Australian Government

Commonwealth Superannuation Corporation

IT User Guide

Technology Group

Version 2.4

UNCLASSIFIED

Document Information

Title	IT User Guide
File Name	CSC Guide for Using Information and Communication Technology.docx
Publisher	Commonwealth Superannuation Corporation
Department	Technology Group
Status	Authorised
Version	Version 2.4
Print Date	18/09/2014

History

Version	Date	Author	Changes from Previous Version
1.0	01/07/10	[redacted]	Initial Draft
2.0	1/3/11	[redacted]	Revised draft
2.1	June 2014	[redacted]	Updated draft
2.2	16/06/2014	[redacted] Business Analyst	Prepared for formal review
2.3	28/07/14	[redacted] Sen. Exec.	Reviewed draft
2.4	17/09/2014	[redacted] Sen. Exec.	Draft edited to reflect ITAG 5/9/14 input

Authorisation

Name	Position	Date
[redacted]	CEO	18/09/2014

References

Document	Reference	Approved	Date
ICT Security Policy Framework		GM F&R	14/09/2014
Mobile Phone Usage Policy and Guide		ITAG	14/03/2014
eBoard Acceptable Use Policy		SE F&T	02/12/2011
CSC Guidelines for travelling overseas with mobile devices		ITAG	09/05/2014

Contents

Introduction

CSC provides Information and Communications Technology (ICT) infrastructure, including desktop PCs, telephones, internet, email and portable devices such as laptops, phones and iPads for business purposes, to serve the interests of CSC and its stakeholders.

Employees have an obligation to use CSC's ICT facilities properly. Improper use of CSC's ICT facilities may compromise its business objectives, expose CSC to unfavourable publicity and breach the rights of other people under legislation such as Sex, Race, Disability Discrimination and Privacy Acts.

This document describes employees' responsibilities relating to CSC's ICT infrastructure and provides a guide to the proper use of CSC equipment.

Application

This Policy applies to all CSC staff (employees, temporary employees and contractors) and is a term and condition for using CSC ICT facilities.

Scope

This document applies to all CSC ICT facilities, including but not limited to:

- Telephone and fax systems
- Desktop and laptop computers
- Remote access systems
- Mobile devices such as smartphones and tablets

It applies whether these facilities are used at a CSC office or outside of the workplace.

The Guide is set out in three subject areas:

- Security (safe use of the system)
- Probity (proper use of the system)
- Efficiency (efficient use of the system)

Related Policies and Guidelines

CSC ICT Security Policy Framework

CSC Mobile Phone Usage Policy and Guide

CSC Guidelines for travelling overseas with mobile devices

CSC eBoard acceptable use Policy

Key Principles

The ICT service represents a considerable investment to the organisation and any failure, compromise or misuse can have material pervasive impacts and as such it should be used professionally. This document may not address all possibilities of acceptable use and employees must use good judgement, and where necessary, seek advice.

Sensitive information is to be classified and handled appropriately to its classification.

The unauthorised disclosure of sensitive information is likely to result in unfair advantage to competitors, loss of trust of Scheme members, and/or embarrassment to CSC or the Australian Government.

Unauthorised disclosure of sensitive information may result in dismissal or criminal prosecution.

Staff and other users are responsible for ensuring that they use the facilities provided in a professional and lawful manner. Misuse may result in immediate withdrawal of access and employees may also be subject to further disciplinary action including dismissal.

Exercise good judgement in your ICT usage, and consider the ramifications for yourself and the organisation if you act inappropriately or unlawfully. If in doubt, err on the side of caution.

CSC may access employees' devices (including mobile devices), email and file records at any time.

ICT facilities must be used for CSC business purposes only, unless specifically provided otherwise.

Where any personal use is allowed, the exemption will be set out in the guidelines.

ICT facilities are not to be used to support any personal business interest of employees or their associates.

Without exception CSC resources must not be used for charity work, fundraising, etc. without written permission from the CEO.

ICT facilities must not be used for any illegal activity or to circulate inappropriate material.

Any harassment, abuse or bullying of others using ICT facilities or otherwise is not permitted.

ICT facilities must not be used to communicate material, including personal opinion, that might be harmful to the interests of CSC or its stakeholders.

Commentary about CSC or its stakeholders, and detailed information about your CSC role, must be avoided on social media such as Linked In, Twitter, Facebook, etc.

Security

This is a fundamentally important aspect for ICT usage. A secure ICT service:

- is **confidential**: access is controlled
- has **integrity**: is complete, uncorrupted, and free from unauthorised change
- is **available** and accessible for use when required.

There are many controls built in to the ICT service to maintain security; however the proper behaviour of each person using the ICT service is crucial. In addition to these specific security policies, many of the guidelines in this document contribute in some manner to ICT security.

Information security

Sensitive information on CSC systems is crucial to managing the Schemes' assets and delivering superior investment performance to members.

Sensitive information includes:

- Personal details of Scheme members
- Personal details of CSC staff
- Confidential information about CSC business
- Details of sensitive or confidential board discussions
- Ministerial, parliamentary or departmental correspondence.

When you create or handle sensitive information:

1. Consider the consequences of damage from unauthorised use or compromise of the information. If adverse consequences could occur due to unauthorised disclosure or if CSC is legally required to protect the information, mark the information appropriately.
2. Do not remove or alter the protective markings on data or equipment.
3. Only the CEO or appropriately authorised manager may make a determination to change the classification of sensitive information.
4. Sensitive information can only be sent outside CSC when a **business purpose** requires communication between CSC and an external entity (eg businesses, members).
5. Only the CEO or appropriately authorised manager may approve the public release of sensitive information.
6. Only the CEO or appropriately authorised manager may approve the removal of sensitive information from CSC premises.
7. All employees must apply the **need to know** principle to the release of sensitive information.
8. Only use the secure means authorised by the Technology Group for transmitting or transferring sensitive information.

9. All sensitive information must be stored and processed away from public access on CSC premises and within the CSC network.
10. Only use the secure means authorised by the Technology Group to dispose of sensitive information.

Network access

When accessing the CSC network:

1. You are responsible for all actions performed using your account.
2. Commit your account password to memory – do not write it down or save it to your phone. If you have forgotten your password, ask IT Help Desk to reset it for you. For users with numerous password-controlled activities, a password management solution will be provided.
3. Never share your password with others or ask another user for their password.
4. Do not log in with another user's account or pretend to be another user.
5. Lock your screen when you leave your computer unattended – shortcut is [⊞ + L]
6. Log out from your account at the end of the day.
7. Immediately report any theft, loss, damage or degraded performance of CSC equipment to IT Help Desk.
8. Do not move or copy corporate data from the CSC network without written authorisation.
9. Contact IT Help Desk if you need to access a flash drive (USB key, memory stick, thumb drive, etc) or CD. These devices are normally blocked to reduce the risk of introducing viruses or losing corporate data.
10. Always store corporate data on the network folders of the appropriate business unit (preferable) or your H: drive. The C: drive of a CSC computer is not backed up and data may be lost if the computer has a fault or is compromised.
11. Do not disrupt network communication or breach security. Security breaches include, but are not limited to, accessing data you are not authorised to access or logging into a server or account you are not expressly authorised to access, unless these duties are within the scope of your authorised duties.
12. Do not perform network monitoring, port scanning or security scanning, unless this activity is a part of your authorised duties.
13. Do not tamper with or circumvent the security of any CSC network, computer or account.
14. Do not interfere with or deny service to any other user.

Remote access

Staff may access the CSC network remotely from personal devices (eg. home PCs) or CSC-issued devices using Citrix. When using this service:

1. Observe all the policies for Network access.
2. Do not use a computer to remotely access CSC unless you are confident that it is reasonably secure – in particular, it is password-protected.
3. Do not use remote access to CSC for non-business purposes.
4. Do not allow remote access to CSC by non-staff unless authorised by the CEO.

Mobile devices

Mobile and portable devices such as laptops, tablets and phones have a high risk of loss or theft and must be treated with extra caution. CSC monitors and manages its iPhones and iPads using Mobile Device Management (MDM) control. This monitoring also includes GPS location information for device tracking.

If you have been issued a CSC mobile device:

1. Secure the device by password or PIN, with the automatic lock screen enabled.
2. As with CSC network access, you are responsible for all actions performed using the device. Never share your password or PIN.
3. Change the device password or PIN at least once every 60 days or as directed by CSC.
4. Avoid storing sensitive corporate data on the device.
5. Ensure that the device remains protected against malware, unauthorised access, unauthorised configuration changes, etc. using security products approved for this purpose by CSC.
6. Physically protect the device from loss, theft, damage or unauthorised access.
7. Do not leave the device unattended in public areas, unlocked offices, vehicles, hotel rooms, homes etc. without physical security such as an approved security cable lock, locked cabinet, drawer or safe.
8. Use caution when connecting the device to unknown or unsecured wireless networks, as they can be ‘tapped’.
9. Use encrypted internet connections (ie. https://) when valuable data and/or passwords are being communicated.
10. Report security incidents and near misses relating to the device to IT Help Desk without delay.

Email and Internet

When using CSC email or the Internet:

1. Do not communicate passwords or usernames.
2. Maintain the confidentiality of sensitive information.
3. Do not email work to your home. Do not use a personal email account for CSC business.
4. Only open email attachments or links when you are 100% certain they are safe. Email may contain malicious software that can damage CSC's network or steal information, passwords etc.
5. Do not access questionable websites or use unauthorised applications such as peer-to-peer sharing tools to download, receive or distribute non-work related videos and games. This constitutes a security breach, exposes CSC to severe risk of data infection from viruses and has an adverse impact on other core services.
6. Do not access email records of other employees. Managers (or persons authorised by management) can access email to ensure compliance with this policy. An authorised employee who has a request to attend to a fault, upgrade or similar situation can also access email. In each case, this will be limited to the minimum needed to complete the task.
7. Do not disclose detailed work related material (including detailed job descriptions) on social media such as LinkedIn and Facebook

Software and Hardware

1. Do not install software or hardware without written authorisation from the Senior Executive Technology & Business Services.
2. Do not download software from the internet or from unauthorised disks, USB drives etc. on to the internal network unless the Senior Executive Technology & Business Services gives you specific written permission.
3. Submit a business case for approval by your General Manager if you require new software or equipment beyond the standard issue.

Probity

These guidelines are to assist you in using email, internet and other IT services properly. At all times you should act professionally and responsibly in using these facilities and if in doubt speak to your reporting manager or the IT team.

Failing to comply with these guidelines is a disciplinary offence that CSC will investigate. In serious cases, the penalty for an offence, or repetition of an offence, may include dismissal. Some forms of misconduct may be open to criminal prosecution.

In addition to these guidelines sanctions set out in the various Acts and regulations governing personnel of particular types of information (eg personal information) may be applied where an employee has been found to misuse the resources to which he/she has been granted access and/or performed activities prejudicial to security and privacy. Depending on the nature of the employee's actions, sanctions may range from counselling and temporary suspension of system access rights through to corrective action and to dismissal and/or legal action.

Network access

When using a CSC computer:

1. Do not procure or transmit material that could be considered offensive or is in violation of sexual harassment or other workplace laws in the user's local jurisdiction.
2. Do not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, installing or distributing "pirated" or other software products that are not appropriately licensed for use by CSC.
3. Do not make unlawful copies of copyrighted material including, but not limited to, digitising and distributing photographs from magazines, books or other copyrighted sources, copyrighted music, or installing copyrighted software for which CSC or the end user does not have an active licence.
4. Do not export software, technical information, encryption software or technology, in violation of international or regional export control laws.
5. Do not make fraudulent offers of products, items, or services.

Mobile devices

Mobile devices must be used lawfully and professionally by legitimate users in accordance with CSC's organisational policy framework. Mobile devices are provided for business purposes, subject to the following:

1. Do not let personal use of a CSC mobile device interfere with or distract from work or subject the organisation to undue risk or expense.
2. Do not tamper with a mobile device and/or interfere with, disable or remove Mobile Device Management controls.

3. Exercise good judgement and especially avoid using CSC equipment for the storage of contraband material or material otherwise unsuited to a corporate device.
4. You are never authorised to engage in any activity that is illegal under local, state, commonwealth or international law while using the mobile device.
5. Avoid circulating opinion in social media, blogs, Twitter, etc. that may reflect badly on or harm CSC or its stakeholders.
6. Usage of CSC equipment may be monitored and mobile devices can be subject to remote monitoring by CSC Technology Group. CSC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Users of CSC mobile devices may also refer to supplementary policy guides:

CSC Mobile Phone Usage Policy and Guide

CSC Guidelines for Travelling Overseas with iPhones, iPads and Laptops

Email

Email is not private and in most cases not secure. You should assume that one day something you send is going to end up on the wrong person's screen. Email can be copied, re-sent, cc'd, bcc'd and generally broadcast to the world and the source is traceable. What you may consider "personal" may be public on the internet and email. The guiding rule for sending email is that if you are the least bit unsure if it is "ok" to send an email due to its content then do not send that email. Check with your reporting manager first.

To protect CSC from the potential effects of the misuse and abuse of email, all users must observe the following instructions when using CSC-provided email:

1. Do not use another person's email or pretend to be another person.
2. Do not send any material that is defamatory, in breach of copyright or confidentiality, or prejudicial to the good standing of CSC in the community or to its relationship with employees, members, suppliers and any other person or business with whom it has a relationship.
3. Do not send joke mail or images that are offensive, harassing or obscene, or download this type of material from the internet.
4. Do not use CSC-provided email to express political views or beliefs which are not part of your official duties without the approval of the CEO.
5. Do not send any material that amounts to gossip about colleagues or that could be offensive, demeaning, persistently irritating, threatening or discriminatory, involves the harassment of others or concerns personal relationships.
6. People sometimes disclose information, express views or include casual remarks in an email which they wouldn't disclose in a formal letter or memo. Avoid responding in the heat of the moment and consider the implications of responding 'reply-all' to email. Be careful when forwarding email as it may contain history from earlier responses.

Email you send

Email has legal status as a document and courts of law accept email as evidence. Even when used for private purposes, CSC can be held responsible for the contents of email messages, including any attachments. Access to email can be demanded as part of legal action in some circumstances.

When using CSC-provided email systems:

1. Do not let personal use of CSC email interfere with or distract from work or subject the organisation to undue risk or expense.
2. Maintain the confidentiality of sensitive information.
3. Include the approved CSC disclaimer on all email you send externally.
4. Set up a standard signature block for your email. Instructions are available from the CSC Intranet:

   https://intranet.csc.gov.au/files/download/?id=317
5. Use CSC letterhead to issue formal memos, documents and letters for which signatures are important, regardless of whether you use a physical or electronic delivery method.

Email you receive

If you receive an email that is inappropriate or suspicious:

1. Do not re-send or otherwise circulate the message.
2. Delete the message, and then empty the Deleted Items folder in Outlook to fully delete email.
3. If the sender is known to you, advise the sender in a new email not to send material of that nature again (do not resend the material with your reply).
4. Advise your reporting manager and IT Help Desk if it is of a serious nature or has occurred regularly.

Internet

Internet access is provided for business use. CSC permits limited private use provided it does not interfere with or distract from your work. Management has the right to access the system to determine whether private use is excessive or inappropriate.

When using CSC-provided internet:

1. Observe all the policies for email usage.
2. Do not access, other than by accident, sites or incoming email portraying obscene, violent, defamatory or unlawful material (images, audio or text) that could be considered offensive by your colleagues or CSC members or cause CSC to be in breach of equal opportunity or anti-discrimination legislation or other elements of the law.
3. Do not download or print material as described above.

4. Do not show or play to others, or allow others to see, hear or read items as described above or otherwise items that could be confronting to others.

Efficiency

Use the allocated IT and communication resources efficiently.

Do not use CSC resources for running a personal business or, without express permission from the CEO, working on charity etc matters.

Use of the Network

When accessing the CSC network:

1. Limit storage on common drives to business-related items only.
2. Use your 'personal 'H: drive for confidential and limited incidental personal storage. System controls prevent the storage of personal video, music etc.

Telephones

CSC acknowledges that you may use its telephone system for reasonable personal use. However, if you make more than a few personal calls a day we ask that you use your own personal equipment. Personal telephone calls to overseas numbers are not permitted.

Mobile phones

The rules for telephones apply to personal use of CSC mobile devices.

If you are going on an overseas holiday, CSC will usually only cover the cost of overseas use if your General Manager has advised IT in advance of your departure that there is a business requirement for you to use the device overseas.

You should be aware that overseas phone (and particularly data) use may incur significant charges, and you should refer to the "Guidelines for Travelling Overseas with iPhones, iPads and Laptops" that can be found on the CSC intranet.

Email

When using CSC email:

1. Use email for formal business correspondence.
2. Do not let personal email interfere with or distract from your work. CSC permits limited personal use of email; however management has the right to access incoming and outgoing email messages to determine whether your usage is excessive or inappropriate. CSC does not permit excessive private use, including mass mailing, reply to all etc. that are not part of your duties.
3. Save and file email to an appropriate common drive if you need to preserve them as formal records.
4. Minimise email size whenever possible by compressing attachments as ZIP files, converting them to PDF, or linking files from common drives instead of attaching them.

5. Delete old non-critical emails after a period of time or save them to the appropriate drive. Email file size limits may be applied by the organisation from time-to-time. IT Help Desk will identify oversize mailboxes and assist with resolution.

Internet

When using CSC-provided Internet access, in office or via a mobile device:

1. Use Internet access mainly for business purposes.
2. Do not use Internet access for running personal business activities or, without express permission from the CEO, engaging in charity work.
3. Do not engage in repeated or prolonged use that is not directly relevant to your work.

Frequently Asked Questions

Is my internet use monitored?

CSC monitors Web usage at the corporate level and can monitor the internet usage of an individual if necessary.

Why has a web site been blocked in my browser?

CSC uses a commercial site classification service that will block (or caution) certain categories of sites. Occasionally a valid site may be blocked because, for example, it is unknown to the categorisation service. Contact the IT Help Desk if you need a valid site unblocked.

Is my email monitored?

CSC can monitor email, but will not generally do so except in the event of an investigation. An archive of all messages communicated by the CSC email system is retained for auditing purposes.

Are my phone calls monitored?

No, CSC does not listen to your phone calls. However, telephone billing records include detail about the numbers dialled, messages sent, time of calls, etc. on a CSC phone and these are retained for auditing purposes. Some phone calls made with other parties such a custodian may be recorded by them.

Is my office attendance monitored?

No, CSC does not monitor your attendance at its offices. No audio or video surveillance is performed within the confines of CSC premises. However, your access to and from the office is recorded both electronically and via closed-circuit television and an access log is retained for auditing purposes.

END OF DOCUMENT