Staff
Information System
Acceptable Use Policy

Hing Shung Chan
Vice President of Information Technology
Information Security Officer

Revision 2
02/17/2017
Youth Consultation Service

Table of Contents

I. Definitions

Users – Everyone who has access to any of YCS IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, customers and business partners.

Systems - All IT equipment that connects to the agency's network or access the agency applications. This includes, but is not limited to, desktop, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

Network – A group of interconnected computers and peripherals that is capable of sharing data, software and hardware resources between many users. Connections occur by cable and/or wireless.

System Administrator – Is the technical custodian of a System. System Administrators are responsible for the technical operation, maintenance and monitoring of the System.

II. Rights and Responsibilities

YCS systems and networks can provide access to resources on and off site, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, policies, regulations, and contractual obligations whether stated or implied.

The Information Systems Acceptable Use Policy does not attempt to articulate all required or proscribed behavior by users. Successful operation of the YCS information system requires all users to conduct themselves in a responsible, decent, ethical, and polite manner. The user is ultimately responsible for his or her actions in accessing and using the YCS information system. As a user of the YCS information system, you are expected to review and understand the guidelines and procedures in this Policy.

YCS system administrators reserve the right to monitor and review electronic information to protect the integrity of YCS information system. For example, system administrators may monitor, test and review files or accounts in order to, but not limited to: 1) analyze the use of the systems for compliance with policies; 2) conduct audits; 3) review performance or conduct; or 4) obtain information. YCS reserves the right to disclose any electronic message to law enforcement officials. And, under some circumstances, YCS may be required to disclose information to law

enforcement officials, the public or other third parties, for example, in response to a document production request made in a lawsuit involving YCS.

III. Background

The information system throughout YCS is moving into the Information Age by providing Email and Internet access for its employees. Providing employees with the ability to communicate with people from throughout the world and access to a vast amount of information necessarily raises concerns that employees will knowingly misuse such privileges. The purpose of the YCS information system is to enhance the way we develop, access, and communicate information during the course of business. Consequently, YCS must exert control over the use of its information system.

III. Role of YCS

A. YCS Responsibilities

Each department manager must work in conjunction with the Information Technology department (IT) in order to coordinate the information system needs as it pertains to each department. Each departmental manager will ensure that all of the employees at that location receive instruction in the Policy, maintain, and make available to Human Resources properly executed Staff Information System Acceptable Use Agreements, and be responsible for interpreting and implementing the Policy.

The IT Department will administer the system and be responsible for maintaining and monitoring all systems. Acting in the role of system administrator, the IT Department has established a process for setting up individual and email accounts (as needed), setting quotas for disk usage, establishing a retention schedule, and developing a virus protection process.

YCS will: 1) establish reasonable boundaries of acceptable use of its information system; 2) educate users about acceptable use, and 3) enforce policies for acceptable use.

B. Technical Services Provided Through YCS

The ability to use YCS information system provides email, Internet access, access to various applications, access to user's files, file sharing, and network printing. Each departmental manager must consider what particular services are needed in order to conduct work-related duties, the resource demands for such services, and the rationale for requesting such service(s).

IV. Staff Acceptable Use Guidelines

This document contains the Information Systems Acceptable Use Policy for a staff member's use of YCS information systems.

A. Business Purpose

1. YCS information systems have been established for a limited business purpose. The term "business purpose" includes all activities deemed necessary in the conduct of day-to-day operations (e.g., communicating via email regarding work-related matters, accessing business applications, etc.).
2. The YCS information system has not been established as a public access service or a public forum. YCS has the right to place reasonable restrictions on materials accessed or posted through the system. Users are required to follow the rules set forth in this policy regarding the appropriate use of information systems.
3. Users may not use YCS information systems for commercial purposes. Therefore, users may not use YCS information systems for personal or private gain, personal business, or commercial advantage (e.g., making purchases, etc.).
4. Users may not use YCS information systems for political lobbying, which includes assisting of advocating, directly or indirectly, for or against a ballot proposition and/or the election of any person to any office.

B. Email and Internet Access

1. Users, if approved by departmental management, will have access to Email and the Internet along with other YCS information systems.
2. All users must sign the attached “Staff Information System Use Agreement” to be granted access to these and other YCS information systems.

C. HIPAA, PII, PHI and ePHI

YCS is a Health Insurance Portability & Accountability Act of 1996 (HIPAA) compliant agency. This includes personally identifiable information (PII), Protected Health Information (PHI) and electronic Protected Health Information (ePHI). The safeguarding of clients’ electronic records is prescribed in a separate policy called “Policy and Procedure for ECR Staffs Security Measure”

D. Unacceptable Uses

The following uses of the YCS information system are considered unacceptable:

1. Illegal Activities

a) Users will not attempt to gain unauthorized access to YCS information systems or to any other computer system through YCS or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files or email messages. These actions are illegal, even if only for the purposes of "browsing."

b) Users will not engage in any activity which, intentionally, disrupts the YCS information system or destroys data. Examples of such "disruptive uses" include unsolicited advertising ("Spam"), propagation of computer viruses, distribution of large quantities of information that may overwhelm YCS information system (e.g., chain letters, network games, or broadcasting messages), and any unauthorized access to or destruction

of YCS information system computers or other resources accessible through YCS information system ("hacking").

c) Users will not use YCS information systems to engage in any illegal act, which includes but is not limited to, arranging for a sale of illegal substances, the purchase of alcohol or firearms, engaging in criminal activity, or threatening the safety of a person.

2. System Security

a) Where applicable, users are responsible for their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should users provide their password to another person. Your system account is **your** responsibility and should be treated as such.

b) Users will immediately notify the IT department if they have identified a possible security problem. Users should not look for security problems, because this may be construed as an illegal attempt to gain access.

c) When downloading information, users will avoid the inadvertent spread of computer viruses by following site-specific virus protection procedures.

3. Inappropriate Language

a) Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language ("Inappropriate Language").

b) Restrictions against Inappropriate Language apply to public messages, private messages, and material posted throughout YCS information system.

c) Users will not post or email information that could cause damage or danger of disruption.

d) Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

e) Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by any person to stop sending email messages, the user must stop, immediately.

f) Users will not post or email false or defamatory information about any person or organization.

4. Respect for Privacy

a) Users will not repost/resend an email message that was sent to them without permission of the person who originally sent that message.

b) Users will not post or email private information about another person.

c) Users acknowledge that YCS system administrators reserve the right to monitor and review electronic (email, etc.) information to protect the integrity of YCS information system as set forth in this Policy. The YCS information system, the Internet, and use of email are not inherently secure or private. For example, the content of an email message is

analogous to a letter, not a telephone call, since a record of the contents of the email may be preserved by the sender, recipient, any parties to whom the email may be forwarded, or by the email system itself. Once an email message is sent, the sender has no control over where it may be forwarded. Users should be the caretaker's of their own privacy and not store sensitive or personal information on YCS information system computers.

5. Respecting Resource Limits

a) Email is to be used, solely, to conduct YCS and YCS-related business.
b) Staff will not use email or any other YCS information system excessively, unless such usage is deemed necessary in order to conduct business. Anyone that chooses to excessively use the YCS email or other information system for their own personal use will have their privileges removed.
c) Users will not post/email chain letters or engage in "spamming." Examples of such "disruptive uses" include unsolicited advertising ("spam"), propagation of computer viruses, distribution of large quantities of information that may overwhelm YCS' information system (e.g., chain letters, network games, or broadcasting messages), and any unauthorized access to or destruction of YCS information system computers or other resources accessible through YCS' information system ("hacking").
d) Users will not download games, programs, files, etc. onto YCS systems without prior approval from the IT department. The installation of games, programs, etc. may cause conflicts which may be of detriment to the system and cause the system to become inoperable.

6. Plagiarism and Copyright Infringement

a) Users will not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were your own.
b) Users will respect the rights of copyright owners. Copyright infringement occurs when work that is protected by copyright laws is reproduced without the author’s permission. If a work contains language that specifies appropriate use of that work, users should follow the expressed requirements.
c) Users will not install any staff owned software on YCS computer equipment. Only YCS licensed software products are to be installed on YCS computer equipment.
d) In addition, it is the practice of YCS and its users not to copy or reproduce any licensed software on the YCS information system, except as expressly permitted by the specific software license.

7. Inappropriate Access to Material

a) Users will not use YCS information systems to access material that is

profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).

b) If users mistakenly access inappropriate information, they should immediately notify the IT department. Doing so will protect user against a claim that he/she has intentionally violated this Policy.

8. Examples of Inappropriate Use

Users are not to participate in any acts of misuse. Examples of misuse include, but are not limited to, the activities in the following list:

- Using a computer account that he/she is not authorized to use.
- Obtaining a password for a computer account without the consent of the account owner.
- Using the YCS network to gain unauthorized access to any computer systems.
- Gaining access to another user's email account in order to view messages.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses and worms.
- Bringing software from home to install on one or more YCS computers.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Violating terms of applicable software licensing agreements or copyright laws.
- Deliberately wasting computing resources (e.g., downloading files, programs, etc. from the Internet).
- Using electronic mail to harass others.
- Masking the identity of an account or machine.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner or the IT Department.
- Accessing any objectionable or inappropriate material over the Internet.
- Posting or emailing defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, offensive, or illegal material.

E. User Rights

1. **Investigations**
   a) Users should expect only limited privacy in the contents of their electronic communications and personal files on YCS information systems. As set forth in this Policy, YCS system administrators reserve the right to monitor and review electronic information (email, files, etc.) to protect the integrity of the YCS information system.
   b) Routine maintenance and monitoring of YCS information systems may lead to the discovery that a user has violated this Policy.
   c) YCS reserves the right to conduct a complete system investigation if there is reasonable suspicion that a user has violated this or any other YCS policy.

2. **Due Process**
   a) YCS will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through YCS information systems.
   b) Notwithstanding YCS cooperation with any governmental investigation noted above, in the event there is a claim that a user has violated this Policy or any other YCS Policy while using YCS information system, said user will be provided with a written notice of the suspected violation and he/she will have an opportunity to present an explanation.

F. Limitation of Liability

YCS makes no guarantee that the functions or the services provided by or through the YCS information system will be error-free or without defect. YCS will not be responsible for any direct or indirect, incidental, or consequential damages, including but not limited to, loss of data or interruptions of service. YCS is not responsible for the accuracy or quality of the information obtained through or stored on the system. YCS will not be responsible for financial obligations arising through the inappropriate or unauthorized use of its information system.

G. Personal Responsibility

Access to YCS information systems is not a right but a privilege that is bestowed on YCS employees solely for business purposes. Such a privilege brings along with it responsibilities in the way in which we conduct ourselves during its use, as set forth in this Policy. YCS staff is responsible for safeguarding all business-related and client-related information that resides on our information system(s) including PII/PHI/ePHI. This information is deemed proprietary and as such, should not be shared with anyone outside YCS without the expressed consent of YCS management.

Staff Information System Acceptable Use Agreement

User Name _____

Location _____

I am responsible for my use of the YCS information system including PII/PHI/ePHI. I understand that my communications over the Internet and through email may be traceable to YCS or to me. I understand that YCS is the sole arbiter of what constitutes a violation of the YCS Staff Information System Acceptable Use Policy.

While YCS does not currently have a practice of regular monitoring or reviewing electronic information, YCS reserves the right to do so for any reason, including, but not limited to: 1) analyzing the use of the systems for compliance with policies; 2) conducting audits; 3) reviewing performance or conduct; or 4) obtaining information. I understand YCS has the right to review any material stored on or transmitted through YCS information system computers, including email, Internet files and software. YCS may edit or remove any material which it, in its sole discretion, believes may be unlawful, indecent, obscene, abusive, or otherwise inappropriate.

Examples of Inappropriate Use
Users are not to participate in any acts of misuse. Examples of misuse include, but are not limited to, the activities in the following list:

- Using a computer account and password that he/she is not authorized to use.
- Using the YCS network to gain unauthorized access to any computer systems ("hacking").
- Gaining access to another user's email account in order to view messages.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses and worms.
- Bringing software from home to install on one or more YCS computers.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Violating terms of applicable software licensing agreements or copyright laws.
- Deliberately wasting computing resources (e.g., downloading files, programs, etc. from the Internet).
- Using electronic mail to harass others.
- Masking (hiding) the identity of an account or machine.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner or the IT Department.
- Accessing any objectionable or inappropriate material over the Internet.
- Posting or emailing defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, offensive, or illegal material.

I have read the YCS Staff Information System Acceptable Use Policy. I agree to follow the rules contained in this Policy. I understand that if I violate the rules my Email, Internet and other information system privileges can be terminated and I may face other disciplinary measures.

Signature _____ Date _____