Acceptable Use Policy

Purpose of this policy

The Department of Planning, Housing and Infrastructure (the Department) provides equipment, services, and information to its employees to support them in fulfilling their roles. These tools include computers, software, communication tools (email, chat), access to internal networks (intranet), access to external networks (internet), as well as telephone systems, voice mail, fax, photocopiers, etc.

While the use of the Department's Information and Communication Technology (ICT) resources is essential in supporting its employees' daily business activities, the Department requires that these resources be used in a responsible way, ethically, and in compliance with all NSW and Commonwealth legislation and regulations and other departmental policies and contracts. Non-compliance could have a negative impact on the organisation, its employees, and its customers.

Employees in the Department are expected to use the ICT resources to deliver on the Department's goals and objectives. The types of activities that are encouraged include:

- communicating with fellow employees, business partners, customers, and citizens within the context of an individual's assigned responsibilities
- acquiring or sharing information necessary or related to the performance of an employee's assigned responsibilities
- participating in educational or professional development activities
- collaborating with various stakeholders, teams across the Department to co-create or deliver solutions

This policy complements the Code of Ethics and Conduct, and supports the requirements set out within the Information Security Management System (ISMS) so the Department can achieve the following information security objectives:

- apply appropriate risk-based controls to manage confidentiality, availability and integrity of information, by focusing on sensitive information
- ensure continual improvement of security controls to maintain an acceptable level of risk
- develop associated policies, standards, processes, procedures, guidelines, reports and other artefacts to effectively operate, manage, measure and govern information security as an integral business process
- increase information and cyber security awareness across the organisation

- provide a framework for appropriate management of internal and external audit issues
- comply with the NSW Cyber Security Policy requirements by achieving and maintaining ISO 27001 certification

The information security practices in conjunction with this policy preserve the reputation and integrity of the Department's information assets.

To whom this policy applies

This policy applies to all employees accessing the Department's information and ICT resources, including individuals seconded from other organisations, volunteers, contingent or labour hire workers, professional services contractors, and consultants.

Policy statement

Ownership of ICT resources

The Department is the legal owner of all physical and electronic information, computing and communication technology resources created or acquired to conduct the Department's business.

The Department delegates to its employees the daily management responsibility and custodianship of information and ICT resources for their use, maintenance, and protection. Employees are responsible for upholding the Department's policies to protect the Department's information and ICT resources.

Personal use of ICT resources

The Department provides ICT resources primarily for authorised business purposes. Incidental personal use is permitted, provided that it does not:

- have a negative impact on overall employee productivity
- cause additional expense to the Department
- compromise the Department, its information or security
- disrupt the network performance
- contradict any other departmental policies or legislation including those relating to improper purposes or conduct (as set out below)
- interfere with public interests in the use of public resources

General use of ICT resources

When using the Department's ICT resources, employees must use their best effort and care to:

- safeguard allocated ICT resources from loss and damage
- respect and protect privacy and intellectual property of all parties
- observe and comply with agency information and record management requirements
- maintain the integrity of the Department's information and ICT resources
- ensure that new software, which may store or process sensitive departmental information, either now or in the future, undergoes a security review by the Digital Information Office via CS Connect
- promptly upgrade or remove any software identified as unsupported by the vendor. For outdated software, update to the latest secure version or seek guidance from the Digital Information Office (DIO) if there are concerns
- lock the screen when the device is not in use and maintain a clear desk to prevent the disclosure of sensitive information. When using a shared device, log off the device when not in use
- limit the printing of information and ensure hard copies are securely destroyed using secure departmental bins or shredders
- limit the removal of hard copy information from departmental offices and locations
- when using email, mobile apps/freeware, web browsing, downloading or sharing ICT resources internally and externally:
    - observe privacy and sensitive information practices to ensure Department's information is classified, protected and confidentiality is maintained accordingly
    - use only authorised and trusted channels for information exchange and sharing, such as approved internal file sharing and secure file transfer technologies
    - be cautious of malware infection risks and malicious intent from unknown email sources, attachments, internet browsing, macros in Microsoft documents and downloading of software.
- promptly report the detection of any suspicious activity that may compromise the integrity of the Department's information and ICT resources via CS Connect

When using the Department's ICT resources, employees must not:

- share login credentials such as passwords, but must instead safeguard them in order to prevent unauthorised access by implementing an appropriately robust password in accordance with system requirements.
- use unofficial VPNs, network monitoring software, or port scanners; skip essential security steps, such as entering passwords or utilising multi-factor authentication; set up hidden traps or lures on the network (called honeypots); or disrupt the work of others by overloading

the system or running web servers or file-sharing services directly from departmental devices.

- subvert the Department's security controls (e.g., turning off or disabling the virtual private network (VPN), secure web gateway (SWG) and anti-virus/anti-malware software) unless authorised to do so.
- use ICT resources for personal profit-making or commercial activities.

Use of internet, social media and internal communication channels

The Department provides internet and social media access to all authorised users to assist them in performing their roles. Access to internet, social media and internal communication channels (such as Viva Engage, Microsoft Teams and email) using the Department's ICT resources must be conducted in compliance with this policy, and other associated policies including the Code of Ethics and Conduct.

DCS-2023-01 Cyber Security NSW Directive issued 6 April 2023 prohibits the installation and use of the TikTok application on departmental devices and on personal devices that are used to access departmental information and email. This application can only be installed and used where a legitimate and approved business reason exists and has been approved by the DPHI Social Media team. All employees using personal devices must ensure compliance with organisational policies by removing the TikTok application on personal devices if the device is used to access departmental information and/or email.

Only approved social media channels and accounts may be used to convey officially sanctioned information. All content published to departmental channels must be accurate, approved for external publication, and adhere to the NSW Government social media guidelines.

Employees are not permitted to create social media channels, digital assets (e.g., websites) or subscription accounts for the Department unless authorised to do so by the DPHI Social Media team.

Use of the Department's internet, social media and internal communication channels must not:

- breach policy by pirating software, breaching third party intellectual property rights (e.g., by downloading movies), hacking, participating in the viewing or exchange of pornography or other obscene materials, or engaging in any other unethical or unlawful conduct
- be used to download and install unauthorised files including games
- be used to conduct non-departmental business activities beyond acceptable use tolerances
- be used to participate in gambling
- be used to promote political commentary or commercial products

- be used to negatively affect the Department's or NSW Government's reputation
- be used to access illegal or restricted websites unless explicitly authorised as part of an employee's role
- breach the NSW Government Brand Framework

Personal use of social media

Employees are personally responsible for content published to private social media accounts. When using social media in a personal capacity, employees must:

- not use departmental contact details to register, or include NSW Government branding or insignia on profiles, except when creating a professional profile on career development sites, such as LinkedIn
- not disclose, display, and discuss information about the Department, unless it is already publicly available
- not publish or report on conversations or classified information that deals with internal matters
- be clear that any personal perspective on a matter reflects their own view
- not comment as an official representative of the Department or NSW Government unless authorised to do so by the DPHI Social Media team
- not publish content that could harm or risk the reputation of the Department, its employees, or associated organisations
- uphold organisational values and align behaviour with the Department's Code of Ethics and Conduct and other relevant policies
- not publish content that includes reference to, video or images of other employees without their consent
- not rely on anonymity or pseudonyms for protection and prevention of potential risks

Conduct that is likely to damage the Department's interests, is incompatible with the employee's duty as an employee, or is likely to cause serious damage to the relationship between the employer and the employee may amount to misconduct.

If employees encounter a breach of any of the above, the matter should be escalated to line managers as priority.

Employees can contact the Social Media team with any questions.

Use of Artificial Intelligence (AI)

Employees must only use approved artificial intelligence (AI) technologies for storing, processing, and accessing sensitive Department information[1]. Many free and/or public AI technologies use the data inputted into the service to train and repurpose content, and this could expose personal data or sensitive departmental information publicly.

AI solutions must meet the requirements of the NSW Government Artificial Intelligence Ethics Policy which states AI must be:

- the most appropriate solution for a service delivery or policy problem
- used in such a way as to mitigate as much potential bias as possible
- used safely, securely, and in line with existing privacy and information access requirements
- a solution that is open and transparent so that NSW citizens have access to efficient review mechanisms
- a solution where the decisions are always subject to human review and intervention

AI solutions must also meet the requirements of the NSW Artificial Intelligence Assurance Framework, where applicable.

Use of electronic communication

Electronic communication is limited to official business and occasional personal use for communicating, exchanging and sharing information with both internal and external parties.

Prior to sending, users must observe the NSW Government Information Classification, Labelling and Handling requirements to ensure the intended recipients are aware of the content sensitivity and requirements for protection.

Employees must not send, share, or forward departmental information, files, and emails to their personal email accounts. The Department monitors all emails and may block communications as required, to protect the Department from fraud and the unauthorised disclosure of sensitive information.

Employees are strongly discouraged from using a work email address for personal email communications including personal email subscriptions. If an employee subscribes to a mailing list, the individual must be aware of how to unsubscribe from the list and is responsible for doing so if their current email address changes. The Department may automatically move personal or bulk email to a specified email folder to optimise email productivity for the good of all employees.

[1] Contact Digital Information Office via CS Connect for more information

Employees must take reasonable care when opening emails to prevent embedded malware such as ransomware, malicious hyperlinks, and viruses. Employees must never click on a URL/hyperlink or open an attachment in an email unless they are reasonably certain the email comes from a trusted source. Any suspicious email must be reported via the *Phish Alert Button* in Outlook as soon as possible, to help enable containment before potential malicious activities spread.

Personal electronic communication conducted on or via departmental resources will not be guaranteed private or secure, nor remain available once employment with the Department ceases.

Use of cloud services

The use of cloud services to store personally identifiable information (PII), official and/or sensitive departmental information must be pre-approved through a security review of the technology and a third-party security assurance review, aligning to the NSW Cyber Security policy. Cloud services deemed to be 'crown jewels', or associated with crown jewels, will have additional security controls mandated to help protect the information stored within.

Users are only permitted to use cloud computing services that are authorised under a licence arrangement. Access to cloud-based services must use an enterprise user account or an account created for a specific business purpose that has been endorsed for use.

Users should not use the Department's cloud-based services for personal use beyond what is considered acceptable as outlined in this policy. Users should not use personal or unapproved cloud services to transact, transfer, share or store the Department's information and records.

Remote working

With best effort and due care, employees are responsible for upholding the department's policies to protect the department's information and ICT resources in a manner consistent with being in the office.

When using mobile apps, employees must assess the risks, and take reasonable care in accepting the usage agreements of the apps that may lead to unwanted disclosure of personal and private information. Such disclosure may directly or indirectly impact Department's business and policies. Employees must not download or install software (including apps) on any Department equipment unless formally approved by management and such use must comply with any applicable licence agreements for Department's business.

When working remotely, employees must utilise, whenever possible, their own private or Department-provided internet connection on departmental mobile devices (ADSL, NBN, Mobile Data) to avoid sensitive information being intercepted whilst being transmitted over the internet. Public Wi-Fi must not be utilised for business purposes as it is insecure and may be used by

individuals with malicious intent on the same network to intercept login credentials and other sensitive information that is being transmitted across the network. This is particularly important for networks that don't require a login for joining.

Employees intending to travel overseas with department-issued devices and/or requiring access to departmental systems while abroad must secure prior approval and contact the Service Desk at least two weeks before departure to implement essential security measures. If the risk to departmental systems and devices is deemed too high, alternative arrangements may be needed, or such requests may be rejected.

Physical access controls

All doors, windows, desks and facilities containing Department's ICT resources must be secured appropriately to prevent unauthorised access. Lost, stolen or damaged passes and keys must be reported to your Service Centre as soon as possible.

Unauthorised physical access into offices through tailgating should not be permitted. Any suspicious activities witnessed should be promptly reported to concierge or Corporate Services through CS Connect.

Reporting security and privacy incidents

All employees are responsible for reporting any actual, perceived, suspected or potential information security incidents[2] as quickly as possible to the Service Centre. Privacy incidents must be reported to the Information Access and Privacy Unit.

Alleged or suspected policy breaches must be reported to people leaders or senior officers and referred for investigation to the Chief Information Security Officer or equivalent.

User awareness training and simulation exercises

All employees must participate in technology and cyber security user awareness training and simulation exercises conducted by the Digital and Information Office (DIO) annually or as required and provide feedback to improve the overall awareness of employees.

Monitoring

Any use of the Department's ICT resources is made with the understanding that such use is not absolutely secure, private nor anonymous and is primarily for business use. Employee usage of the Department's ICT resources may be subject to authorised investigation for potential policy non-

[2] Contact Digital Information Office via CS Connect to report information security incidents.

compliance, abuse of privileges as well as any legal or misconduct matters that require evidence to be obtained from the ICT resource.

Requests for access to information to support authorised investigations must be approved by the Chief Information Security Officer and the relevant Executive Director, or their authorised delegate(s).

The Department reserves the right to monitor all internet, digital communications and email activity originating from company-owned equipment or accounts or taking place over departmental networks. If the Department discovers activities that do not comply with applicable law or corporate/departmental policy, records retrieved may be used to document the incident in accordance with due process.

The Department employs continuous CCTV cameras, physical access controls, computer and application activity logging and monitoring to ensure the safety and security of information, people, assets, property and finances, and support any potential security incident investigations. All reasonable care is taken to protect user privacy. Access to monitoring system records is restricted to authorised personnel.

The Department will respond promptly to requests for information arising from criminal investigations and legal proceedings, requests by Parliament under Standing Order 52 notices and requests under the Government Information (Public Access) Act 2009, including the Department's information, records and ICT resources. The Department, therefore, reserves the right to access any of its information systems and data repositories to inspect, review, store or retrieve data in those systems.

This policy is consistent with the NSW Workplace Surveillance Act 2005, State Records Act 1998 and Government Information (Public Access) Act 2009.

Exemptions

- Exemptions to this policy shall comply with the ISMS Exemption Request Management Standard
- Exemptions shall only be approved where it is technically, practically, or financially infeasible to comply with this policy, and the risk is accepted by the appropriate risk stakeholders, in alignment with the technology and cyber security risk management process.
- Reviews of exemptions shall be performed annually or as needed.

Failure to comply with this policy

Should an employee fail to comply with a requirement set out in this policy, then misconduct action may be taken against the employee which may include termination of employment. Non-compliance may also constitute a breach of the ethical and behavioural standards that employees are expected to demonstrate during their employment. These are set out in the Code of Ethics and Conduct.

Individuals who are not government sector employees such as volunteers, contingent or labour hire workers, professional services contractors and consultants may have their services, contract or agreement terminated immediately, or legal action could be taken if they are found to have violated this policy.

Review timeframe

Digital Information Office will review this policy no later than 3 years from the date the document is approved. This policy may be reviewed earlier in response to post-implementation feedback, changes to legislation, or as necessary in accordance with the Department's policy and procedures.

Related documents

A full list of legislative requirements that may impact information security is maintained within the Information Security Management System (ISMS).

- ISO/IEC 27001: 2013 – Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002: 2013 – Information technology – Security techniques – Code of practice for information security management

This policy should be read in conjunction with the following documents:

- Cyber Security Policy
- Access Control Policy
- ISMS Exemption Request Management Standard
- Code of Ethics and Conduct
- NSW Cyber Security Policy
- NSW Cyber Security Strategy
- NSW Government Social Media Guidelines
- NSW Government Brand Framework

Policy metadata

Table 1. Policy metadata

Category	Description
Status	Final
Date of approval	TBA
Approver	Deputy Secretary
Group	Corporate Services
Division	Digital Information Office
Policy owner	Chief Digital and Information Officer
Document location	DPHI Intranet and Internet
Next review date	June 2026
Associated procedure	N/A
Any additional applicability	Additional applicability will be considered in the future
Superseded document	ICT Acceptable Use Policy, Department of Planning and Environment ICT Conditions of Use policy, Department of Industry Information and Communication Technology Acceptable Use Policy, Office of Environment and Heritage
Further information	cybersecurity@dpie.nsw.gov.au
Document Reference	POL21/11

Version control

Table 2. Version Control

Version	Date issued	Change
1	27.05.2021	Merged policies of previous departments/agencies for new Department policy.
1.1	3.05.2022	Updated to reflect new branding and name change
1.2	29.05.2023	Updated to reflect direction on the TikTok application and included some additional requirements. Removed internal links.

Appendices

Appendix 1 – Definitions

Appendix 1 – Definitions

Table 3 – Definitions

Term	Definition
Agency	Has the same meaning as defined under the Government Sector Employment Act 2013.
Availability	Ensuring that Department's ICT resources are accessible for use as, and when they are required.
Care	The obligations of the user to take all reasonable action to protect the Department's information and ICT resources to prevent damage, harm, injury or loss (including economic loss).
Confidentiality	The state of sensitive information being protected from unauthorised access, ensuring that only those with authorisation can access information assets.
Department	The governance arrangement of a general government sector entity[1].
Information	Information held by an agency is defined in Clause 12 of Schedule 4of the Government Information (Public Access) Act to mean: • information contained in a record held by the agency • information contained in a record held by a private sector entityto which the agency has an immediate right of access • information contained in a record that is in the possession under the control, of a person in his or her capacity as an officer or member of employee of the agency. This policy uses the word 'information', which includes 'records' and all types of information, as defined in the Act.

Term	Definition
Information and Communication Technology resources (ICT resources)	Any information, or other assets associated with information and information processing facilities, such as: • information as defined above • laptops, desktops, tablets, external hard-drives, USB memory sticks, memory cards, printers, scanners, faxes, and multi-function devices (devices that provide more than one function e.g. printing, copying scanning) • telephones, mobile phones, and smart phones • secure offices, computer room, network equipment locations, and data centres • network systems, software, applications, apps, and web sites.
Information Security[2]	Preservation of confidentiality, integrity, and availability of information.
Information Security Incident[3]	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Integrity	In the context of Department's ICT resources, the Department can trust the information processed to be complete, accurate and relevant. Other characteristics of integrity may also be observed in Part 2 of the Government Sector Employment Act 2013.
Intellectual Property (IP)[4]	What can be legally owned as the product of intellectual activity in the industrial, scientific, literary, artistic, musical and dramatic fields.
Login credentials	Login credentials are given to authenticate a user and allow access to ICT resources (e.g. User ID and Password pair, User ID and Password associated with one time password, User ID and Password associated with some personal questions only the user can answer)
Remote working	Including working from home, remote working is a method of working that uses technology to facilitate employee working outside of official physical work locations.
Personal information	has the meaning as defined in the Privacy and Personal Information Act 1988.

Term	Definition
Privacy Incident	An action or omission that results in loss, theft, misuse or unauthorised disclosure of personal information, or has the potential to do so.
Security Incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.
Service Centre	A single point of contact and communication for business transactions and incident management matters. CS Service Centre provides technology, finance and human resource support for the majority of the Department of Planning, Housing and Infrastructure, and Department of Regional NSW users. However, some users may rely on support from other Service Centres responsible for the management of their ICT systems and/or devices.
Social media	Sites, tools, applications, and platforms that provide users with infrastructure and resources to connect and communicate with each other. This includes but is not limited to: • Social networking websites/applications, e.g., Facebook, LinkedIn, Twitter • Video and photo sharing websites/applications, e.g., YouTube, Instagram • Blogs, forums, and discussion boards, e.g., Whirlpool • Instant messaging software/applications
User	Employees, contractors, consultants and volunteers engaged by a Department agency who have access to any Department's ICT resources.

[1] Governance Arrangements Chart NSW Department of Premier and Cabinet

[2] ISO/IEC 27000:2016

[3] ISO/IEC 27000:2016

[4] NSW Intellectual Property Management Framework