Acceptable User Policy

GOVERNMENT OF THE COOK ISLANDS

Effective: June 2016

Policy Statement

This policy outlines the acceptable use of Information and Communications Technology (ICT) Resources owned by Government.

Government ICT resources and the services accessible on them are provided to users and contractors of government to enhance their capacity to perform their job to the best of their ability. Therefore government has ownership over information created, stored and disseminated using these resources.

Scope

This policy applies to all Public Sector Agencies and should be read in conjunction with relevant legislation and associated documents listed below.

Government ICT resources include:

- Computers and desktop devices
- Portable devices
  - Laptops
  - Tablets
  - External hard drives and USBs
  - Mobile phones and/or SIM cards
- Internet and broadband
- Centralised and agency network systems (hardware and software)
- Other ICT media and devices such as radio, cameras, television, microfilm, DVDs etc….

Principles

Employees must be good stewards of public-funded resources and comply with the Public Service Code of Conduct and values identified below:

Honesty	acting honestly, being truthful, and abiding by the laws of the Cook Islands
Impartiality	providing impartial advice, acting without fear or favour, and making decisions on their merits
Service	serving the people well through faithful service to the Government of the Cook Islands
Respect	treating the people, the Government of the Cook Islands and colleagues with courtesy and respect
Transparency	taking actions and making decisions in an open and transparent manner
Accountability	being able to explain the reason for actions taken and taking responsibility for those actions
Efficiency and Effectiveness	achieving good results for the Cook Islands in an economical way

The duty to act as a good employer requires employers develop and implement personnel policies which ensure the fair and proper treatment of employees during employment.

Legislation and Regulations

Public Service Act 2009, Official Information Act 2008, Spam Act 2008, Copyright Act 2013, Crimes Act 1969 and other relevant legislation.

Definitions

Acceptable Use means conduct expected from a user of Government ICT resources within conditions of use established through this policy

Agency means any public service department, instrument, or agent of the Government and includes a body corporate or organisation that is wholly owned or controlled by the Crown

Employee means any person who is an employee of the Public Sector

Employer means the Public Service Commissioner and Heads of Public Sector agencies or their delegated authority

Information and Communications Technology (ICT) includes any communication devices or applications encompassing computers, laptops, tablets, external hard drives and USBs, mobile phones and SIMs, internet, and network hardware and software

ICT Support is placed within the Office of the Prime Minister and provides general user and ICT systems support across the Public Sector

Instant Messaging is a type of online chat which offers real-time text transmission over the Internet

Internet is a global computer network providing a variety of information and communication facilities, consisting of interconnected networks

Malware is software which is specifically designed to disrupt or damage a computer system

Official Information is any information and records (data, media) created, stored, disseminated or retrieved on Government ICT Resources

Network includes hardware (computer equipment and devices) and software required to set up, manage, and protect a network of computer hardware and information (e.g. firewalls)

Public Sector includes Public Service Departments, Crown Agencies, Island Governments, State Owned Enterprises and Ministerial Support Offices

Public Service Commissioner means the Public Service Commissioner appointed under Article 73 of the Constitution and Section 5 of the Public Service Act 2009

SIM means Subscriber Identification Module which is a removable card inside a cell phone used to store data that is unique to the phone user

Spam means irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.

Trojan Horse program means a program designed to breach the security of a computer system while ostensibly performing some innocuous function.

Virus means a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

Worm means a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program

USB means Universal Serial Bus, commonly known as flash drives is used for data storage

User is any employee, employer, contractor or individual using Government ICT Resources

Procedures

Employers are responsible for administering and promoting adherence with this policy. Employers should also ensure users have access to the policy.

Employer Obligations

Employers must:

- Establish procedures for implementation with thresholds for acceptable use
- Establish procedures for work-related transactions or payments made over the internet
- Manage acceptable use thresholds and mitigate risks for inappropriate or prohibited use
- Monitor the use of ICT resources to enhance productivity and reduce wastage
- Raise user awareness of their responsibilities and consequences for breaches of the policy
- Initiate investigations and timely action for breaches of the policy
- Authorise the establishment or suspension of user access to Government ICT Resources
- Approve deviations to the policy e.g. access to a prohibited site for investigation purposes

User Obligations

Users are expected to conduct themselves honestly and appropriately when using Government ICT resources, while respecting copyright, software licensing rules, intellectual property rights, and privacy legislation.

Users must:

- Read and adhere to the policy
- Use ICT resources responsibly to perform their job effectively
- Appreciate that access to ICT resources is a privilege that should not be abused
- Keep the personal use of ICT resources to a minimum
- Avoid improper or prohibited use of ICT resources

Role of ICT Support

ICT Support provides user and systems support across the Public Sector and monitors use of the centralised ICT network by:

- Briefing agencies on acceptable use of the centralised network
- Maintaining logs, backups and archives of computing activities including workstations, laptops, servers, printers, and network connected devices
- Maintaining network upgrades, software installations and software licensing renewals
- Monitoring network and email server performance
- Retaining logs, backups and archives of all internet, network and email usage
- Reporting inappropriate or prohibited use of resources to employers with recommendations
- Reporting serious prohibited use to other authorities as required e.g. Police
  Providing information to support investigations into inappropriate or prohibited use
  Providing access to user logs in the event that there is a perceived threat to the:
  - ICT network systems
  - Safety and privacy of employees and users
  - Reputational risk of government
  - Legal liability of government

These records may be retrieved and cited as evidence in investigations or legal proceedings.

Conditions of Use

Government reserves the right to:

- Monitor user activity and take appropriate action if misuse of resources is identified
- Inspect the use of ICT resources, together with files, user email accounts and messages, logs contained on devices
- Examine files and directories where it is necessary to determine the ownership or recipients of lost or misdirected files where: the network security is threated or compromised, an activity has detrimental impact on the quality of service to other users, or there is inappropriate or prohibited use of the ICT resources.

Employers must authorise user access to Government ICT resources subject to acceptable use. Acceptable use is where ICT resources are used only for the purposes for which they are authorised and according to conditions of use outlined in this policy. Employers are responsible for establishing and managing procedures to ensure adherence with this policy. Queries regarding access or acceptable use of ICT resources should be directed to employers, the agency ICT Manager or ICT Support.

Acceptable Use

Users must adhere to acceptable use of Government ICT resources to prevent or mitigate risks from inappropriate, prohibited or unauthorised use of these resources.

Confidentiality

Users must:

- Apply confidentiality, privacy and classification standards and practices to the access, storage, retrieval, and dissemination of official information

- Be aware that unauthorised disclosure of classified or sensitive information is a breach of legislation such as the Official Information Act and Government Code of Conduct Policy
- Take extreme care with the use of email in these circumstances to avoid unauthorised publication of classified and sensitive official information
- Understand all information created, stored or disseminated on Government ICT resources is official information and may be monitored or retrieved for investigations, or requested by law

Security

Users must:

- Take appropriate measures to protect and prevent unauthorised use of ICT resources
- Use passwords or personal identity numbers on devices (laptops, desktops and mobiles)
- Ensure passwords are complex enough to increase protection
- Lock computers when not in use to avoid use by others (Press windows key + L)
- Log off a shared computer to allow use by others
- Not share passwords or authorised access to ICT resources with other users
- Not store official information on a private emails or devices (laptops, desktops, hard drives)
- Avoid using the same username and password for the ICT network, to access internet sites

Email and Instant Messaging Use

Users must:

- Ensure all emails do not contain any offensive material, harass or threaten others
- Ensure emails are only sent to intended recipients – less use of 'reply all'
- Immediately return emails received in error and delete the message and attachments
- Not reply to or open any attachments accompanying spam messages (ie unsolicited commercial email)
- Not use work email to receive notifications from personal subscriptions or websites for example Facebook, Twitter, etc
- Not use work email to send personal promotions and advertisements unless endorsed by the Employer

Internet Use

Users must not:

- Access online media streaming sites (e.g. radio, music and video broadcasts) unless they are work-related
- Create and post to personal blogs
- Create personal web pages
- Conduct a private online business (using TradeMe, eBay or Facebook etc...)

Excessive web browsing that is not work related is inappropriate. The term "excessive" is to be negotiated between employers and employees.

Employees may perform personal online banking and contribute to work-related online discussion groups, as long as it does not impact their work, and wherever possible is conducted outside working hours.

Network and Hardware Use

Network hardware (network drives and computer local drives) and software and other hardware devices such as portable external hard drives, USBs, printers, modems, mobiles, SIM cards owned by government or used on government assets form part of Government ICT resources.

Users must:

- Use centralised and agency networks appropriately to disseminate work-related information
- Not save software and/or large personal files to government network drives. These drives are regularly monitored, particularly when disk space is at a premium. Personal files such as: graphics, music, video files and '.exe' files will be targeted and removed
- Take reasonable steps to ensure portable devices such as external hard drives or USBs are free from viruses

Software Use

All Government computers have anti-virus software installed that automatically checks all downloaded files. Employers must approve any software installation or uploading.

Users must:

- Only download software from known or trusted sources
- Not distribute games, entertainment and pirated software, to deliberately propagate any virus, worm, Trojan horse, trap-door programme code and/or any other virus
- Not upload any software or data, owned and/or licensed to the Government

Personal Use

Personal use of Government ICT resources must be authorised by employers with thresholds for acceptable use.

Users must:

- Ensure personal use of ICT resources is minimised
- Ensure that personal use does not interfere with their job performance
- Be aware any personal information created, disseminated or retrieved using Government ICT resources may be monitored, and is stored or retrieved as official information
- Be aware they forgo a certain level of privacy when they choose to use government ICT resources to produce or share personal information or communication

Intellectual Property Use

When using Government ICT Resources, users be aware of international copyright laws that protect the rights of owners of intellectual property.

Users must:

- Ensure that the intellectual property rights of the providers of material are respected
- Obtain written permission from the copyright owner to reproduce copyrighted material, including trademarks and logos, text, sound, photographs, illustrations and other graphic images, audio and video files
- Ensure copyrighted material used in information and communication is identified as such

Reproduction of copyright material for the purpose of further distribution outside of what is allowed under the copyright laws is illegal and the use of Government resources for this crime may render the Government liable to prosecution.

Prohibited Use

Prohibited use does not allow the use of ICT resources to create, store, disseminate or retrieve information or material that can result in serious risk, danger, harm or breaches of legislation. Breaches of prohibited use conditions can lead to instant suspension of user access, disciplinary action, and criminal prosecution.

Users must NOT use Government ICT resources to:

- Operate a private business
- Intentionally create, store, disseminate or retrieve information that may:
  - Damage the Government's reputation
  - Be misleading or deceptive
  - Result in victimisation or harassment
  - Lead to criminal penalty or civil liability
  - Be offensive, obscene, threatening, abusive or defamatory
  - Put other users at risk for their personal safety
  - Put other users or government at risk of breaching legislation
- Intentionally create, store, disseminate or retrieve sexually explicit information or material

Attempts to disable, defeat or circumvent any Government ICT systems will be subject to immediate dismissal and/or prosecution. The use of Government ICT resources for illegal activity is grounds for immediate dismissal.

Inappropriate Use

Inappropriate use is where users do not adhere to acceptable use of ICT resources and use resources to access, create, store, disseminate or retrieve inappropriate material. Inappropriate use may lead to suspension of user access, disciplinary action, and criminal prosecution. Users must:

- Be aware that by accessing some internet sites, they may inadvertently be re-directed to an inappropriate site and if this occurs, they should immediately exit the site Seek permission from their employer to access 'blocked' sites for their work
- Report inappropriate messages they believe is offensive, humiliating or intimidating
- Not access, download or store inappropriate or prohibited material
- Not save software or personal files on ICT network drives that reduces disk space
- Not use ICT resources to encourage others to engage in industrial action against government
- Not initiate fraudulent, unlawful or abusive communication
- Not use ICT networks to promote private events, promotions or activities

ICT Support monitors internet use and blocks access to certain websites such as:

- Adult content (pornography) sites
- Gambling sites
- Dating sites

- Chat rooms (not work-related or inappropriate)
- Crime, terrorism or hate sites
- Violence/undesirable activity sites
- Malicious content sites
- Blocked sites (illegal websites)

Unauthorised Use

Unauthorised use includes: unethical, unlawful, inappropriate or prohibited use of Government ICT resources that can lead to disciplinary action and legal proceedings. Users can only access prohibited information websites with prior approval from their employer.

Users must not:

- Attempt to access any hardware, data or programmes that they do not have authorisation or explicit consent to access
- Take official information created, stored, disseminated or retrieved on Government ICT resources from the agency when their employment or work ceases.

Other Provisions

All records relating to the administration of this policy must be kept for at least seven years and are only accessible by the employer and/or authorised staff. After the required seven year period, the agency may destroy the documentation in adherence with government official information management policies.

The Office of the Prime Minister – ICT Division is responsible for reviewing and updating this policy from time to time.

Associated Documents

National ICT Policy, Code of Conduct Policy, Information Management Policy, Official Information Requests Policy

Other information

For policy queries contact the Office of the Prime Minister on phone (682) 25494 or email: support@cookislands.gov.ck