Internet Policy

Purpose

This policy sets out the key considerations and principles for accessing and using the Internet through Information and Communication Technology (ICT) facilities provided by the City of Sydney, including mobile devices, and personal devices connected to the City of Sydney's networks.

Scope

This policy should be read and understood in conjunction with the City of Sydney values, policies and Code of Conduct. It applies to all users of the City of Sydney's ICT facilities, including Councillors, employees, workers and third parties who have authorised access to the City of Sydney ICT facilities.

Definitions

Term	Meaning
Employees	All City of Sydney employees including permanent (whether full-time or part-time), temporary, casual employees and apprentices.
Information and Communication Technology (ICT) facilities	The technology used to store, process, access and manipulate information. The City of Sydney's ICT resources include but are not limited to all City of Sydney networks, including Local Area Networks (LANs), Wide Area Networks (WANs), and Intranet; emails; hardware; software; servers; desktop computers; printers; scanners; portable computers; mobile devices; storage devices; and cloud services.
Malware	Malicious software programs designed specifically to damage or disrupt a system, including viruses, worms etc.
Proxy and peer-to-peer file sharing sites	Websites that allow computer systems to share files directly, anonymously on the network without the need of a central server.
The Internet	Access to the world wide web through ICT facilities provided by the City of Sydney.
User	Any person using City of Sydney ICT facilities and services to access the Internet, including Councillors, Employees, Workers and authorised third parties.
Web filtering	Examining a Web page to determine whether some or all of it should be blocked to the user by checking the origin or content of a Web page against a set of rules pre-defined by the City of Sydney.
Workers	All employees, agency contractors (labour hire), work experience students and volunteers.

Primary Use

Access to the Internet via City of Sydney ICT facilities is to be used primarily for business purposes, legitimately related to a user's duties at the City of Sydney.

Conditions of Use

All users must use the Internet in an appropriate and professional manner, and in accordance with City of Sydney values, policies, legal and Code of Conduct requirements.

The City of Sydney's 'Pop Up Screen' appears each time users log-on to the City of Sydney's network. By clicking OK and entering the City of Sydney's network, users are acknowledging that they understand and agree to comply with this policy and all its provisions.

The City of Sydney will log, collect and analyse information regarding the use of the Internet in accordance with the *Workplace Surveillance Act 2005* and other relevant legislation and policies. The City of Sydney reserves the right to monitor Internet usage to meet the City of Sydney's statutory obligations and to support the City of Sydney's business needs.

Acceptable Use

Limited personal use of the City of Sydney's internet service and web browsers is permitted and must be:

- Lawful and in accordance with City of Sydney policies, values, legal and Code of Conduct requirements;
- In the knowledge that all Internet use can be monitored by the City of Sydney;
- Not excessive and not adversely affect the productivity and performance of the user's duties;
- Not adversely affect the Cit of Sydney's ICT facilities and services; and
- Not to conduct or solicit private business.

Copyright:

Material on the Internet is protected by copyright, unless specifically stated otherwise. The reproduction, forwarding or in any other way republishing or redistributing words, graphics or other materials must be done only in accordance with copyright law.

Unacceptable Use

The following non-exhaustive list of uses of the City of Sydney's ICT facilities are contrary to City of Sydney values, policies and Code of Conduct requirements:

- Any use of the Internet that adversely affects the performance of the user's duties;
- Stealing, using or disclosing a password without authorisation;
- Expressing personal views as representing those of the City of Sydney;
- Sharing sensitive information (refer Sensitive and Security Classified Information Schema), unless authorised to do so.

- Users of the City of Sydney's ICT facilities and services must not create, send, store, download, access, use, solicit, display, publish or link to any of the following:
  - Software that has not been approved by Technology & Digital Services;
  - Obscene, offensive, hateful and other potentially objectionable images or material;
  - Material that may vilify or cause offence;
  - Material that is intended to annoy, harass or intimidate;
  - Material that infringes intellectual property rights (including copyright);
  - Material that is defamatory;
  - Material that contains malware; or
  - Material that breaches any legislation, such as the Spam Act 2003, by sending unsolicited commercial electronic messages.

Governance and Security

The City of Sydney applies web filtering policies and tools to prevent access to the following types of websites that users are expressly prohibited to use:

- Websites that pose national security risk (an example includes TikTok);
- Websites that allow proxy and peer-to-peer file sharing;
- Websites created specifically for malicious purposes;
- Websites that have been compromised and may contain malware. Please note websites that were previously accessible may become compromised and will be blocked until they have been cleansed by the owner of the website;
- Websites that provide gambling services;
- Websites that contain obscene, sexually explicit or tasteless material; and
- Websites that promote criminal activity, hacking, intolerance, discrimination and hate.

Users should be aware that if they connect to a website that contains prohibited material, they must immediately disconnect from that site. The ability to connect with a specific website does not imply that users are permitted to visit that site.

The Director, People Performance and Technology may authorise access to prohibited sites for a purpose that would normally breach this policy, when the use legitimately relates to the user's role or duties at the City of Sydney.

Monitoring

The City of Sydney must comply with legislative obligations to retain, release and facilitate the retrieval of certain information held on the City of Sydney's systems. The City of Sydney may also access electronic records or logs when investigating possible misuse of City of Sydney Internet services or other potential misconduct.

The Director, People Performance and Technology may authorise:

- Examination of computers and equipment at any time to detect viruses, inappropriate usage, illegal software or files; and
- Monitoring of Internet services to detect inappropriate usage. This may include monitoring the accounts used, time and duration of network activity, access to web pages, volume and content of data storage and transfers, content, transmission and storage.

Responsibilities

Users will:

- use the Internet in a lawful manner and in accordance with City of Sydney values, policies and Code of Conduct.
- protect the City of Sydney network and resources by not accessing websites or downloading files or programs that may contain malware.
- report to Technology & Digital Services when there is suspicion of a security incident, such as a virus infection. In the event of a virus infection, the user must note the symptoms and any error messages appearing on the screen, and disconnect the computer from the network, if not possible then shutdown the computer to prevent spread of the infection to other devices on the City of Sydney's network.

Managers will:

- ensure that staff have read and agreed to this policy.
- ensure that staff personal usage of the Internet is at an acceptable level and does not interfere with their productivity, conduct or performance.
- escalate security incidents, breaches and weaknesses.

Chief, Technology & Digital Services Unit will:

- ensure the physical and environmental security of technologies used for City of Sydney Internet services.
- ensure the retention of web usage logs and other relevant records.

Consultation

Consultation has taken place with Technology and Digital Services, Data and Information Services, Legal Services and Governance.

References

Laws and Standards

- Workplace Surveillance Act 2005
- Anti-Discrimination Act 1977
- Copyright Act 1968 (Cth)
- Local Government Act 1993
- Privacy and Personal Information Protection Act 1998
- Public Interest Disclosures Act 1994
- Racial Discrimination Act 1975 (Cth)
- Spam Act 2003 (Cth)
- Government Information (Public Access) Act 2009

Policies and Procedures

- IT Systems Security Policy
- Code of Conduct

- Email Policy
- Social Media Policy
- Mobile Device policy
- Mobile Device Procedure
- Bring Your Own Mobile Device (BYOD) Policy
- Disciplinary Procedure
- Fraud and Corruption Control Plan
- Internal Reporting Policy – Corrupt Conduct and Serious Wrongdoing
- Harassment Bullying Policy
- Privacy Management Plan
- Sensitive and Security Classified Information Schema
- Telephone Service Standards
- Purchase Card Policy

Review period

This policy will be reviewed every 3 years.

Approval Status

The Chief Executive Officer / Council approved this policy on 21/9/2023

P.M. Barone

Approval History

Stage	Date	Comment	TRIM Reference
Original Policy	May 2014	Endorsed by the Executive.	2014/239272
Reviewed	June 2017	Fit for purpose. No major changes.	2017/444050
Reviewed	6 July 2020	Fit for purpose. No major changes.	2020/193542
Reviewed	21 September 2023	Updated Governance & Security references. Minor formatting and reference changes.	2020/301066
Commence Review Date	21 December 2025		
Approval Due Date	21 September 2026		

Ownership and approval

Responsibility	Role
Author	Chief, People and Culture
Owner	Chief, People and Culture
Endorser	City of Sydney Executive
Approver	Chief Executive Officer

CITY OF SYDNEY INTERNET POLICY

I have read the City of Sydney Internet Policy (”the Policy”). I understand the Policy, my obligations and I agree to comply with the Policy’s provisions.

When I logon to the computer network and click OK on the pop-up screen displayed, I am acknowledging my understanding of the Policy and my agreement to comply with the Policy’s provisions.

I understand that:

- Use of the Internet should be primarily for business purposes legitimately related to my duties at the City of Sydney, and must comply with City of Sydney values, policies and Code of Conduct.

- Use of the Internet must not include creating, sending, storing, downloading, accessing, using, soliciting, displaying, publishing or linking to any of the following:
  - software that has not been approved by Technology & Digital Services;
  - obscene, offensive, hateful and other potentially objectionable images or material;
  - material that:
    - may vilify or cause offence;
    - is intended to annoy, harass or intimidate;
    - infringes intellectual property rights (including copyright);
    - is defamatory;
    - contains malware;
    - breaches any legislation, such as the *Spam Act 2003,* by sending unsolicited commercial electronic messages.

Name (print) …………………………………………………

Signature ……………………………………………………….

Date …………………………………………………………...