configured to operate as servers, including but not limited to: file, print, mail, web, chat, media streaming, name, time, directory, quote, network management, or proxy servers. Any computer ostensibly configured as a client but running special software that provides services to other users is regarded as being a server and deemed to be in violation of this policy. I-House Information Technology support personnel may restrict, limit, or disable specific application traffic to ensure that other mission-critical network traffic is not affected or disrupted in any way.

B. No User shall attempt to access any service or resource if he or she has not been explicitly authorized access by the appropriate I-House authority. All network access ports are provided for use with a single computer system. No router, wireless access point, hub, or other network device may be installed in any I-House facility without prior review and written approval from the Department of Information Technology Services. Users of the I-House network shall not perform any activity which disrupts network or server resources, impedes or prevents network or server access by others, or attempt to access private data of others. Examples include, but are not limited to, port scanning software, packet sniffers, mail bombing, ping flooding, SMURF attacks, and/or SYN flooding. Users found to be in violation of this policy will be denied access without prior notice.

C. Additionally, Community Members agree that they will not under any circumstances:

1. Make any automated use of I-House Computing Resources, or take any other action that I-House deems imposes or potentially imposes an unreasonable or disproportionately large load on I-House Computing Resources, or I-House's servers or network infrastructure;

2. Use I-House Computing Resources in any manner that could disable, overburden, damage or impair I-House Computing Resources or interfere with any other person's use of I-House Computing Resources;

3. Use any software, technology, robot, spider or other automatic device, process or means to access I-House Computing Resources for any purpose, including monitoring, harvesting, copying or manipulating any material, information or data available on I-House Computing Resources;

4. Use any manual process to monitor or copy any of the I-House Computing Resources or any material, information or data available on I-House Computing Resources;

5. Attempt to gain unauthorized access to, interfere with, damage, or disrupt any aspect of the I-House Computing Resources, the servers from which I-House Computing Resources are operated, or any server, computer, or database connected to I-House Computing Resources; or

6. Otherwise interfere or attempt to interfere with the proper functioning of I-House Computing Resources.

D. To ensure the security of I-House Computing Resources, Information Technology Services has implemented security devices which will ensure that the I-House network is adequately protected from malicious traffic to/from Resident Member and staff systems. These devices will block traffic identified as viruses, worms, and exploits.

9. Wireless Network Access & Usage

A. The primary mission of the wireless networks is to provide general network access for Community Members. I-House must maintain administrative control of the radio frequency spectrum that wireless devices use as their base transport mechanism. Other devices exist that also use the same frequency band and can cause interference on the wireless network. These devices include, but are not limited to, other wireless networking devices, cordless telephones, cameras, keyboards, mice, audio speakers, ad-hoc (peer-to-peer) networks and computers or other devices equipped with a wireless card and software to act as an access point. Information Technology Services staff will work with Community Members to determine if use of such devices can be accommodated without causing interference to the wireless networks.

B. Wireless network usage is bound by the same policies governing the use of I-House's wired network. Priority for use of I-House's wireless networks is managed in the following order: (i) current Resident Members; (ii) current employees; and (iii) visiting guests. To ensure adequate security, all systems and devices intended for use on the institution's wireless networks must complete an authentication process. Wireless devices which do not authenticate will not be allowed access. Current Resident Members and employees will connect to the I-House wireless network authenticating with their network account. Visiting guests will connect to the I-House-Guest wireless network authenticating by entering the password and agreeing to the terms and conditions and acceptable use policy.

10. Termination, Suspension, and Limitations of Access

A. Community Members agree that I-House may, with or without prior written notice, terminate, suspend, or otherwise limit a Community Member's access to I-House Computing Resources for cause. Cause for such termination, suspension, or other limitation of access shall include but not be limited to:

1. (i) conduct that is in violation of this Policy or other incorporated agreements, rules or guidelines;
2. (ii) failure to pay any amount owed I-House;
3. (iii) any request by law enforcement or other government agency;
4. (iv) unexpected technical or security issues or problems; and
5. (v) engagement in fraudulent or illegal activities.

B. Community Members agree that all such terminations, suspensions, or other limitations of access for cause shall be made in I-House's sole discretion, and I-House shall not be liable to any Community Member or any third party for any such termination, suspension, or other limitation of the Community Member's or any third party's access to I-House Computing Resources. I-House is not responsible for any loss or damage arising out of a Community

Member's failure to comply with this Policy.

11. Enforcement of this Policy

A. Any Community Member determined to have violated this Policy may be subject to disciplinary action, to be determined based on the violation, up to and including termination of the individual's association with I-House (i.e. cancellation of membership status, termination of employment).

12. Modifications to the Policy

A. This Policy will remain in effect unless it is revoked or modified in writing by Information Technology Services.

Contact

All questions, comments, concerns, requests for technical assistance, and other communications may be directed to the Department of Information Technology Services, by email at it@ihousenyc.org or by phone at extension 7888.