Comcare Technology

Technology Common Use Policy

Version 1.1

Issued 20/11/2013

Australian Government

Comcare

Table of Contents

DOCUMENT CONTROL

Revision History

Version	Date	Author(s)	Stakeholder to receive version	Reason(s) for change
0.1	5 Nov 2012	s47F	s47F	Initial Draft
0.2	7 Nov 2012	s47F	s47F	Incorporates reviewer feedback
1.0	11 Dec 2012	s47F	Noted Exec Committee / CSG Meetings of 13/11/12	Final Version
1.1	20 Nov 2013	s47F	s47F	Updates to include wireless access

Document Purpose

The purpose of this document is to outline Comcare Technology ('Technology') Common Use policy.

Distribution List

Name	Position	Role
s47F	Chief Information Officer	Signatory
s47F	Policy and Communications Officer	Reviewer
s47F	Network Manager	Reviewer
s47F	Service Delivery Manager	Reviewer
s47F	ICT Governance & Contract Management	Reviewer

Related Documents

Document Type	Document name	Location / Path / TRIM Reference
Policy	CEO Directions: Use of Technology Resources	
Policy	Comcare Security Policy	
Policy	Technology Security Policy	

1 Introduction

A wide range of Technology resources is available to assist Comcare staff with the performance of their official duties.

Comcare permits limited personal use of its technology resources as long as such use has no more than a negligible impact on the capacity of Comcare staff to perform their official duties.

No use of Comcare's technology resources is private and all use will be monitored to ensure compliance with this policy as well as other applicable policies, guidelines and legal requirements.

It is important for Comcare staff to understand their privileges and responsibilities in relation to Comcare's technology resources as well as what disciplinary action may result if staff do not comply with this policy.

2 Definition of Terms

Term	Definition
Access Restriction Notice	A notice confirming that Comcare has prevented a particular website, or other Internet content, from being accessed by Comcare staff in accordance with paragraph 3.2 of this Direction.
ASA	Agency Security Adviser – Director Property & Services
Case	The 'box' or enclosure which contains the main computing components of a Desktop Computer, also referred to as the 'desktop' or 'tower' depending on its dimensions.
CEO	The Chief Executive Officer of Comcare appointed by the Governor-General under s 74(1A) of the *Safety, Rehabilitation and Compensation Act 1988* (Cth).
CIO	The Chief Information Officer plans, organises, directs, controls and coordinates the Technology strategies, plans and operations to ensure technology infrastructure supports Comcare's overall operations and priorities.
CMSA	Comcare's Health and Safety Management Arrangements
Comcare Executive	Comcare staff at Director Level or above
Comcare staff	The staff of Comcare as defined by s 88 & 89 of the *Safety, Rehabilitation and Compensation Act 1988* (Cth).
Desktop Computer	A personal computer in a form intended for regular use at a single location, as opposed to a mobile computing device such as a Laptop or tablet or smartphone. A reference to the term 'Desktop Computer' in this Direction includes the Case, the output devices (including monitors), the input devices (including mouse, keyboard), and any speakers, headsets, printers, scanners or other peripheral devices that may be attached to the Desktop Computer from time to time.
Dissemination Limiting Markers (DLMs)	Dissemination Limiting Markers (DLMs) are protective markings for information where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling.
Email Classification Software	The software application (sometimes referred to as Comcare's "email [protective] marking software") that controls the insertion and handling of appropriate security classifications and protective markings with respect to all of Comcare's incoming and outgoing emails;
FedLink	FedLink provides secure communications between Federal Government agencies at the PROTECTED and IN-CONFIDENCE security levels. Refer to Appendix A for further information.

Term	Definition
Good	A software application that allows personal mobiles to access Comcare's email and calendar functionality within Outlook.
HSMAs	Comcare's Health and Safety Management Arrangements
ITSA	Information Technology Security Adviser
Laptop	A small mobile computer that is capable of being carried and used from many different locations.
Mobile Worker	A staff member who spends at least 25 per cent of their time out in the field (rather than simply travelling between offices, meetings or conferences) and requires access to a computer whilst in the field to efficiently perform their work functions. This does not include someone who works from home or uses a mobile device unless they also meet the above criteria.
Portable Communications Device	Any portable device capable of communicating with other devices such as a mobile phone, a smart device or any other portable communications device.
Portable Device	A laptop, smartphone, tablet or any other mobile device designed for portability and intended for use from remote locations.
Portable Resource	Any portable technology resource including, but not limited to: • a Portable Computer; • a Portable Communications Device; • a Portable smart device; or • a portable storage device or removable storage medium such as a USB storage device (also known as a USB key, flash drive or memory stick), compact disk (CD), digital versatile disk (DVD) or external hard drive.
Prevented Delivery Notice	A notice confirming that Comcare has prevented a message based communication (such as an email) from being delivered to its intended recipient in accordance with paragraph 3.2 of this Direction.
Prohibited Material	Material defined as Prohibited Material in paragraph 7.1 of this Direction.
Protective Markings	Once information has been identified as requiring some form of protection and special handling a protective marking is to be assigned to the information. The marking indicates: - that the information has been identified as sensitive or security classified, and - the level of protective procedures that are to be provided during the use, storage, transmission, transfer and disposal of the information. A protective marking indicates the required level of protection to all users of the information. The system, therefore, provides an assurance that information of broadly equivalent worth or value is given an appropriate and consistent level of protection. Information requiring a protective marking that is held on Technology systems is to be identified in the same way as information held on other mediums (such as paper documents) and given an appropriate level of protection. There are three types of protective markings: - Security Classifications; - Dissemination Limiting Markers (DLMs); and - Caveats.
PSPF	Commonwealth Protective Security Policy Framework

Term	Definition
Security staff	Comcare's Technology staff and all Comcare staff defined as security contacts within the CEO Direction - Protective Security
Smart Device	The term "Smart Device" refers to the latest generation of mobile phone and tablets that have telephony, Internet access and computing capabilities. This includes iPhones, iPads, tablets and a range of equivalent devices.
Smartphone	A smartphone is a mobile phone built on a mobile operating system, with more advanced computing capability and connectivity than a standard mobile phone. Smartphones includes features such as: • the functionality of portable media players; • high speed data; • wifi; • digital cameras; • pocket video cameras; and • GPS navigation units to form one multi-use device.
Tablet	A tablet refers to a mobile Personal Computer. It has a touchscreen that allows the user to operate the computer with a stylus or digital pen, or a fingertip, instead of a keyboard or mouse. Tablets can use operating systems normally used on smartphones such as Android or iOS (Apple). This gives Tablets the same connectivity as a mobile phone but with more power and functionality.
Technology Manager / Technology Team Manager	All staff at the Executive level who are employed by Comcare to manage Technology Resources, Technology staff and/or Security.
Technology Resources	All technological resources which assist Comcare staff to access, use, store and/or communicate information including current resources such as: • Desktop Computers, Portable Computers, Smartphones, Tablets and other computing devices; • mobile and fixed line voice communications devices including traditional telephones, video conferencing units and mobile phones; • server equipment and other networking devices and infrastructure; • output devices such as printers, projectors and audio output devices; • image based devices such as scanners, photocopiers and facsimile machines; • business systems and other Comcare owned software applications including Internet, email and instant messaging browsers; and • any other Technology Resources that may be made available to Comcare staff from time to time.
Technology Service Desk	Technology Service Desk – responsible for the management and deliver of technology services in Comcare
Technology Service Providers	External companies or organisations that supply services procured by Comcare including, but not limited to: • Technology consultancy services; • Data centre hosting; • Internet service provision; and • software services.
Technology staff / Technology Team members	All staff and contractors employed or engaged by Comcare Technology from time to time to carry out application development, security and/or network administration tasks.
TRIM	Comcare's Electronic Document and Record Management System (EDRMS).

Term	Definition
WHS	Workplace Health and Safety.
WHS staff	All staff appointed or engaged by Comcare to ensure that Comcare staff comply with the requirements of the *Work Health and Safety Act 2011* (Cth).
Wireless / Wifi	Wireless commonly termed Wifi refers to the technology that provides a Local Area Network connection using a wireless signal. Wi-Fi provides network access for portable devices such as laptops without the need to connect to a network cable. Wi-Fi networks have limited range and a lower bandwidth compared to a cable connection and may not suitable for all applications.

3 Monitoring of Technology Resources

3.1 Monitoring

Comcare extensively monitors and logs all use, including personal use, of Comcare's technology resources.

Comcare's technology resources are monitored to:

- ensure compliance with this policy as well as other applicable policies, guidelines and legal requirements;
- assist Comcare's Technology with their system administration, security, maintenance and resource management duties; and
- assist Comcare's WHS staff with their injury prevention and management duties.

Comcare's monitoring and reporting practices may include:

- monitoring, logging and reporting on the timing, source, destination and contents of voice, Internet, email and other message based communications;
- monitoring, logging and reporting on access to, and use of resources such as desktop computers, portable computers, storage devices, server equipment and other network devices (including printers); and
- the implementation of rest break software which monitors activities such as key strokes, mouse clicks, time using a computer, break compliance, use of software applications and selected rest break settings.

By way of example, this means that Comcare Technology can, and will at times, view email messages passing within Comcare's communications infrastructure and also access information regarding websites visited by Comcare staff, the time spent on those websites, and any interactive activities undertaken by Comcare staff.

Members of the Comcare Executive or the Director of People may initiate targeted investigations into the use of technology resources by specific Comcare staff where the Comcare Executive believes there may have been a breach of this policy or another applicable policy, guideline or legal requirement. A range of additional investigative, monitoring, logging and reporting practices may be implemented by Comcare if a targeted investigation is initiated.

Comcare's Technology will ensure that all monitoring, logging and reporting practices comply with all applicable legal requirements including those arising under the *Telecommunications (Interception and Access) Act 1979* (Cth) and the *Privacy Act 1988* (Cth).

3.2 Use of information

Subject to the exceptions contained in the Information Privacy Principles set out in the *Privacy Act 1988* (Cth), the *Freedom of Information Act 1982* and the CEO Direction on Privacy, information collected through Comcare's monitoring, logging and reporting practices will only be made available to:

- Authorised Comcare Technology staff;
- Members of the Comcare Executive; and
- Comcare's WHS staff.

3.3 Blocking / access restriction

In addition to monitoring the use of technology resources, Comcare also reserves the right to block and/or restrict access to certain communications, including communications that are suspected of containing:

- unsolicited marketing material (eg spam,etc);
- malicious software or other executable files (eg viruses, Trojans, worms etc);
- email attachments which, together with the rest of an email, result in a total message size which exceeds 10 megabytes; and/or
- prohibited material, as defined in paragraph 7.1 of this policy.

If Comcare prevents the delivery of a message based communication such as email or access to a particular website or other Internet content, a Prevented Delivery Notice or Access Restriction Notice will be provided to any affected Comcare staff member(s).

4 Compliance

4.1 APS Code of Conduct

Comcare's technology resources must not be used in any way that compromises the integrity and good reputation of Comcare or the Australian Public Service (APS).

Comcare staff must always use Comcare's technology resources in accordance with the APS Code of Conduct set out in the *Public Service Act 1999* (Cth).

4.2 Deemed Policy Acceptance

Comcare staff must not use Comcare's technology resources unless they have read, understood and accepted the directions set out in this policy.

If Comcare staff are unsure as to whether a certain use of Comcare's technology resources would contravene this policy, they must contact the Technology Service Desk for clarification before using the technology resources in that manner.

In requesting access to and using Comcare's technology resources, Comcare staff are deemed to have read, understood and accepted the directions set out in this policy.

5 Consequences of non-compliance

5.1 Process for actioning non-compliance

All instances of suspected non-compliance with this Direction will be handled as follows in accordance with the CEO Instruction: Breaches of the Code of Conduct.

5.2 Sanctions for non-compliance

Non-compliance with this Direction may result in disciplinary action under the Public Service Act 1999 (Cth) including, but not limited to:

- termination of employment;
- reduction in classification;
- re-assignment of duties;
- reduction in salary;
- deductions from salary, by way of fine; or
- reprimand.

Non-compliance with this Direction may also result in withdrawal of personal use rights or loss of other privileges.

Staff must also understand that the penalties specified in the Criminal Code Act 1995 (Cth), the Crimes Act 1914 (Cth) and other applicable legislation may also result from improper use of Commonwealth information and resources.

6 Permitted Use of Technology Resources

6.1 Permitted Use

Comcare's technology resources are the property of Comcare and, as such, they may only be lawfully used by Comcare staff in the manner that Comcare permits.

Comcare staff is only permitted to use Comcare's technology resources for the performance of their official duties subject to the limited personal use exception set out in paragraph 6.2 below.

All other use of Comcare’s technology resources by Comcare staff is strictly forbidden, unless appropriately authorised in writing in advance.

6.2 Limited Personal Use

Limited personal use of Comcare's technology resources by Comcare staff is permitted as long as:

- it is not prohibited use as defined in this policy; and
- it has no more than a negligible impact on Comcare's operational effectiveness, clients, staff and resources.

As a guide, use that occurs more than a few times per day and/or for periods longer than a few minutes would not be considered limited personal use.

While Comcare staff may use Comcare's technology resources for limited personal use, that use must be confined as much as possible to lunch breaks and before or after working hours.

Comcare does not accept responsibility for any loss or damage, however caused (including through negligence), which Comcare staff may directly or indirectly suffer in connection with their personal use of Comcare's technology resources, nor does it accept any responsibility for any such loss arising out of personal use of, or reliance on, information contained on or accessed using Comcare's technology resources.

7 Prohibited Use of Technology Resources

7.1 Prohibited Material

Prohibited Material is material that Comcare staff is forbidden, by this policy or any other lawful direction from the Chief Executive Officer, to create, access, store or communicate using Comcare's technology resources, including:

i. material that contains:
   a. text, graphics or other material of a sexual nature (including pornography and other sexually explicit material);
   b. multimedia files such as movie, video or audio files (eg mpeg, mp3 etc) except material that is expressly permitted and appropriately authorised in writing in advance;
   c. images of children you do not know or do not have specific permission to use;
   d. images of any children in any state of undress;
   e. jokes or comments of a personal nature (eg about race, age, gender, disability, marital status, sexual orientation, religion, political beliefs or appearance);
   f. offensive language or other offensive material;
   g. disparaging comments about any persons including staff of other agencies, politicians, members of the public or any government;
   h. chain messages (including messages containing text or graphics promising good fortune if the recipient forwards the message to others or bad fortune if they don't);
ii. material that constitutes a form of unlawful discrimination or potential harassment;
iii. material that constitutes a breach of the Privacy Act, or is contrary to any other legislation;
iv. material that disrespects the privacy of others or breaches their confidentiality;
v. criminal skills material including, but not limited to, instructions on how to defraud a Government agency, how to access personal information of other people, how to obtain drugs or stolen property and how to create weapons or explosives;
vi. gambling material;
vii. racially offensive material being material which, if communicated, would constitute offensive behaviour within the meaning of section 18C of the Racial Discrimination Act 1975; and
viii. defamatory or abusive material.

Comcare staff should inform the Technology Service Desk if they:

- receive any prohibited material;
- are offended by any material they receive; and
- are unsure whether material is prohibited material.

7.2 Prohibited Use

While it is not practical to exhaustively define every possible form of prohibited conduct in this Direction, the following list contains examples of some of the conduct that is prohibited.

Comcare staff must not use Comcare's technology resources to:

i. engage in any unlawful conduct, including any conduct that contravenes the *Privacy Act 1988* (Cth), the *Copyright Act 1968* (Cth), the *Spam Act 2003* (Cth), the *Do Not Call Register Act 2006* (Cth), the *Telecommunications Act 1997* (Cth), the *Telecommunications (Interception and Access) Act 1979* (Cth), the *Archives Act*

1983 (Cth), the *Sex Discrimination Act 1984* (Cth), the *Disability Discrimination Act 1992* (Cth), the *Crimes Act 1914* (Cth), the *Criminal Code Act 1995* (Cth), the *Public Service Act 1999* (Cth) or the *Commonwealth Authorities and Companies Act 1997* (Cth);

ii. engage in any sexual conduct that may make a person feel offended, humiliated and/or intimidated, where that reaction is reasonable in the circumstances (eg communicating a suggestive, graphic or sexually explicit message, even if the intended recipient consents in advance; or using a desktop computer, laptop or other device to access graphic or sexually explicit material);

iii. engage in any conduct that vilifies, harasses or discriminates against a person on the basis of their race, sex, religion or disability;

iv. express or promote a political view or criticise a government action or policy;

v. set up and/or maintain an unauthorised web page, or advertise, operate or promote a private business enterprise;

vi. communicate material promoting the business activities of an individual or organisation other than Comcare without authorised written approval (excepting fundraising for charities and social clubs where approval may be sought from an EL2 or SES officer);

vii. solicit a donation, or conduct opinion polling or social research without authorised written approval;

viii. infringe, or authorise the infringement of, copyright or other intellectual property rights;

ix. access, attempt to access, use, attempt to use, communicate or attempt to communicate information, including Comcare information, without appropriate authorisation;

x. damage, corrupt or destroy, or attempt to damage, corrupt or destroy any Comcare information or other information accessible using Comcare's technology resources without appropriate authorisation;

xi. engage in activities which may compromise the security of, or cause damage or disruption to, the operation of Comcare's technology resources or any other network or computer system;

xii. represent oneself anonymously or as someone else, whether real or fictional;

xiii. subvert, or attempt to subvert restrictions on the use of Comcare's technology resources;

xiv. access, use or participate in chat sites, newsgroups or discussion forums without authorised written approval except for those Social Media sites which have been previously authorised;

xv. download, install, store or execute any executable program or computer software without express prior written authorisation from the Comcare Chief Information Officer;

xvi. access, store or communicate any prohibited material without prior written authorisation; or

xvii. engage in any behaviour that is expressly prohibited elsewhere in this policy or by any other lawful direction of the CEO.

If Comcare staff are unsure about whether any proposed conduct may constitute prohibited use for the purposes of this policy, they must seek clarification from Comcare's Technology Service Desk *before* engaging in the proposed conduct.

8 Classified Information

Comcare is responsible for protecting information in accordance with the applicable requirements of the Commonwealth *Protective Security Manual and the Privacy Act 1988* (Cth). Comcare's technology resources must not be used to communicate personal or commercially sensitive information except where Comcare information systems employ appropriate authentication and encryption mechanisms (eg the Customer Information System).

Comcare's e-mail system generally does not provide for the secure communication of information. It must not be used to communicate personal or commercially sensitive information (classified using a Dissemination Limiting Markers - DLM) unless an authorised secure connection facility is employed (eg FedLink).

FedLink provides secure communications between agencies across the public Internet at the UNCLASSIFIED with DLMs and higher security levels. A list of agencies connected by FedLink is available at http://www.fedlink.cybertrust.com.au/status.htm.

If you need to transfer personal, sensitive or information classified using DLMs to an organisation not on the Fedlink list contact the Technology service desk. Alternative secure communications can be made available such as our secure email link to ACT Government email addresses.

9 Employee Representatives

Employee representatives and union delegates may use Comcare's technology resources to communicate between themselves and the staff they represent in undertaking industrial relations activities relating to Comcare. However, this does not include material related to elections external to Comcare, the promotion of union membership, or the promotion or advancement of industrial action.

10 Supervision of Comcare staff

Supervisors must ensure that:

- their staff comply with this policy; and
- the Technology Service Desk is notified of any changes to staff system access requirements, including reduction of access rights.

11 Use of Resources

All Comcare staff will have access to a desktop or a laptop computer and other Technology resources to assist them with the performance of their official duties. This policy sets out the practices that must be followed when using Comcare's technology resources to ensure they continue to operate correctly and that support costs are minimised.

Technology is responsible for the provision, support and maintenance of all technology resources owned by Comcare. The Comcare operating system installed on Comcare's desktop and laptop computers has been designed to meet the needs of Comcare staff.

General users are provided access to the Windows desktop, MS Office applications, user drives, email and business applications required to perform their role. Access to business applications is approved by Business and System owners. User access privileges are modified as required when the staff member's role changes.

User accounts will be disabled when a staff member ceases employment or at Comcare's discretion. User account information will be maintained for a maximum of 60 days. After 60 days, disabled accounts will be removed from the system and their profiles and email will be archived for 3 months. After this timeframe, access to the users file or email data will be by backup restoration and requires a business case.

11.1 Software

A standard suite of software is installed on each desktop and laptop computer. In addition, a number of additional software products and services are made available on some computers to meet specific needs (e.g. Microsoft Project).

All software operated by Comcare staff using Comcare's technology resources must be licensed to Comcare. The unlawful reproduction or operation of computer software using Comcare's technology resources is strictly forbidden. In order to comply with Comcare's licensing agreements, software must not be copied from one desktop computer to another.

Comcare staff must not install any software, including games, utilities, screen savers or different versions of standard software, on desktop and laptop computers and/or other technology resources.

If a staff member has a portable device (smartphones and tablets), a range of applications certified by the manufacturer as safe for use in their device are available from an authorised website. These applications are available both free of charge and at cost.

If a staff member wishes to purchase an application for use on their corporate smart device, they must pay for the application using their own funds. If there is any doubt in regard to use of portable device applications, please contact the Technology Service Desk for further information.

Technology will scan Comcare's Desktop Computers on a regular basis to maintain software licence commitments. Technology staff are authorised to remove any unauthorised software or copyright data such as music or videos.

11.2 Hardware

Comcare devices must not be connected to any other organisations' network unless authorisation is provided. Comcare devices must not be connected with any business network, other than Comcare's without the permission of the Chief Information Officer.

Comcare staff is required to power down their desktop or laptop and monitors when they are finished using them at the end of each day. This practice ensures optimal performance for your PC the next business day and saves on power.

This practice will ensure critical software updates are applied to desktop or laptop computers ensuring they are kept up to date. Technology may at times force a restart of your desktop computer or laptop outside of business hours should this practice be required.

To ensure that warranty provisions are not breached and that the security of desktop computers, technology resources and the Comcare network is not compromised, Comcare staff must not attempt to connect any peripheral device to a desktop and laptop computer and/or a technology resource. In particular, personal items such as tablets, smart phones, MP3 players or IPODs, must not be connected or synced to Comcare equipment.

Privately owned laptops or portable devices must not be connected to the Comcare network unless prior authorisation has been provided.

11.3 Moving Computer Equipment

Other than designated portable devices such as laptop computers, tablets or smartphones, technology resources must not be moved without prior consultation and approval from the Technology Service Desk.

Comcare's Technology Service Desk must be consulted prior to the relocation of any fixed desktop and laptop computers and/or technology resources to allow sufficient time for any necessary changes to the network to be made.

Movements of technology resources between State offices must be made via the Technology Service desk to ensure that the correct modification of configurations is made and that the Technology Asset Register is changed to reflect the equipment location.

11.4 Bring Your Own Device Option

Comcare supports the use of the Bring Your Own Device option for staff who have private smartphones and tablets and who are authorised to access email from their device. For further details, refer to the Portable Device Policy.

11.5 Storing files

Records are corporate assets which belong to Comcare. All staff and their colleagues need to know where these records are and how to access them. Staff must not store corporate records in a private store, such as a desk drawer, CD/ DVD's or computer hard drive.

Corporate records should be placed into Comcare's recordkeeping system (EDRMS) - TRIM. The corporate document storage location is backed up on a daily basis.

12 Email Security

Comcare classifies all email messages according to their degree of sensitivity and confidentiality. Staff must ensure that all emails are:

- appropriately classified and marked;
- prepared on the assumption that they may have legal consequences; and
- handled with the same courtesy, discretion and formality as traditional paper based communications.

Email messages sent to internal addresses remain within Comcare's secure network so there is minimal risk of unauthorised interception. Externally addressed emails leave Comcare's secure network and, in many cases, pass over a number of networks where there is a significant risk of unauthorised interception.

Staff must ensure that the content of any externally addressed email is appropriate for transmission over unsecured networks. Staff must also bear in mind that email can have the same legal effect and consequences as written communications in many circumstances.

12.1 Email Classification

An information classification system is used at Comcare. Appropriate classification information is set out in this document as well as the following documents:

- Comcare's Security Policy; and
- CEO Direction - Protective Security.

Staff must familiarise themselves with each of these documents and contact Comcare's Technology Service Desk for clarification regarding anything they do not understand before using Comcare's Technology Resources.

Comcare staff must be aware that Dissemination Limiting Markers (DLMs) are used to classify information and emails.

Comcare staff who use the Good application on a smart device (that is; smartphone or tablet) must ensure that they only access information that is rated as unclassified or lower.

12.2 Receiving Emails

All inbound emails are passed through filtering mechanisms before being allowed into Comcare's email network. All inbound emails received from other government agencies with a classification marking of PROTECTED or higher will be blocked at Comcare's email gateway (Fedlink). The sender will be notified of the delivery failure and its cause.

All other emails will be delivered to their intended recipients.

12.3 Sending Emails

All outbound emails with a DLM protective marking will be checked by the email gateway to verify the recipient is available via a secure connection. If the intended recipient is not a FedLink member or has an exemption, the email will be blocked, and the sender will be notified of the delivery failure and its cause.

Emails that are sent to another Federal Government agency or department are transmitted via our 'Fedlink' connection. FedLink provides secure communications between agencies across the public Internet at the UNCLASSIFIED with DLMs and higher security levels. To determine if an email recipient's organisation uses a secure email connection, please review FedLink members at http://www.fedlink.cybertrust.com.au/status.htm

All outbound emails with either no, or an incorrectly labelled, classification marking will be blocked at Comcare's email gateway. The sender will be notified of the delivery failure and its cause.

If you need to transfer personal, sensitive or information classified using DLMs to an organisation not on the Fedlink list contact the Technology Service Desk. Alternative secure communications can be made available such as our secure email link to ACT Government email addresses.

Comcare provides a Secure File Transport system that can facilitate the secure encrypted transfer of sensitive data outside of email. This is particularly useful for large files which exceed the email size limits.

Comcare staff must not misclassify emails in an attempt to circumvent any of the implemented blocking rules, and must contact the Technology Service Desk with any email classification issues they may have.

12.4 Filtering

Technology has implemented a number of email filters. These include, but are not limited to, filters for spam detection, virus detection and denial-of-service attacks.

Email filters require constant work to maintain accuracy, and some undesirable emails may still be received for example spam messages. If a breach occurs, staff must notify the Technology Service Desk within 24 hours.

12.5 Storage

All email traffic (inbound, outbound and internal) is logged and stored in compliance with the *Telecommunications (Interception and Access) Act 1979 (Cth)*

The primary purpose of the email storage process is to support business continuity. Storage allows for the restoration of data in the case of loss or corruption.

The secondary purpose of the email storage process is to support capacity planning and statistical reporting.

13 Remote / Mobile Computing

This section relates to the use of Comcare computing equipment not located on Comcare premises including privately owned computers that can be connected to the Comcare network.

Comcare has a Portable Device Policy that describes the procedures, standards, and guidelines around the use of mobile devices for work related purposes. Remote access connection will generally be restricted to SES, EL2 staff, approved home based staff or Mobile Workers.

Accessing the Comcare network using dial-up, broadband and mobile communications presents a number of security issues that need to be addressed to ensure adequate measures are in place to protect the integrity and confidentiality of data and computer systems.

Comcare staff may be required to apply software upgrades to Portable Computers as requested by Comcare's Technology Service Desk (e.g. updates to virus scanning software).

13.1 Connecting to the Comcare Network

Portable device computers will be supplied to authorised staff with a standard Comcare remote access installed. Staff will be able to connect to the Comcare computer network from remote locations and have access to most of the services available to staff located on Comcare premises.

All authorised Comcare staff will have access to electronic mail. Access to host based applications (e.g. PRACSYS, Finance 1, Aurion, file servers etc.) will only be available to staff specifically authorised to use those systems.

Some applications will not be accessible by remotely connected computers due to performance or technical reasons.

Remote access connection will be approved on the basis of demonstrated need and will generally be restricted to SES and EL2 staff, mobile workers and approved home based Comcare staff.

To apply for a remote access connection, Comcare staff must complete the Mobile Worker Requirements Form (located on the intranet on the Corporate Forms & Templates page), and forward it to the Technology Service Desk.

14 Comcare Wireless Network Access

Comcare has secure Wireless Networks (Wi-Fi) installed at all offices for use by staff and guests. Wi-Fi provides network access for portable devices such as laptops and tablets without the need to connect a network cable.

The wireless network is designed for using the internet through a browser such as Internet Explorer to access websites.

Use of a Comcare wireless network is subject to all relevant CEO Directions and Instructions, Comcare Security Policy and Technology policies.

14.1 Staff Access

Secure wireless network access is provided to staff that have been issued with a laptop.

14.2 Guest Access

Comcare provides secure guest wireless access in all offices to provide visiting clients, vendors, consultants, and others with Internet access. Access to Comcare's guest wireless networks is provided upon Director approval.

This service is offered as a convenience and is a way to make meetings or engagements as productive as possible with guests able to access email or websites during their visit.

Two options are available for obtaining guest wireless network access:

1) Access can be allocated on a guest by guest basis. A two day notice period is required before the service can be enabled.
2) Managers may apply for a guest access service to be created that they can issue to guests as they require. In this case, the guest access will be allocated to the relevant manager as the owner of the service. This will allow managers to have a working guest wireless service they can use without delay. In this case managers will be responsible for managing passwords.

To request guest wireless network access, staff must:

1) Login to the Comcare Technology Service Desk Portal;
2) Select:
    a. Log a Request;
    b. Service: Request
    c. Category: Guest wireless access
    d. Complete the information as requested
    e. Select: "Send E-mail to Director" button, once all mandatory information is entered.
3) Once submitted, the request will be automatically sent to your Director for approval. Once approved, the Technology Service Desk will enable wireless access.
4) The access is provided for a maximum period of 90 days. If the service is required for longer than 90 days, authorisation will have to be requested and approved again.

15 Internet Services

All Comcare staff is provided with access to the Internet. The Internet is used extensively to access information and conduct electronic transactions.

Comcare audits, monitors and logs all use, including personal use, of Comcare's Internet service.

Access to the Internet from within the Comcare network is filtered. Comcare staff must notify their supervisor if they inadvertently access any prohibited material.

15.1 Internet Filtering

Comcare implements Internet content filtering services designed to restrict access to prohibited material. However, the effectiveness of Comcare's filtering application may vary

and the fact a website is accessible does not imply that Comcare staff may access that site in circumstances where such access would constitute prohibited use.

Comcare's Internet filtering application may restrict access to useful Internet content. Where such restrictions are encountered, Comcare staff may seek approval for access to the relevant content from Comcare's Technology Service Desk.

If Comcare staff inadvertently access a website containing prohibited material, they must make a record of the date and time, leave the site and inform their supervisor. Comcare staff and their supervisors must pass site details to the Technology Service Desk for inclusion in Comcare's Internet filtering lists.

15.2 Social Media use in Comcare

Comcare permits staff to access selected social media websites. Comcare audits, monitors and logs all use, including personal use, of access to social media websites.

Comcare staff must report any suspicious contact of any form when using social media and the Internet to the Technology Service desk. For example, suspicious contact could be someone asking specific questions about your job or seeking information about Comcare.

At all times Comcare employees must ensure that they follow the APS Values and Code of Conduct. In addition, when using social media such as social networking sites or blogs, Comcare employees must ensure that they do not:

- speak on behalf of Comcare unless tasked to do so;
- undermine their effectiveness at work;
- be mindful of the direction for acceptable use;
- imply Comcare endorsement of personal views; and
- disclose confidential information obtained through work.

16 Procurement of Technology Resources

To ensure consistency and compatibility with Comcare's existing technology resources and services, all procurement must be arranged by Technology staff.

17 Security of Technology Resources

Comcare's Security Policy describes measures that Comcare will take to protect the confidentiality and integrity of information systems and data.

All staff must ensure that they understand their responsibilities with respect to Technology Security and promptly report any incidents to their supervisor and the Technology Service Desk.

User identification and passwords issued to authorised system users are key security components. They must not be disclosed to anyone else.

If inadvertent or unintentional disclosure of user identification or a password occurs, Comcare Staff must inform the Technology Service Desk immediately upon becoming aware of the disclosure.

17.1 Portable Devices

All Comcare owned portable technology resources must be registered on the Comcare Technology Asset Register. Comcare staff may be held responsible for any loss or damage to a

portable device that has been issued to them until it has been returned to the Technology Service Desk.

The Comcare staff member assigned to the portable device is ultimately held responsible for the return of any equipment that has been issued.

Comcare staff must ensure that any portable device issued to them is held in safe custody at all times. Staff must transport portable devices in carry-on baggage or secure them in checked baggage when travelling by air. Staff must not leave portable devices unattended, or in clear sight, when travelling by car.

Comcare staff must take reasonable care to ensure that non-Comcare personnel do not see or hear information stored, displayed or communicated using Portable Technology Resources. Staff must ensure that display devices are not visible by non-Comcare personnel while they are in use.

Where a portable device is lost or stolen, Comcare staff must:

- notify the Technology Service Desk immediately, to arrange cancellation of the service;
- notify any theft to the police and obtain a police report; and
- if sensitive information was stored on the Technology Resource, notify the ITSA and ASA through the Technology Service Desk.

Comcare laptops have been implemented with disk encryption software so that all data is encrypted when the laptop is powered off.

Comcare mobile devices have encryption to protect Comcare data stored on the device.

Comcare uses 'Good for Enterprise' to provide encrypted storage and communication of emails to authorised Smartphones and Tablets.

17.2 Security of Portable Storage Devices

Portable storage devices are items that can be used for short term storage and transfer of information. These devices can be connected to laptops, smartphones and tablet computers to enable information to be transferred. The portable storage devices referred to are:

- USB Flash Drive (secured and unsecured);
- Portable hard drive (secured and unsecured);
- Compact Disk (CD),Digital Video Disk (DVD) and Blu-Ray Disks (BD).

An authorised and approved Comcare portable storage device is to be used to transfer Comcare information.

Comcare portable storage devices must be configured so that information stored on the device is secured and encrypted in accordance with the Defence Signals Directorate Information Security Manual. This is a mandatory requirement particularly relevant to large amounts of data and more sensitive Comcare information. If assistance or more details are required, contact the Technology Service Desk.

Where possible, keep information on the Comcare network and securely transfer electronically rather than using a physical portable storage device.

Comcare physical security procedures are to be used when handling or storing a portable storage device that contains classified Comcare information. The Comcare Security Intranet site provides useful reference material.

17.3 Security of Communications

Comcare staff must not use portable technology resources to store or communicate information that is classified PROTECTED or above.