Community Advocacy and Awareness Trust (CRAWN Trust)
INFORMATION, COMMUNICATION AND TECHNOLOGY POLICY
APRIL 2024

Table of Contents

1. PURPOSE

This policy will provide guidelines to ensure that all users of information and communication technology (ICT) at Community Advocacy and Awareness (CRAWN) Trust's services or on behalf of the organisation:

- understand and follow procedures to ensure the safe and appropriate use of ICT at the service, including maintaining secure storage of information
- take responsibility to protect and maintain privacy in accordance with the service's Confidentiality and Privacy Policy
- are aware that only those persons authorised by CRAWN Trust are permitted to access ICT services within the organisation
- understand what constitutes illegal and inappropriate use of ICT facilities and avoid such activities.

2. POLICY STATEMENT

i. VALUES

CRAWN Trust is committed to:

- professional, ethical and responsible use of ICT at all CRAWN Trust workplaces
- providing a safe workplace for staff, interns, volunteers, board members, consultants and others formally engaged with CRAWN Trust using the service's ICT facilities
- safeguarding the privacy and confidentiality of information received, transmitted or stored electronically
- ensuring that the use of CRAWN Trust ICT facilities complies with all CRAWN Trust policies and relevant government legislation
- providing staff, interns, volunteers, board members, consultants and others formally engaged with CRAWN Trust with online information, resources and communication tools to support the effective operation of the service.

ii. SCOPE

This policy applies to all CRAWN Trust staff, interns, volunteers, board members, consultants and others who enter a formal agreement with the organisation.

This policy applies to all aspects of the use of ICT including:

- internet usage
- electronic mail (email)
- electronic bulletins/notice boards
- electronic discussion/news groups
- weblogs (blogs)
- social networking
- file transfer
- file storage (including the use of end point data storage devices – refer to Definitions)
- file sharing
- video conferencing i.e. Zoom, Webex, Skype, Teams, etc.
- streaming media
- instant messaging
- online discussion groups and chat facilities
- subscriptions to list servers, mailing lists or other like services
- copying, saving or distributing files
- viewing material electronically
- printing material
- portable communication devices including mobile and cordless phones.

3. BACKGROUND AND LEGISLATION

i. Background

The ICT environment is continually changing. While ICT is a cost-effective, timely and efficient tool for research, communication and management of a service, there are also legal responsibilities in relation to information privacy, security and the protection of staff, interns, volunteers, board members, consultants and others formally engaged with CRAWN Trust.

County and national laws, including those governing information privacy, copyright, occupational health and safety, anti-discrimination and sexual harassment, apply to the well-being of individuals in the workplace. Illegal and inappropriate use of ICT resources includes pornography, fraud, defamation, breach of copyright, unlawful discrimination

or vilification, harassment (including sexual harassment, stalking and privacy violations) and illegal activity, including illegal peer-to-peer file sharing.

ii. Legislation

Legislation and standards Relevant legislation and standards which protect an individual from harm include but are not limited to:

- Information, Communication and Technology Policy, 2019
- Privacy and Data Protection Policy, 2018
- The Constitution of Kenya, 2010
- The Copyright Act, 2001
- The Occupational Health and Safety Act, 2007
- The Kenyan Employment Act 2007
- Sexual Offences Act

4. DEFINITIONS

The terms defined in this section relate specifically to this policy. For commonly used terms e.g. Approved Provider- , Nominated Supervisor, Regulatory Authority etc. refer to the General Definitions section of this manual.

Anti-spyware:

Software designed to remove spyware: a type of malware (refer to Definitions), that collects information about users without their knowledge.

Chain email:

An email instructing recipient to send out multiple copies of the same email so that circulation increases exponentially.

Computer virus:

Malicious software programs, a form of malware (refer to Definitions), that can spread from one computer to another through the sharing of infected files, and that may harm a computer system's data or performance.

Cyber safety:

The safe and responsible use of technology including use of the internet, electronic media and social media in order to ensure information security and personal safety.

There are three main areas of risk to safety:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interactions with other users (including bullying) Conduct: personal online behaviour that increases the likelihood of, or causes, harm

Defamation:

To injure or harm another person's reputation without good reason or justification. Defamation is often in the form of slander or libel.

Disclaimer:

Statement(s) that seeks to exclude or limit liability and is usually related to issues such as copyright, accuracy and privacy.

Electronic communications:

Email, instant messaging, communication through social media and any other material or communication sent electronically.

Encryption:

The process of systematically encoding data before transmission so that an unauthorised party cannot decipher it. There are different levels of encryption available.

Endpoint data storage devices:

Devices capable of storing information/data. New devices are continually being developed, and current devices include:

- laptops
- USB sticks, external or removable hard drives, thumb drives, pen drives and flash drives
- iPods or other similar devices
- cameras with USB drive connection
- iPhones/smartphones
- PCI/PC Card/PCMCIA storage cards
- PDAs (Personal Digital Assistants)
- other data-storage devices (CD-ROM and DVD)

Firewall:

The primary method of keeping a computer/network secure. A firewall controls (by permitting or restricting) traffic into and out of a computer/network and, as a result, can protect these from damage by unauthorised users.

Flash drive:

A small data-storage device that uses flash memory, and has a built-in USB connection. Flash drives have many names, including jump drives, thumb drives, pen drives and USB keychain drives.

Integrity:

(In relation to this policy) refers to the accuracy of data. Loss of data integrity may be either gross or evident (e.g. a computer disk failing) or subtle (e.g. the alteration of information in an electronic file).

Malware:

Short for 'malicious software'. Malware is intended to damage or disable computers or computer systems.

PDAs (Personal Digital Assistants):

A handheld computer for managing contacts, appointments and tasks. PDAs typically include a name and address database, calendar, to-do list and note taker. Wireless PDAs may also offer email and web browsing, and data can be synchronised between a PDA and a desktop computer via a USB or wireless connection.

Portable storage device (PSD) or removable storage device (RSD):

Small, lightweight, portable easy-to-use device that is capable of storing and transferring large volumes of data. These devices are either exclusively used for data storage (for example, USB keys) or are capable of multiple other functions (such as iPods and PDAs).

Spam:

Unsolicited and unwanted emails or other electronic communication.

Security:

(In relation to this policy) refers to the protection of data against unauthorised access, ensuring confidentiality of information, integrity of data and the appropriate use of computer systems and other resources.

USB interface:

Universal Serial Bus (USB) is a widely used interface for attaching devices to a host computer. PCs and laptops have multiple USB ports that enable many devices to be connected without rebooting the computer or turning off the USB device.

USB key:

Also known as sticks, drives, memory keys and flash drives, a USB key is a device that plugs into the computer's USB port and is small enough to hook onto a key ring. A USB key allows data to be easily downloaded and transported/transferred.

Virus:

A program or programming code that multiplies by being copied to another program, computer or document. Viruses can be sent in attachments to an email or file, or be present on a disk or CD. While some viruses are benign or playful in intent, others can be quite harmful: erasing data or requiring the reformatting of hard drives.

5. PROCEDURES

The Approved Provider- CRAWN Trust is responsible for:

- ensuring that the use of the service's ICT complies with all county and national (refer to Legislation and standards), and all service policies (including Confidentiality and Privacy Policy and Code of Conduct Policy)

- providing suitable ICT facilities to enable staff and those formally associated with CRAWN Trust to effectively manage and operate the service providing clear procedures and protocols that outline the parameters for use of the service's ICT facilities

- embedding a culture of awareness and understanding of security issues at the organisation

- ensuring that effective financial procedures and security measures are implemented where transactions are made using the service's ICT facilities, e.g. handling fee and invoice payments, and using online banking, MPesa?

- ensuring that the service's computer software and hardware are purchased through the CRAWN Trust purchase order system from an appropriate and reputable supplier

- identifying the need for additional password-protected email accounts for staff, interns, volunteers, board members, consultants and others formally engaged with CRAWN Trust and providing these as appropriate

- identifying the training needs of and staff in relation to ICT, and providing recommendations for the inclusion of training in ICT in professional development activities

- ensuring that procedures are in place for the regular backup of critical data and information at the service

- ensuring secure storage of all information at the service, including backup files

- adhering to the requirements of the Confidentiality and Privacy Policy in relation to accessing information on the service's computer/s, including emails

- considering encryption (refer to Definitions) of data for extra security

- ensuring that reputable anti-virus and firewall software (refer to Definitions) are installed on service computers, and that software is kept up to date

- developing procedures to minimise unauthorised access, use and disclosure of information and data, which may include limiting access and passwords, and encryption (refer to Definitions)

- ensuring that the service's liability in the event of security breaches, or unauthorised access, use and disclosure of information and data is limited by developing and publishing appropriate disclaimers (refer to Definitions)

- developing procedures to ensure data and information (e.g. passwords) are kept secure, and only disclosed to individuals where necessary

- developing procedures to ensure that all staff, volunteers and students are aware of the requirements of this policy

- ensuring the appropriate use of endpoint data storage devices (refer to Definitions) by all ICT users at the service

- ensuring that all material stored on endpoint data storage devices is also stored on a backup drive, and that both device and drive are kept in a secure location

- ensuring compliance with this policy by all users of the service's ICT facilities

- All CRAWN Trust staff, those formally associated with the organisation, and other authorised users of the service's ICT facilities are responsible for:

    - complying with all relevant legislation and service policies, protocols and procedures

    - completing the authorised user agreement form

    - authorising the access of staff, interns, volunteers, board members, consultants and others formally engaged with CRAWN Trust to the service's ICT facilities, as appropriate by regularly up-dating password access.

    - keeping allocated passwords secure, including not sharing passwords and logging off after using a computer

    - maintaining the security of ICT facilities belonging to CRAWN Trust

    - accessing accounts, data or files on the service's computers only where authorisation has been provided

    - co-operating with other users of the service's ICT to ensure fair and equitable access to resources

    - obtaining approval from the approved provider (i.e. Airtel or Safaricom, or other) for CRAWN Trust through the purchase order system, before purchasing licensed computer software and hardware

    - ensuring confidential information is transmitted with password protection or encryption, as required

    - ensuring no illegal material is transmitted at any time via any ICT medium

    - using the service's email, messaging and social media facilities for service-related and lawful activities only

- using endpoint data storage devices (refer to Definitions) supplied by the service for service-related business only, and ensuring that this information is protected from unauthorised access and use

- ensuring that all material stored on an endpoint data storage device is also stored on a backup drive, and that both device and drive are kept in a secure location

- notifying the approved provider of any damage, faults or loss of endpoint data storage devices

- restricting the use of personal mobile phones to rostered breaks

- ensuring electronic files containing information about children and families are kept secure at all times (refer to Confidentiality and Privacy Policy).