Acceptable Use Agreement

Version 2.1 September 2018

1. CONTEXT

King's University College Information Technology Services Acceptable Use Agreement (AUA) promotes the efficient, ethical, and lawful use of IT resources. Protecting and preserving College IT resources is a cooperative effort that requires each member of the College community to act responsibly and guard against abuses.

As part of its educational mission, the College acquires, develops, and maintains various IT assets. These assets are intended for College-related purposes, including, but not limited to, direct and indirect support of academic and administrative functions, student and campus life activities, and communication within and beyond the College community.

The College collects, stores, and transmits electronic information of a sensitive nature to facilitate and enable its academic, research and other College-related functions. The exposure of sensitive information to unauthorized individuals could cause irreparable harm to the College or members of the College community, and could also subject the College to fines or other government sanctions. Additionally, if College information were tampered with or made unavailable, it could impair the College's ability to conduct its operations.

The College recognizes the importance of information security and the protection of its IT assets. The College is therefore committed to preserving the confidentiality and integrity of its IT assets and use reasonable, appropriate, practical and effective security measures to protect against unauthorized use, modification, disclosure, and destruction of said assets.

2. APPLICATION

This agreement and related procedures covers all IT assets and applies to:

a) All King's University College employees, students, contractors, visitors, volunteers, and members of its Board of Directors.

b) External organizations and their respective employees, contractors, and representatives who use or are granted access to College IT assets or network resources.

c) The use of shared services with the constituent university. As a condition of access to King's University College IT resources, users must also abide by the Code of Behaviour for Use of Computing Resources and Corporate Data at the University of Western Ontario. This code is available at https://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp113.pdf

For the purposes of this agreement:

a) "**employee**" includes all (regular and contract positions) unionized and non-unionized academic, administrative and support personnel (including those whose salary is paid through sources other than College operating funds, such as grants, research grants and external contracts);

b) **"student"** means an individual registered at the College or Western University at the undergraduate, graduate or postdoctoral level, whether enrolled full-time or part-time;

c) **"guest"** means anyone external to the College who is using IT resources while participating in an event, maintenance work or through consultation or services;

d) "**IT asset"** or "**IT assets**" is meant to encompass all and collectively refer to College IT resources and the electronic information stored on, within or passing through a College IT resource;

e) "**IT resource**" or "**IT resources**" includes (and is not limited to) the following that are owned by and/or operated or managed by the College, or that are licensed to the College or operated by an external organization on behalf of the College: software, systems, networks, computers, or any other computing resource or hardware, servers (physical or virtual), data storage or network devices, email servers, print and fax servers, telephone systems, magnetic media or network and any othe**r** communication devices;

f) "**College Community"** is meant to encompass all College employees, individuals holding College academic appointments whether permanent or visiting, students, board members, contractors, visitors, and volunteers.

3. ACCEPTABLE USE

a) The College does not permit the use of IT assets that:

1. Interfere with or are a nuisance or menace to the College, its employees, students or others, or to its operations;

2. Are contrary to, or inconsistent or incompatible with, or do not respect the mission, image and reputation of the College;

3. Pose a significant/material/unacceptable health, safety or security risk; or,

4. Are contrary to applicable laws.

b) All software purchased by the College or developed by employees or contractors for the College is the College's property and protected by applicable copyright laws from unauthorized use and duplication, unless otherwise agreed to in writing;

c) Every user must understand the sensitivity of their information and treat it accordingly. Even if technical security mechanisms fail or are absent, every user must still attempt to maintain the security of information commensurate to its sensitivity;

d) The College does not routinely monitor, inspect, copy or disclose the electronic information stored on, within or passing through a College IT asset unless such action is, to the extent that it is strictly necessary, to ensure the proper functioning of the operations of the College or a College IT asset, to prevent or correct improper use of an IT asset, to ensure compliance with this agreement or an information security procedure, or unless such action is permitted or required by applicable laws;

e) The College will maintain reasonable processes to deal with viruses, to reject emails from unwanted SPAM sources and to scan incoming and outgoing network traffic to detect and protect against malicious content; the College cannot guarantee the success of such processes, and the user must accept the risk inherent in the use of the technology;

f) The College will take appropriate preventative and corrective action where violation (or threat of violation) of this agreement and will, where warranted, hold individuals responsible in accordance with applicable collective agreement provisions, terms of employment or other College policies, regulations or applicable laws.

g) Responsibilities of IT resource users:

1. Use resources only for authorized purposes.

2. Protect your user identity, password and system from unauthorized use. All users are responsible for all activities on their user accounts or that originate from their devices.

3. Access only information that you own, that is publicly available, or to which you have been given authorized access.

4. Use only legal versions of copyrighted software in compliance with vendor license requirements.

5. Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

h) Unacceptable uses of IT resources include but are not limited to the following:

1. Using the resources for any purpose which violates local, provincial or federal laws.

2. Using the College's systems or networks in a manner not authorized by the College.

3. Unauthorized copying of information stored on the College's IT assets.

4. Using excessive computing resources, data storage or network bandwidth in activities such as the propagating or broadcasting of inappropriate messages to lists or individuals or generally transferring unusually large or numerous files or messages or printing excessive amounts of paper.

5. Sending or storing for retrieval patently harassing, objectionable or extremely offensive, intimidating, or abusive material. Such material includes but is not limited to racist material, hate literature, sexist slurs or sexually explicit material. The College Harassment and Discrimination Policy can be found at : https://www.kings.uwo.ca/kings/assets/File/policies/Harassment_and_Discrimination_Policy.pdf

6. Misrepresenting your identity or affiliation while using IT resources.

7. Using someone else's identity and password for access to IT resources, logging others into the network to access IT resources, or using the network to make unauthorized entry to other computational, information, or communications devices.

8. Attempting to evade or crack passwords of systems on the network.

9. Attempting to circumvent or subvert system or network security measures.

10. Reproducing, downloading and/or distributing material protected by trademark, trade secret, or other intellectual property without appropriate authorization.

11. Making or using illegal copies of copyrighted materials, software or movies, storing such copies on College systems, or transmitting them over College networks.

12. Copying or modifying files belonging to others or to the College without authorization, including altering data, introducing or propagating viruses, Trojans or worms, or simply damaging files.

13. Purposefully interfering with or disrupting another user's work or the proper functioning of IT resources.

14. Intercepting or altering network packets.

15. Engaging in any other activity that interferes with the work of other students, faculty, or staff or the normal operation of the College IT resources.

4. MAINTENANCE

The Director of Information Technology Services is responsible for the interpretation of this agreement. The agreement will be reviewed on a regular basis or as deemed appropriate based on changes in technology or regulatory requirements.

For more information or questions about this document, contact King’s Information Technology Services at its@kings.uwo.ca.