New Employee Induction

Treasury Policies Part 2 - Key Information and Communication Management and Technology Policies

This section of your induction covers some key policy matters that we want you to be aware of from your first day with us. As you read through the policies please pay particular attention to the areas outlined in the table below. Make note of any areas that you do not understand, so that you can seek clarification. You will be asked to verify that you have read and understood these policies on your first day of work. This activity is likely to take around 45 minutes.

Policy	Key areas to read
Information and Communication Management and Technology Policies	
1. Information and Communication Technology Security	You need to read the Policy, Policy Statement and Scope on page 1, plus the Employee Responsibilities and Definitions. Other Responsibility areas are to be read if they are relevant to your position. You need to be aware of the responsibilities that all employees have in relation to keeping information and ICT services and systems secure and preventing breaches of confidentiality and integrity of information.
2. Acceptable Use of Information and Communication Technology	Please read the entire document and ask questions if you are unsure about the contents. This policy outlines what is and is not acceptable use of ICT and important employee responsibilities in using ICT resources.
3. Use of email, internet and social media	Please read the entire document and ask questions if you are unsure about the contents. Covers what is appropriate and inappropriate use of these mediums. Make sure that you read the definition of 'misuse and inappropriate use' on page 4.
4. Information Management Records	You need to read the Policy, Policy Statement and Scope on page 1, plus the Employee Responsibilities (page 2) and Definitions (pages 5-7). Other Responsibility areas are to be read if they are relevant to your position. This policy sets out the requirement for all employees to secure and store information appropriately in both hard and soft copy.

ICT Security Policy

Identification

12/8343 - ICT Security Policy

Policy

This policy is part of the Department's Security Policy (TRIM Reference 12/35709*) and should be read and interpreted in that context. It sets out the Department's definition of, commitment to, and requirements for, Information and Communication Technology (ICT) security.

The objective of this policy is to:

- minimise the exposure of the Department to ICT related risk; and
- provide direction and support for ICT security management.

Policy Statement

The Department's ICT infrastructure, inclusive of all electronic information, shall be secured against breaches of confidentiality and integrity of information or interruptions to the availability of ICT services and systems.

Scope

ICT Security incorporates:

- Controlling access to ICT infrastructure;
- Protection of all Departmental electronic information;
- Security of all Departmental ICT systems; and
- Network security.

Separate Departmental policies cover security of Departmental records, ICT Disaster Recovery; ICT Change Management, ICT Asset Management, ICT Support and email, Internet and social media.

The policy applies at all times to all Departmental employees and contractors, on all Departmental sites, and to all cases where Departmental information that is not public information is taken offsite.

Responsibilities

Executive Committee

The Executive Committee is responsible for approving this policy and ensuring the policy is applied.

Director, Information Systems Branch (ISB)

Based on a security risk assessment, the Director ISB is accountable for approving:

- changes to ICT Infrastructure and development and deployment of new ICT Infrastructure.
- the direct or indirect connection of all ICT equipment to the Department's network.
- all remote access to the Department's internal ICT infrastructure.
- all mechanisms for the transfer of electronic information to and from external sources to the Department's internal ICT infrastructure.
- the severing of the Department's external network connections in the event of an identified security threat.
- physical access to the Department's ICT server rooms and ICT equipment and cabinets.
- storage of passwords electronically, following endorsement from the relevant Branch Head(s) and Business System Owner(s).
- software to be installed on Departmental assets.

The Director ISB is responsible for ensuring the following:

General security responsibilities

- the Department complies with the Tasmanian Government Security ICT Policies and Standards.
- A security risk assessment is performed at least annually as well as when changes are made to the Department's ICT Infrastructure and as new security threats are made public.
- information and education are provided to Departmental staff on how they can minimise ICT Security risks.
- automated alerts for ICT security breaches are in-place where practical and that any ICT alerts received are investigated by ISB in a timely manner.

Responsibilities for access to systems and data

- system level/root passwords are known only to authorised staff.
- archived media, including but not limited to backup media, are stored in a physically secure environment.
- access to websites identified by ISB as a security risk are blocked.
- where practical, there is appropriate segregation of system environments (test, production, training, etc) and internal and external systems.
- systems do not knowingly include undocumented or unauthorised mechanisms to access the data or application.
- where practical, dummy data is substituted for identifying fields in databases during application and system testing.

Device Responsibilities

- all Devices that connect to the Department's Network Domain:
  - have installed and are running current virus and anti-malware management software
  - only run software approved by the Director ISB
  - are patched for security based on a risk assessment approved by the Director ISB
- all PCs (including virtual PCs) are password protected and have a password protected screen saver that is enabled after 10 minutes of inactivity on the PC.
- user accounts are disabled from logging on to the Department's Network Domain after seven failed login attempts in a row.

Mobile Device Responsibilities

- all Mobile Devices managed by the Department (ie devices that run the Department's mobile device management software) have:
  - a minimum 4-digit passcode enabled
  - screen lock enabled after five minutes of inactivity
  - remote locate and wipe functionality enabled;
  - erase all data enabled after 10 unsuccessful logins;
  - an encrypted secure section to store non-public Departmental information; and
  - appropriate alerts raised if applications that are considered to be a security risk are installed on the device.
- ISB does not access or monitor personal information (eg photos and videos, shopping lists, documents, saved games) stored on a Mobile device.

Auditing and Monitoring Responsibilities

- system audit logs are retained and adequately secured.
- the usage of the Department's ICT infrastructure is appropriately monitored and available for the purposes investigating and ensuring compliance with the Department's security and ICT policies.
- the Department does have access to, record or audit staff personal information, settings or applications on a mobile device;

Physical Security Responsibilities

- physical access to ICT Infrastructure, including but not limited to network cabling, servers and storage must have appropriate physical security and environmental (e.g fire safety) controls in-place based on a risk assessment and comply with relevant legislation.

- all dedicated rooms for ICT Infrastructure must have physical access controls such as electronic or physical locks. Any access to ICT rooms must be approved by the Director ISB or their nominated delegate and an audit log of server room access must be maintained.
- all Departmental ICT devices, except mobile devices, must not be relocated or taken off-site without the approval of the Director ISB or their nominated delegate.
- storage media, including but not limited to disks, tapes and portable storage devices, that are sold, returned for warranty or otherwise allowed to leave the ownership and control of the Department are fully erased such that the data cannot be recovered or is rendered permanently unusable.

Corporate Management Group (CMG)

CMG members are responsible for:

- approving their staff[1] and contractors access to information in systems that they use to meet their business requirements and access to other Departmental ICT resources such as the Internet and email. Approval is to be based on a security risk assessment and performed in accordance with the *Personal Information Protection Act (2004)*.
- revoking the approval to access information in systems when access is no longer required or desirable.
- ensuring that their staff and contractors understand and comply with this policy.
- ensuring that, based on a security risk assessment, where necessary a written agreement is in place with any external party receiving or using Departmental data, setting out requirements for security of data while in use and destruction of data on completion.
- based on a security risk assessment, endorsing for the Director ISB approval their staff or contractors storing any passwords electronically.
- ensuring appropriate security procedures are in-place and adopted for any non-Treasury information systems used by their staff and contractors. This includes, but is not limited to, ensuring appropriate approval processes for accessing the systems.

Business System Owners

For the business systems they own, Business System Owners are responsible for:

- ensuring approved system access / revocation is appropriately applied, managed and regularly audited.

[1] This includes the access any staff on short-term or long-term leave should have to business systems, email and other ICT resources.

- ensuring where practical, dummy data is substituted for identifying fields in databases during application and system testing.
- As outlined in the Tasmanian Government Identity and Access Management Toolkit, ensuring that users of their systems are identifiable with appropriate levels of identity checks based on a security risk assessment.
- based on a security risk assessment, endorsing, for the Director ISB approval, staff storing any passwords electronically for the systems they own.
- ensuring system administrator passwords are known only to the relevant Business Unit System Administrator(s). This includes, but is not limited to ensuring that any system administrator passwords are changed when the system administrator leaves the role.
- ensuring that the system enforces password standards that are as close as practical to the Departmental Password Standards and for ensuring that education and procedures are in-place to achieve as close as practical to complete compliance with the Departmental Password Standards.

Business Unit System Administrators (BUSAs)

BUSAs are responsible for:

- only using their administrator logins for systems administration tasks and using their normal standard user login at all other times.
- reporting to ISB any unexpected activity which might pose an ICT security threat.

Employees

Employees are responsible for:

- understanding and adhering to the this policy and following ISB provided information and education to minimise the Department's ICT security risks.
- not sending confidential data unencrypted across the Internet (e.g by email or FTP), unless approved by the Branch Head on advice from the Director ISB.
- managing their passwords and not writing these down, sharing them, or storing them electronically (unless approved by the Director ISB), and not attempting to obtain or use another person's password.
- securing access to their computers before they leave their desktop computers unattended and turning off their PC(s) at the close of each business day.
- ensuring that if their mobile device has access to Departmental resources (e.g email or calendars) then their device is physically and electronically secure, including but not limited to the use of passcodes / passwords and virus protection.
- if their mobile device is configured to access Departmental resources (e.g email or calendars), contacting the ISB Service Desk immediately if their device is lost or stolen.

- not allowing sensitive or confidential information to be visible to unauthorised persons from their computer screens.
- only storing business information in Departmental systems (eg TRIM, TRACS, BMFRS, GLIS), server file shares (eg G: drive) or ISB provided or approved device. Unless approved in writing by the Director ISB, Departmental information that is not public must not be stored to any other media including but not limited to Departmental laptops, PC hard drives, personal devices, and Cloud / Internet based services (eg Dropbox).
- ensuring that the integrity and confidentiality of the information is maintained when undertaking work outside the Treasury environment.
- logging information security incidents through the Department's Information Security Incident system.
- not attempting to install or run software on Departmental ICT infrastructure unless approved by the Director ISB.
- reporting the loss of mobile devices, including USB devices, iPhones and iPads, and laptops immediately to ISB.
- notifying ISB immediately in the event of a virus being detected or of any suspected virus or ICT security threat.
- notifying ISB immediately of unexpected activity which might pose an ICT security threat.
- complying with the Departmental Password Standards where possible.

Definitions

Account	A combination of a username (identifier) and password allocated to an Authorised User to access ICT Services, Facilities and Infrastructure.
Authorised User	An individual who has been granted access to Department ICT infrastructure.
Business System	Software that supports one or more business processes (e.g. payroll or receipting).
Business System Owner	The position with the responsibility for managing a business system. Generally the business system owner is the relevant branch head.
Business Unit System Administrator (BUSA)	The position responsible for the day-to-day operation of a business system and for liaison with system users, ISB and external service providers. Generally the BUSA is a member of the Branch that uses the system.

ISB Provided and Managed Encrypted Devices	Any device provided and managed by ISB that encrypts the information on the device. Currently ISB provide and manage the following type of encrypted devices: encrypted USB Keys, iPhones (version 4 and above), and iPad (version 2 and above). Any devices that are not provided and managed by ISB, regardless of whether they are one of the above type of devices, are explicitly excluded from this definition and should not be used to store Departmental information that is not public .
Department's Network Domain	The computer network provided by the Department to access Treasury ICT resources.
Device	Any PC, server, mobile device, virtual PC, virtual server, appliance or other electronic device capable of accessing, storing and communicating data.
Encryption	The process of transforming information using an algorithm to render it unreadable to those without access to the encryption key.
ICT	Information and Communication Technologies. This is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services.
ICT Infrastructure	All ICT components supporting information interaction, storage, or communications and the ICT facilities on which they operate including all PCs, terminals, mobile computing devices, licences, centrally managed data, network connections, video conference rooms, and software owned or leased by the Department.
Mobile Device	A portable computing device such as a smartphone, laptop, or tablet computer.
Operating System	An operating system (OS) is a set of programs that manage computer hardware resources and provide common services for application software. The operating system is the most important type of system software in a computer system.
Departmental Password Standards	The Departmental Password Standards are as follows: - passwords are changed at least once every 90 days; - passwords are not the same as any of the previous 24 passwords or the username; - passwords are at least six characters in length; - passwords contain at least one character from three of the following four categories: o uppercase characters (A through Z); o lowercase characters (a through z); o numbers (0 through 9); and o non-alphabetic characters (for example - ! $ # %).

PC	A desktop workstation, laptop (including Virtual PCs)
Server	A device that provides or more such services to serve the needs of other devices or users.
Virtual PC or Server	One instance of an Operating System along with one or more applications running in an isolated partition of a device. It enables different operating systems to run in the same device at the same time as well as prevents applications from interfering with each other.

Legislative Framework

As listed in the Department's overarching Security Policy.

Related documents

Document	TRIM Ref
"Security Policy"	"12/35709"
" 201112 ICT Disaster Recovery and Business Continuity Policy"	"11/175887"
" 201112 IM Project Initiation Policy"	"11/175760"
" 201112 ICT Asset Management Policy"	"11/175731"
" 20120202 ICT Change Management Policy"	"12/11956"
" 20120202 ICT Support Policy"	"12/11962"
"201103 Use of email, internet and social media policy"	"11/13065"
"Clean Desk Policy"	"09/176761"
"Tasmanian Government Information Security Policy Manual CURRENT from November 2011"	"11/169484"
"200906 Identity and Access Management Toolkit Version 1.3 Final June 2009"	"D/40863/001"
"Tasmanian Government WAN and Internet Services Information Security Policies and Standards - V2.A - March 2009"	"12/40961"

Document acceptance and release notice

1. Build Status:

Version	Date	Author	Reason	Section
0.A	Feb 2012	Glenn Lewis	Initial Draft	
0.B	March 2012	Glenn Lewis	Amendments following ARMC review	
0.C	June 2014	Glenn Lewis	Added responsibilities for mobile devices.	
0.D	Jan 2015	Glenn Lewis	Updated mobile device responsibilities.	
0.D	May 2015	Glenn Lewis	Updated to incorporate physical security.	

Policy: Acceptable Use of Information and Communication Technology Policy

Identification

TRIM "12/158602" - "Acceptable Use of Information and Communication Technology Policy"

Policy

The Department provides Users with ICT resources to support work related tasks and has a responsibility to ensure that usage is appropriate and complies with all legislative requirements. This Policy should be read in conjunction with the State Service Code of Conduct (*State Service Act 2000*) and the *State Service Regulations 2001* which provide overarching responsibilities. This Policy is also underpinned by the separate ICT Security Policy and the Department's use of Internet, Email and Social Media Policy and Guidelines (refer to the Related Documents section of this Policy).

Policy Statement

Departmental ICT Resources and the services accessible on them are provided to Users to carry out tasks related to their job.

Personal use of Departmental ICT Resources must not result in loss of productivity, added costs to government, disruption to IT systems or harm to the Government's reputation.

Use of Departmental ICT Resources must be appropriate, and not jeopardise the integrity, security or service levels of the Department, nor harm the reputation of the Public Service and the Departmental, its employees, workplace, clients and stakeholders.

Use of Departmental ICT Resources must comply with any codes of conduct, ministerial directives or legislative requirements which apply to the User.

Scope

The Policy applies to all Departmental employees and contractors using Departmental ICT Resources at all times, irrespective of physical location.

Responsibilities

Employee & Contractor ("User") Responsibilities

- Users are responsible and accountable for their own usage of ICT resources;
- Users shall not deliberately damage or tamper with physical ICT equipment;
- Users must not exceed Reasonable Personal Use (refer to the Definitions section);
- Users who use Departmental ICT Resources for Reasonable Personal Use must not create or cause any loss of productivity, added costs to government, disruption to IT systems or harm to the Government's reputation;
- Users must not save or install personal software or any other form of software on Departmental ICT Resources without formal approval from the Director ISB;

- Users must not install Departmental software on private ICT resources without formal approval from the Director ISB;
- Users must not utilise Departmental printers for private printing purposes, apart from Reasonable Personal Use;
- Users must not use Departmental ICT Resources to gain unauthorised access to internal or external ICT systems;
- Users must be aware that their use of Departmental ICT Resources may be monitored;
- Users must abide by the Department's ICT Security Policy and Internet and Email Use Guidelines; and
- Users must be aware that if they are using their own mobile device (phone, tablet, etc) they are responsible for the configuration and setup of the device including but not limited to its physical and information security. The Department is in no way liable for the IT support, repair or replacement of a user's personal device.

Director, Information Systems Branch Responsibilities

- Monitor and report usage of Departmental ICT Resources to the Director Corporate Support, on an as-needed basis;
- Approve installation of Departmental software on private ICT resources; and
- Approve installation of software on Departmental ICT resources.

Secretary

- Investigate complaints about, and recommend an appropriate course of action, following the misuse of Departmental ICT resources.
- Has delegated discretion to determine if a failure to comply with this Policy has occurred inadvertently.
- Approve access to, and searching of, a staff email account (including approval of forwarding of some or all new incoming emails to an alternate email account).

Branch Head Responsibilities

- Advise the Director CSD if they, or their staff, have observed inappropriate usage of Departmental ICT resources in breach of this Policy; and
- Undertake regular monitoring to ensure that their staff comply with Reasonable Personal Use of Departmental ICT resources.

Definitions

Departmental ICT Resource	All electronic equipment and associated information systems and services funded and/or provided by the Department.

Reasonable Personal Use	ICT resources may be used for incidental amounts of personal, educational and recreational use. Use must not result in loss of productivity, added costs to government, disruption to IT systems, or harm to the Government's reputation.
User	Any employee or contractor approved by the Department to use Departmental ICT resources.

Legislative framework

All legislation is Tasmanian unless otherwise stated.

Anti-Discrimination Act 1998: Prohibits discrimination and other specified conduct and provides for the investigation and conciliation of, and inquiry into, complaints in relation to such discrimination and conduct.

Criminal Code Act 1924: Criminal activity, including fraud, certain types of inappropriate or pornographic material.

Ministerial Direction No 10: Internet and Email use by State Service Officers and Employees: Provides a framework for government policy and clarity in relation to the appropriate use of Internet and email facilities.

Personal Information Protection Act 2004: Legislation to provide for the management of personal information collected by agencies.

Public Interest Disclosures Act 2002: Encourages and facilitates disclosures of improper conduct by public officers and public bodies, to protect persons making those disclosures and others from reprisals, to provide for the matters disclosed to be properly investigated and dealt with and for other purposes.

State Service Act 2000: The State Service Principles of the State Service Act require the State Service to be accountable for its actions and performance [s7(1)(d)]. Heads of Agencies must uphold, promote and comply with the State Service Principles [s8].

State Service Code of Conduct: establishes standards of behaviour and conduct that apply to all employees, including officers and Heads of Agency.

Related documents

Document	**Reference**
ICT Security Policy	TRIM "12/8343"
Use of email, internet and social media	TRIM 12/199121[v3]
Guideline: Use of email, internet and social media guidelines	TRIM 13/27146[v2]
Clean Desk Policy	TRIM "09/176761"

Document acceptance and release notice

Build Status:

Version	Date	Author	Reason	Section
0.1	Sept 2012	ISB	Initial Draft	
0.2	Dec 2012	ISB	Revised draft following stakeholder consultation	
0.3	June 2014	ISB	Updated the link to the Department's current email Internet and Social media policy and guidleines and added the mobile device responsibility.	
0.4	July 2015	ISB	Updated to change the Director Corporate Support responsibilities to the Secretary and to explicitly state approvals required for email searching.	

Amendments in this release:

Section title	Section number	Amendment summary

Distribution

Version	Issue date	Issued to
0.2	21/1/13	Executive Committee

Policy: Use of email, internet and social media

Identification

TRIM 12/199121[3]

Policy

To set out the appropriate and reasonable use of email, the internet and social media for employees, volunteers and others associated with Treasury.

Policy Statement

Use of email, the internet and social media, must be appropriate, and not jeopardise the integrity, security or service levels of the Department, nor harm the reputation of the Government, State Service and the Department, its employees, workplace, clients and stakeholders. Any comments on official information must follow the Department's *Guidelines for disclosure of official information* ref: 09/161981*.

The basis of this policy is *Employment Direction no 12: 2003 Internet and email use by state servant officers and employees* and the other legislation, policies and guidelines detailed in this policy.

Scope

This document sets out the policy for employees' and volunteers' use of email, the internet and social media, whether for official or private purposes when acting as an employee or representative of the Department or State Service. The policy applies at all times. There are consequences and sanctions for misuse.

Employees' and volunteers' use of email, the internet and social media is subject to the same legislation, policies and guidelines as participation in any other media, public forum or engagement with the community. This includes comments made by an employee or volunteer using email, the internet and social media.

Responsibilities

Employees and volunteers must be aware that:

- internet and email records are "discoverable" in any court of law - that is, a party to a legal action can compel their production as evidence in the proceedings; and they would be examined and, if relevant, used as evidence in respect of any breach of the State Service Code of Conduct, not just action taken in respect of any breach of the policy and/or the Employment Direction;
- the State Service Code of Conduct defines standards of behaviour and conduct that apply to all employees. Use of email, the internet and social media must be in accordance with Section 9 of the State Service Code of Conduct and *Employment Direction no 12: 2003 Internet and Email Use by State Servant Officers and Employees*, as detailed in the Legislative Framework section of this Policy;

- the responsibility for employees or volunteers making public statements is defined by Regulation 11 of the *State Service Regulations 2001* as detailed in the Legislative Framework section of this policy;
- they are accountable for their private actions that may have a bearing on the Department, State Service or their standing as a public official;
- they are responsible for all email sent and received by their Departmental email account and for the nature of the content they view on internet sites and social media; and
- their use of email, the internet or social media may be monitored or accessed in response to a complaint or investigation. This includes reading the content of files and emails stored on Departmental systems, including those emails deleted from an email inbox, and viewing an employee or volunteer's internet usage.

Employees and volunteers must:

- not misuse (see definitions) email, the internet or social media;
- be responsible and accountable for their own usage of email, the internet or social media, including maintaining awareness of the relevant policy provisions that apply;
- not exceed Reasonable Personal Use of email, the internet or social media (see definitions);
- not create or cause any loss of productivity, added costs to government, disruption to IT systems or harm to the Government's reputation;
- advise their supervisor or manager if they:
    - have emailed information to unintended recipients where this may have the potential to harm the Department or government's reputation; and
    - notice inappropriate or unlawful content relating to the Department or content that may otherwise have been published in breach of this Policy.
- comply with Departmental policies and approvals processes when they publish any information relating to the Department; and
- be aware of information security when they access Treasury information remotely. The Department gives them the ability to access email, and other information resources, when they are away from the workplace. However, there is no expectation that they will need to do this. If they access information, including email remotely, they are responsible for the security of the information they access. It is recommended that they:
    - only access email remotely from a PC (or other device) that is trusted and has up-to-date anti-virus software;
    - take care to ensure that no-one can see their username and password being entered or read the information being accessed; and
    - ensure that they have logged off before leaving the PC (or other device) or that the device is locked with appropriate password or pin protection.

All employees and volunteers will be made aware of their obligations under this policy by the officer who engages them through the relevant induction process. Any breach of this policy may result in early termination of engagement.

Deputy Secretary, Corporate and Governance Division Responsibilities

- Ensure that users of Departmental email, the internet or social media are made aware of this policy.
- Investigate complaints about or alleged misuse of email, the internet or social media, to recommend an appropriate course of action.
- Approve access to Departmental personal information stores, including email and internet use, in response to a complaint or investigation, or if it is suspected that misuse has occurred.

Corporate Management Group Responsibilities

- Promote awareness of this policy and manage the reasonable personal use of their employees' and volunteers' Departmental email, the internet or social media.
- Advise the Director CGD if they, or their employees or volunteers, have observed inappropriate or unlawful use of email, the internet or social media in breach of this Policy.
- Manage their employees' and volunteers' compliance with reasonable personal use of Departmental email, the internet or social media.

Head of Agency responsibilities

The Head of Agency, or delegate, has the discretion to determine if a breach of this policy has occurred and the appropriate course of action as a result of the breach.

Sanction for misuse of email, the internet or social media

Sanctions for misuse of email, the internet or social media will vary depending on the nature and seriousness of the incident. The Head of Agency, or delegate, will determine the appropriate action.

(a) Where misuse may constitute a contravention of law in Tasmania, evidence should be provided to the relevant external authority. Internal action under the State *Service Act 2000* may also be taken in accordance with (b).

(b) Where misuse may constitute a breach of the Code of Conduct (Section 9 of the *State Service Act 2000*), any action taken must be in accordance with *Employment Direction No. 5 – Procedures for the Investigation and Determination of whether an Employee has breached the Code of Conduct.*

(c) Where the nature or the seriousness of the misuse is not considered to be a breach of the Code of Conduct, action may be taken in accordance with the Department's Managing Unsatisfactory Performance Guidelines.

Definitions

Email inboxes	Includes emails that employees or volunteers have sent or received, network back-ups and archives that may contain copies of emails that have been deleted.
Employee	A person employed by the Department under a contract of employment.
Inappropriate Use	Refer to the definition below for **misuse and inappropriate** use.
Misuse and inappropriate use	**Misuse and inappropriate use** of email, the internet and social media includes, but is not limited to: • jeopardising the integrity, security or service levels of the Department or harming the reputation of the State Service and/or the Department, its employees, workplace, clients and/or stakeholders. • initiating or perpetuating violence or intimidation of others, either inside or outside the workplace. Treasury is a White Ribbon workplace and has a zero tolerance towards violence against women. • using email, the internet and social media for communicating or publishing defamatory comments or disclosing inappropriate information about the Department and/or its employees, workplace, clients and stakeholders. • downloading, storing or transmitting excessive information for personal use or otherwise using facilities to the detriment of the Department’s efficient operation. • accessing, displaying or transmitting pornographic, obscene, or other objectionable material including adult only or violence-related content. • initiating or forwarding material that may be considered offensive, defamatory, disparaging, threatening, discriminatory, hateful, bullying or harassing to others, this includes material that objectifies or belittles women. • the distribution of hoaxes, chain letters, or advertisements. • downloading from, transmission over or publishing on the internet, social media or via email, material which is in breach of copyright. • the use of email, the internet and social media for personal financial gain, including gambling. • undertaking personal commercial activities using Departmental facilities that exceed reasonable personal use. • gaining unauthorised access to other systems. • downloading and/or installing unlicensed software without appropriate departmental approval. • using facilities for the initiation and/or distribution of unauthorised and

	unsolicited information of a political, sensitive or commercial-in-confidence nature to others. • unwarranted or unauthorised access, duplication, or distribution of client, staff, or departmental information or records. • forging or misrepresentation of identity using electronic facilities. • compromising the privacy of others. • representing personal opinions as those of the Department. While some uses of electronic facilities including email, internet and social media facilities are not illegal (eg downloading and viewing some types of pornographic material) they are inconsistent with community expectations of State Service officers and employees or volunteers and are not considered an appropriate use of government resources.
Departmental Information	Information that relates to the business activities of the Department in any media, i.e. paper or electronic. This includes all information that we produce and that comes into the Department including from Cabinet, Ministerial Offices, federal government, clients and stakeholders.
Official or private use	Whether using Departmental email, the internet and social media, for official or private purposes, employees and volunteers are reminded that comments will often be permanently available and able to be reproduced in other media. The definition of official and private use is as follows: • official use: using email, the internet and social media when acting as an employee of, or volunteer to, the Department or State Service of Tasmania. • private use: using email, the internet and social media in a private capacity.
Personal information stores	Personal information relates to private or personal matter and has no relevance to the business activities of the Department. The Department allows for the storage of "minor amounts of personal information" for occasional private, educational and recreational use. Personal use must not result in added costs to the Department, disruption to Information Technology systems or harm the Department's reputation. (Information Management Records Policy 07/7958*).
Reasonable personal use	Email, the internet and social media may be used for incidental amounts of personal, educational and recreational use during lunch breaks, time-off or outside normal working hours. Use must not result in loss of productivity, added costs to government, disruption to IT systems, or harm to the Department or Government's reputation.
Social media	Describes the internet based tools used for publishing, sharing and discussing information. Social media includes blogs, wikis, file-sharing, user generated video and audio, crowd sourcing, virtual worlds and social networking sites. Popular social media sites include Facebook, Twitter,

	YouTube, LinkedIn, Wikipedia, Skype, dating sites, virtual games and virtual social worlds.
User	Any employee, contractor or volunteer approved by the Department to use Departmental email, the internet and social media.

Legislative framework

Employees' contractors' and volunteers' use of email, the internet and social media is subject to the same legislation, policies and guidelines as participation in any other media, public forum or engagement with the community. This includes comments made by an employee, contractor or volunteer using email, the internet and social media.

The list of legislation below is not exhaustive but indicates the type and range of legislation relevant to the use of email, the internet and social media. All legislation is Tasmanian unless otherwise stated.

Anti-Discrimination Act 1998: Prohibits discrimination and other specified conduct and provides for the investigation and conciliation of, and inquiry into, complaints in relation to such discrimination and conduct.

Criminal Code Act 1924: Criminal activity, including fraud, certain types of inappropriate or pornographic material.

Employment Direction No 12: Internet and Email use by State Service Officers and Employees: Provides a framework for government policy and clarity in relation to the appropriate use of internet and email facilities.

Employment Direction No 28: Family Violence – Workplace Arrangements and Requirements.

Personal Information Protection Act 2004: Legislation to provide for the management of personal information collected by agencies.

Public Interest Disclosures Act 2002: Encourages and facilitates disclosures of improper conduct by public officers and public bodies, to protect persons making those disclosures and others from reprisals, to provide for the matters disclosed to be properly investigated and dealt with and for other purposes.

State Service Act 2000: The State Service Principles of the State Service Act require the State Service to be accountable for its actions and performance [s7(1)(d)]. Heads of Agencies must uphold, promote and comply with the State Service Principles [s8].

State Service Code of Conduct: establishes standards of behaviour and conduct that apply to all employees, including officers and Heads of Agency.

All employees should be aware of their responsibilities under the State Service Code of Conduct (*State Service Act 2000*). This policy is based on section 9 where employees must:

- (3) treat everyone with respect and without harassment, victimisation or discrimination;
- (4) comply with all applicable Australian law;
- (7) maintain appropriate confidentiality about dealings of, and information acquired by them in the course of their employment;
- (9) use Tasmanian Government resources in a proper manner;

- (10) not knowingly providing false or misleading information in connection with their employment;
- (11) not make improper use of information gained in the course of their employment;
- (13) behave in a way that upholds the State Service Principles in particular that the State Service is apolitical, performing its functions in an impartial, ethical and professional manner; and
- (14) at all times behave in a way that does not adversely affect the integrity and good reputation of the State Service.

State Service Regulations 2001. Regulation 11, public statements by officers and employees

Regulation 11 advises the following:

> An officer or employee is not, without the permission of the Minister administering the Agency in which the officer or employee is employed, to make any communication or contribution, directly or indirectly, anonymously or otherwise, on any matter affecting the Agency in which the officer or employee is employed, or the functions or duties of the officer or employee, to any newspaper or publication of a like nature other than –
>
> a) in the case of an officer or employee who is a member of a professional health organisation, a journal or publication relating to or relevant to the profession of that officer or employee; or
>
> b) in the case of an officer or employee who is a member of an employee organisation, a journal or publication issued by or under the authority of that employee organisation.

SPAM Act 2003 (Commonwealth): Prohibits spam (unsolicited commercial electronic messaging) in Australia.

Related documents

Document	**TRIM Ref**
Guideline for the use of email, internet and social media	13/27146*
Acceptable use of Information and Communication Technology Policy	12/158602*
Security Policy	12/8343*
Clean Desk Policy	09/176761*
Guidelines for the disclosure of official information	09/161981*
Procedures: Responding to requests for information	08/188426*
Information Management Records Policy	07/7958*
Copyright Policy	09/180515*
Promoting and Managing Respectful Workplace Behaviour Policy	16/36507*

Contacts

Manager, Corporate Information and Communication

Manager, Human Resources

Document acceptance and release notice

Build Status:

Version	Date	Author	Reason	Section
[v3]	April 2016	Joy Crane	Policy changes to align with White Ribbon accreditation	Misuse and Inappropriate Use Legislation and Policy
[v2]	5 Dec 2013	Lynne Valentine	Policy changes requested by the Secretary and Exec.	Scope CMG Responsibilities
[v1]	May 2013	Lynne Valentine	Update the use of email and internet guideline to include social media and use the new policy template.	All

Amendments in this release:

Section title	Amendment summary
Misuse and Inappropriate Use	Include reference to inappropriate behaviour in relation to initiating or perpetuating violence in context of White Ribbon and Treasury's zero tolerance towards violence against women.
Legislation	To include reference to Employment Direction No 28.
Policy	To include reference to Treasury's Promoting and Managing Respectful Workplace Behaviour Policy.
Job Titles	Update of job titles referred to in the policy.

Distribution

Version	Issue date	Issued to
[v3]	April 16	All staff through their Branch Heads using Issues for Branch Discussion.
[v2]	December 13	All staff through their Branch Heads using Issues for Branch Discussion.
	15 Nov 13	Secretary for approval
[v1]	28 June 13	All staff for consultation
	13 May 13	Executive Committee for approval

Policy: Information Management Records Policy

Identification

Information Management Records Policy - ref 07/7958[12]
Current from 8 August 2014

Policy

Records must be created, captured, maintained, shared, secured and disposed of in a manner that complies with the Department's legal, administrative, operational and cultural requirements.

Policy statement

Information is a key resource for the Department that enables sound decision making, the development of well-targeted evidence-based policies, and the delivery of high quality services. In order to meet these objectives, we need to share information across the organisation so that we can:

- improve our evidence base to support policy development;
- break down the information and knowledge barriers across the Department;
- identify staff that have knowledge of the topic we are working on so that we can collaborate with them, and share ideas and corporate memory; and
- improve productivity by reducing security restrictions and duplication.

This policy is part of the Department's Security Policy - ref 12/35709* and is informed by the Tasmanian Government Information Security Policy - ref D/36629/003.

The Department must maintain appropriate custody of records on behalf of the Crown until dealt with in accordance with the *Archives Act 1983*.

All employees who create, manage and handle departmental information must comply with the *Archives Act 1983*, relevant legislative requirements and departmental policies including that they identify and capture all business records.

The Department of Treasury and Finance operates a clean desk policy where outside core work hours:

- desks must be cleared and office doors must be locked; and
- Departmental information that is not public information must be locked in desk drawers or filing cabinets provided for this purpose and secured when used off site.

Scope

This policy sets out the requirements to manage and share departmental information, regardless of the system they are stored in or their format including in approved departmental databases.

This policy applies to all employees and contractors at all times and wherever they are.

Access to all departmental information including approved departmental databases is given to employees with a need-to-know.

Failure to comply with this policy may result in a breach of the State Service Code of Conduct and action under Section 10 of the *State Service Act 2000*. This policy may be used where an employee is under investigation for a criminal or civil offence, or any other breach.

Information Security Classification

We classify information depending on the risk and consequences to the Department if the information is compromised. We handle information according to its classification using the Records handling procedure Ref: 13/9408*.

The default information security classification for all departmental information is X-IN-CONFIDENCE. Staff have access to all information unless it is classified as PROTECTED or HIGHLY PROTECTED, or statutory restrictions apply eg taxpayer information.

Responsibilities

Employee responsibilities

- Comply with departmental information management policies and procedures, and legislative requirements that are relevant to your position/s.
- Identify business records and create, capture, register and retain records to support your business activities.
- Report information security breaches.
- Do not disclose information about individuals whose information you have access to or invade their privacy.
- Understand that all records may be subject to "discovery", including drafts and revisions. This includes Right to Information, Parliamentary enquiry, audit, Ministerial or Ombudsman requests, or a legal discovery order.
- Use the:
  - Records handling procedures to handle information - ref 13/19408*. This includes the need to not leave departmental information that is not public information unsecured at any time; and
  - TRIM Managing Electronic Records and Emails procedure to store information in TRIM - ref 07/8002*.

Assistant Directors responsibilities

- If delegated by their Branch or Division Head, approve access to information that is legislated, classified as PROTECTED or HIGHLY PROTECTED, or restricted in their area of responsibility.

Corporate Management Group (CMG) responsibilities

RESPONSIBILITY AND RESOURCING

- Approve access to information that is classified as PROTECTED or HIGHLY PROTECTED in their area of responsibility, unless statutory restrictions apply. Delegate this responsibility to Assistant Directors if appropriate.
- Make sure that their staff are aware of, and comply with, this policy.
- Make sure that adequate records of business activities are managed, destroyed and retained in accordance with the *Archives Act 1983*.
- Provide adequate resources to maintain departmental records.

COMPLIANCE

- Comply with departmental information management policies and procedures and relevant legislative requirements to maintain business records relating to the activity of your area of responsibility. Conduct regular clean desk policy checks to verify compliance.

- Manage the disposal, security and accessibility of your departmental records. Use a risk-based approach to determine the identity, access management and information security classifications for your Departmental services and information assets using the procedure ref 12/87916*.
- Insert standard clauses into contracts allowing for the proper management and accountability of records created by contractors.

Executive Committee responsibilities

- Review and monitor this policy.
- Ensure this policy complies with relevant legislation and regulations.

Director, Corporate Support responsibilities

- Approve access to:
  - an employee's personal information stores, including email and iSpace in the course of a complaint or investigation of that employee.
  - TRIM for non-departmental employees or contractors in exceptional circumstances.

Chair of Departmental Committees responsibilities

- Ensure that the Executive Officer follows record keeping procedures for committees.
- Review and maintain the list of committee members in TRIM and email.

Information Services responsibilities

In accordance with the Department's legislative requirements, Information Services:

- deliver effective and efficient information support services for hard copy and electronic records in TRIM;
- provide advice and develop policies and procedures to manage hard copy and electronic records;
- work with Branches and the Tasmanian Archives and Heritage Office to develop and maintain the Department's:
  - Business Classification Scheme including approved acronyms and abbreviations; and
  - Disposal Schedules for the time period that information should be kept for depending on the value of the information.

Information Systems Branch responsibilities

Provide application support and maintain approved departmental databases and/or liaise with third party support providers.

Contractors

Contractors are responsible for their contractual obligations for recordkeeping.

Definitions

The definitions of departmental information, records are detailed first and then followed by an A-Z list.

Departmental information

Information that relates to the business activities of the Department in any media, ie paper or electronic. This includes all information that we produce and that comes into the Department including Cabinet, Ministerial Offices, federal government, clients and stakeholders.

RECORDS

A record is any departmental information that is: “created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.” [1]

Records:

- have ongoing use as a means of accountability, operational continuity, legal evidence and are all subject to Right to Information (RTI), Parliamentary, Ministerial and Ombudsman requests, and legal discovery orders, including drafts and revisions;
- contain the memory of the Department’s decision-making and may be in hardcopy or electronic format;
- are classified depending on the level of importance to the Department. Any record may move from one category of importance to another over time due to a change in circumstances; and
- including personal information, are “discoverable” in any court of law. A party to a legal action can compel their production as evidence in the proceedings.

For records managed by Information Services through TRIM: Before TRIM was implemented in 2007-08 the record was the hardcopy record placed on file. After implementation, the electronic record, including verified scanned images will be considered the record.

There are three types of records:

- business records
- short-term records; and
- personal information that is not classified as a Departmental record.

Business records – all systems and information assets

Information that relates to the business activities of the Department and which must be retained as a record.

Business records:

- may explain or justify what has been done, illustrate the extent of individual or group responsibility for decisions taken, illustrate the order of events and the Department’s role. Depending on security requirements, these records should be readily accessible by those who have a need-to-know.
- document business activities and include information created or received by the Department. They may record the substantive activities and policies of the Department. Business records include information that is required for use by others, or affect the work of others.

[1] Source: Australian Standards (AS ISO 15489.1)

- are stored in approved departmental databases including CHRIS for human resource administration data such as pay and leave, GLIS for gaming and licensing, TRO for administering taxpayer data, BMFRS and Finance1 for budget and finance, TRIM for managing business records, and websites. Business system information only needs to be stored in TRIM if it provides supporting evidence for a business transaction or is a snapshot at a point in time that cannot be reproduced by the originating application.

Business records include:

- HR employee records in the CHRIS system, financial reporting information in Finance1, and taxpayer information in TRO;
- any material reflecting the substantive activities of the Department;
- periodic and final versions of reports;
- policy documents, procedures, guidelines and manuals for business operations and systems;
- information that is required for evidentiary purposes;
- systems specifications and technical documentation, and systems change management requests and issues reports;
- formal communications between employees, departments, organisations, clients, taxpayers or constituents;
- formal minutes of committees;
- file notes documenting actions, decisions or significant conversations;
- PMIs; and
- project documents.

Short-term records
Records that are used to facilitate departmental activity but are of little importance and do not support or contribute to the business activities of the Department.

Short-term records include records which duplicate or extract information already held elsewhere or have little or no business, fiscal, evidential, cultural, or known historical value. Short-term records can be destroyed when all business needs to refer to the records have ceased.

Examples include:

- drafts and working papers;
- temporary data files created in order to manipulate or transfer systems information, and systems testing information;
- documents received from outside the Department that are kept for reference including promotional material, invitations, price lists, catalogues, and external publications;
- internal documents kept solely for reference including drafts, duplicates of internal circulars, duplicates of departmental publications or copies of other records held elsewhere in the Department;
- documents used in the preparation of other records including working papers, background notes and reference material that does not relate to policy development or significant projects;
- documents containing personal information and copies of personal documents acquired by the Department, which are not required on a continuing basis to support the activities to which they relate;
- records documenting informal communications, for example emails sent instead of a

phone call, cover notes, recorded phone messages or email subscription messages, and invitations to attend a function in an official capacity;

- personal notes on the status of current work;
- records documenting requests for, and the provision of, information that is readily available to the public or authorised for unlimited public access, including promotional material, publications, annual reports and routine information; and
- appointment timetables including diaries, schedules and calendars that do not contain records. These records may be kept permanently for employees that have held prominent positions in the Department.

Short-term records:

- may be kept in business systems or registered in TRIM to help achieve business outcomes and efficiencies; and
- are subject to discovery, including drafts and revisions. This includes a Right to Information, Parliamentary enquiry, audit, Ministerial or Ombudsman request, or a legal discovery order.

Personal information

Personal information that relates to private or personal matter has no relevance to the business activities of the Department.

The Department allows for the storage of 'minor amounts of personal information' for occasional private, educational and recreational use. Personal use must not result in added costs to the Department, disruption to Information Technology systems or harm the Department's reputation. Examples include:

- information related to personal interests/development;
- personal communications; and
- résumés.

Personal information may be stored in an employee's iSpace in TRIM but should not be placed on departmental files or server drives. Business records must not be stored in an employee's iSpace for example draft business records, flex sheets and PMIs.

The Department does not accept any responsibility for the integrity or longevity of information stored in iSpace or other personal information stores. iSpace will be deleted 10 days after an employee leaves the Department.

Personal information stores for complaints or investigation

Personal information and audit logs, if reviewed and found to be relevant, may be used as evidence by the appropriate authorities, where an employee is under investigation for:

- a criminal or civil offence; and/or
- respect of any breach, or suspected breach, of the Code of Conduct and/or Employment Direction.

INFORMATION SECURITY CLASSIFICATION

The Tasmanian Government Information Security Policy outlines a standard set of information security classification definitions, markings and procedures that provide appropriate access to, and handling of, our information. These classifications aim to reduce the risk associated with transfer of information within and between Tasmanian Government agencies or information coming into or leaving agencies. Information is assessed using a risk-based approach and classified as PUBLIC, UNCLASSIFIED, X-IN-CONFIDENCE, PROTECTED and HIGHLY PROTECTED.

PUBLIC

Information that is clearly and self-evidently publicly available and has been authorised by the owner/custodian for public access and circulation, examples include: books, magazines and other publications including Treasury publications such as published Budget Papers.

UNCLASSIFIED

Information that may need to be protected and controlled and is not to be considered PUBLIC information. Official information needs to be specifically classified as PUBLIC before it is released into the public domain.

X-IN-CONFIDENCE

Information that if compromised could cause limited damage to the State, the Government, commercial entities or members of the public. As a minimum, requires a low level of confidence in the identity of the individual accessing the information. Examples are STAFF-IN-CONFIDENCE and COMMERCIAL-IN-CONFIDENCE.

Restricted information: X-IN-CONFIDENCE information is open to all Treasury employees unless statutory restrictions apply eg taxpayer information. Branch Heads can restrict X-IN-CONFIDENCE files. Examples include:

- PMIs, flex time and general staffing issues;
- Branch staffing and budget files contain working, temporary and duplicate information. They are restricted to the Branch and the Branch Head may restrict further if needed; and
- Tender files are restricted to the evaluation panel members and Branch Directorate when working through the tender process. Most tenders can be open to all staff once the tender contract is awarded. Branch Heads to approve restricted or PROTECTED files on case-by-case basis depending on the risk of the information being compromised.

PROTECTED

Information that if compromised could cause damage to the State, the Government, commercial entities or members of the public. As a minimum, requires a moderate level of confidence in the identity of the individual accessing the information. This includes CABINET-IN-CONFIDENCE.

HIGHLY PROTECTED

Information that requires a substantial degree of protection as compromise of the information could cause serious damage to the State, the Government, commercial entities or members of the public. As a minimum, requires a high level of confidence in the identity of the individual accessing the information.

Other definitions

Approved departmental databases

The Department maintains a range of databases to support the storage, access, workflow and usage of data. This includes but is not limited to: human resource administration data such as pay and leave; gaming, licensing and taxpayer data; budget and finance systems; registers; and websites.

The relevant databases are identified in the ISB Information Management ICT policies. All departmental databases must be approved by, and supported by or through, the Information Systems Branch.

Business Classification Scheme

Records are stored in the Department's Business Classification Scheme (BCS) which is a hierarchical list of terms that defines the Department's business functions, activities and transactions.

Contractor

A person engaged by any person (otherwise than as an employee) to perform work for gain or reward.

Core work hours

Core work hours are from 8.45 am to 5.06 pm.

Classified information

Information that requires protection from unauthorised disclosure[2].

Departmental information

Information that relates to the business activities of the Department in any media, ie paper or electronic. This includes all information that we produce and the information that comes into the Department including Cabinet, Ministerial Offices, federal government, clients and stakeholders.

Discovery

All records may be subject to discovery including drafts and revisions. This includes Right to Information, Parliamentary enquiry, audit, Ministerial or Ombudsman requests. Records are "discoverable" in any court of law as evidence in the proceedings; and they would be examined and, if relevant, used as evidence in respect of any breach of the State Service Code of Conduct, not just action taken in respect of any breach of the guideline and/or an Employment Direction.

Disposal

The *Archives Act 1983* stipulates that no government employee, or any other person, may dispose of records of any type without the written authority of the State Archivist. We facilitate this through our Disposal Schedule and a range of processes relating to records retention, destruction or transfer to the Archives Office. These have been developed in accordance with the *Archives Act 1983* and apply to all departmental information.

Disposal Schedule

An authorisation from the State Archivist that specifies the minimum time the Department is required to keep records and their destruction or transfer.

Employee

A person employed by the Department under a contract of employment.

[2] Definition from the Australian Government Information Security Manual (ISM) produced by the Defence Signals Directorate (DSD).

Information assets

Information assets: all assets in or on which information is stored and include, but are not limited to information/data, computer hardware, personnel, software; and physical equipment.

Information/data assets: include, but are not limited to:

- hardcopy files: whether or not centrally stored files;
- documents: including plans, manuals, whether or not on centrally stored files;
- applications databases including records contained in TRIM and on network or local drives;
- emails stored on computers;
- firmware: floppy discs, CD Read Only Memories, Programmable ROMs;
- reference material: including library;
- websites including tresNet.

iSpace in TRIM

iSpace in TRIM is used for the storage of personal information and is secured to the employee. It is not to be used for business records such as drafts, flex sheets and PMIs. In the context of the *Personal Information Protection Act 2004* by storing personal information in TRIM the employee consents to it being there.

Need-to-know

The "need-to-know" principle requires that information is only available to those who need to access information for their assigned duties.

Non-departmental employee

Includes contractors, consultants, short-term labour hire, interns and work experience students conducting work for the Department.

Public information

Information that is clearly and self-evidently publicly available and has been authorised by the owner/custodian for public access and circulation, examples include: books, magazines and other publications including treasury publications such as Budget Papers.

Scanned Images

Records converted by scanning to electronic images must have the degree of authenticity, reliability and accuracy to be reproduced as true copies. This enables the original source record to be disposed of in compliance with departmental and Archives Office of Tasmania requirements.

Legislative framework

Refer to the legislative framework in the Security Policy 12/35709*.

Related documents

Information Management Procedures:

- Procedure to determine the identity, access management and information security classifications for Departmental services and information assets – ref 12/87916*
- Records handling procedures - ref 13/19408*
- TRIM Naming Conventions - ref 07/8005*
- TRIM Managing Electronic Records and Emails - ref 07/8002*
- Scanning Procedure - ref 10/46004*
- TRIM Security Management for access in TRIM - ref 10/30235*
- Managing Groups in TRIM - ref 10/32106*

Other related documents:

- Tasmanian Government Information Security Policy - ref D/36629/003
- Security Policy - ref 12/35709*
- Policy: Use of email, internet and social media - ref 12/199121*
- Acceptable Use of Information and Communication Technology Policy - ref 12/158602 *
- Copyright Policy - ref 09/180515*
- ISB ICT Policies - TresNet

Contacts

Assistant Director, Corporate Information Support

Manager Information Services, Corporate Information Support

Document acceptance and release notice

1. Build Status:

Version	Date	Author	Reason	Section
[12] Revision 8 preserved with mark-ups that was approved by the Executive	8 August 2014	Lynne Valentine	Change: • the policy to reflect a sharing information based on a need-to-know rather than restricting. • definitions of business and short term records for drafts and working papers. Included information security classification definitions • removed definitions for restricted, sensitive, classified, legislative and personal information as they are covered by the information classifications and record types • responsibility of CMG members to approve access, and delegate it, for information that is, PROTECTED or HIGHLY PROTECTED, unless statutory restrictions apply. • updated for changes to Clean Desk Policy 09/176761[2] to reflect core work hours. Definition for business system information and retention of staff email boxes accepted on 20 January 2014.	Policy statement: Information Security Classification: and Definitions
[11]	13 January 2014	Lynne Valentine	NOT USED – draft to Executive 20 January 2014 – needs to be updated for changes to Clean Desk Policy 09/176761[2] for core work hours and sharing information. Security Classifications to be discussed with the Deputy Secretaries. New version based on Version [9] to: • Incorporate the Clean Desk Policy 09/176761[V1] • Definitions: update discovery and add type of business system information to be stored in TRIM. • Simplify the policy by moving the processing components into a new Records handling procedures 13/19408. Reorganised the definitions to include the definitions for all record types upfront followed by other definitions.	
[10]	13 September 2013	Lynne Valentine	NOT USED – draft to Executive for 13 September 2013 includes Clean Desk Policy and Information Security Classification amendments. Agreed in principal to be used for implementation of the Information Security Classifications.	All

[9]	5 April 2013	Lynne Valentine	NOT USED – draft to Exec refer minutes of meeting 13/43252. Add definition of work in progress documents and updated the definition of discovery. Simplify the policy by moving the processing components into a new Records handling procedures 13/19408. Reorganised the definitions to include the definitions for all record types upfront followed by other definitions.	All
[8]	20 June 2012 17 April 2012	Lynne Valentine	Approved by the Executive on 12 June 2012 (ref 12/77813). Includes feedback from the, Executive, CMG and ARMC and consistency review with other security policies. Includes policy approved by the Executive on 28 February 2012 (ref 12/25167) for default classification for all departmental information is X-IN-CONFIDENCE with a risk based approach used to determine higher levels of classification ie PROTECTED and HIGHLY PROTECTED.	All
[7]	20 December 2011	Lynne Valentine	Annual review of policy including the expansion of the policy from TRIM to all departmental information. Updated to include the updated Information Security Policy that was approved by Cabinet in November 2011 and includes Security Classification and the Identity Access Management Toolkit.	All
[6]	20 December 2011	Lynne Valentine	Working draft not used.	
[5]	19 April 2010	Lynne Valentine	Include ICSC feedback on version [4]. Noting by the CMG.	All
[4]	16 February 2010	Lynne Valentine	Policy reformatted into final new template. Added new security policy agreed to by CMG on 15 February 2010. Amended for annual review and ARMC Peer Review 1 March 2010.	Policy Statement, Scope, Responsibilities, Definitions Related documents Legislative Framework
Refer to the actual version of the document for changes as numbering of sections may change between versions.				
[3]	27 March 2009	Lynne Valentine, Tina Howard, Jo Spencer	Policy reformatted into new template and annual policy review process	3, 4, 5
[2]	09 January 2008	Lynne Valentine, Tina Howard, Michael Adams, Allison Mitchell	Policy amended as a result of: ▪ Review following the implementation of TRIM in pilot branches; ▪ peer review by IGFP; and ▪ annual policy review process	1.0, 2.0, 2.1, 2.1.1, 2.1.3, 3.4, 3.6, 3.7, 4.1, 4.1.2, 4.1.3, 4.2, 4.4, 4.5, 4.7, 5.0
[1]	20 November 2006	Lynne Valentine	Approved by CMG	

			Includes amendments from CMG meeting 16 October 2006	2.1.1, 2.1.2 and 4.2

2. Amendments in this release:

Section title	**Amendment summary**
Policy statement	Include that this policy incorporates the Clean Desk Policy and its aims.
Employee responsibilities	Reviewed and moved procedural items to the new Records handling procedure 13/19408*. Include the Clean Desk Policy requirement for employees not to leave departmental information that is not public information unsecured at any time.
CMG responsibilities	Reviewed and moved procedural items to the new Records handling procedure 13/19408*. COMPLIANCE - included the need to conduct regular clean desk policy checks to verify compliance.
DEFINITIONS	• Moved definitions of types of Records up front so that it is easy for staff to find • New definition for: Business system information only needs to be stored in TRIM if it provides supporting evidence for a business transaction, or is a snapshot at a point in time and cannot be reproduced by the originating application. • Added definitions for information security classification. • Updated the definition of discovery to broaden it for all requests, and use and relevance as formal evidence. **From**: All business and short-term records, including email, drafts and revisions, from all information assets may be subject to an RTI request or a legal discovery order. **to**: All records may be subject to discovery including drafts and revisions. This includes Right to Information, Parliamentary enquiry, audit, Ministerial or Ombudsman requests. Records are "discoverable" in any court of law as evidence in the proceedings; and they would be examined and, if relevant, used as evidence in respect of any breach of the State Service Code of Conduct, not just action taken in respect of any breach of the guideline and/or an Employment Direction.

3. Distribution

Version	**Issue date**	**Issued to**
[12]	8 August 2014	Executive for approval – APPROVED with minor amendments (revision 8 preserved with mark-ups)
[11]	20 January 2014	Executive for approval- NOT APPROVED and/or used
[10]	13 September 2013	Executive for approval - NOT APPROVED and/or used
[9]	22 April 2013	Executive for approval - NOT APPROVED and/or used
[8]	12 June 2012	Executive for approval
	6 June 2012	CMG for endorsement
	19 April 2012	ARMC for endorsement
[7]	27 March 2012	Issued to ARMC for endorsement
[6]	20 December 2011	Working draft - deleted
[5]	19 May 2010	Issued to CMG for noting. Published on TresNet
[4]	4 May 2010	Draft issued to ICSC for approval.
[3]	April 2009	Published on TresNet
[2]	20 November 2006	CMG. To be published on TresNet.
[1]	3 April 2008	Published on TresNet