Sydney Opera House Policy

Title:	Acceptable Information and Technology Use and Surveillance Policy
Policy Number:	SOH146
Effective Date:	15/05/2024
Authorisation:	Chief Executive Officer
Authorisation Date:	15/05/2024
Superseded Policy:	SOH116 Information Systems and Security Policy
Accountable Director:	Executive Director, Corporate Services & CFO
Responsible Officer:	Chief Technology Officer

1. CORE PROPOSITION

1.1. The Sydney Opera House's (SOH) Information and technology assets are valuable and must be protected and used appropriately. The Acceptable Information and Technology Use and Surveillance Policy (this Policy) sets out:

- IT users' responsibilities to ensure the confidentiality, integrity and availability of these assets (sections 4–7).
- How use of these assets is monitored and enforced through workplace surveillance (sections 8-10).

Notice to employees

1.2. This Policy is a notice to all employees of workplace surveillance, as required by the *Workplace Surveillance Act 2005 (NSW)*. Surveillance by authorised SOH employees of network and internet access, including email, is carried out on an intermittent and ongoing basis in accordance with this Policy.

2. SCOPE

This Policy applies to all Information and technology assets managed by or on behalf of SOH and all IT users.

3. DEFINITIONS

3.1. **Authorised SOH users** – users who, as part of their duties and responsibilities, are required and authorised to access surveillance data, only to the extent required to fulfil their duties and responsibilities.

3.2. **Device** (s) – any item (s) used for business communication e.g. a computer whether desktop or laptop, mobile phone, tablet, desk phone, television or two-way radio.

3.3. **Generative artificial intelligence (AI)** – a subset of AI that generates novel content such as text, images, audio and code in response to prompts. Generative AI technologies use large language models (LLMs) that specialise in the generation of human-like text.

3.4. **Information and technology asset** – an identifiable collection of data, including devices, systems and information, stored in any manner, that has value for SOH, e.g. ticketing management system, customer personal information, structural building information, corporate banking data, online drives and email.

3.5. **Supervisor** – employees, contractors, consultants and persons otherwise engaged to undertake work on behalf of SOH, with management responsibilities.

3.6. **Surveillance data** – any information collected by or on behalf of SOH about an IT user's behaviour on SOH Information and technology assets, e.g. web browsing history, radio transmission, email content, online chat content or information about the physical movement of Devices.

3.7. **IT users** – SOH employees, contractors, consultants, and persons otherwise engaged to undertake work on behalf of SOH, who access Information and technology assets managed by or on behalf of SOH.

4. ACCEPTABLE USE

4.1. Use of SOH Information and technology assets must be lawful, ethical and constructive, including as set out in this Policy.

4.2. It is unacceptable to use Information and technology assets in a way that could damage SOH's reputation. This includes communications that may:

- Be misleading or deceptive.
- Result in discrimination, victimisation or harassment.
- Reasonably found to be offensive, obscene, threatening, abusive or defamatory.
- Lead to civil liability or criminal penalty.

4.3. Examples of unacceptable use include:

- Tasteless material (such as the depiction of injury or animal cruelty).
- Pornographic or sexually explicit material.
- Racist, sexist or homophobic material.
- Personal political or religious material.
- Posting business-related information to online forums or blogging sites.
- Unauthorised use of intellectual property, including proprietary software.
- Unauthorised use of confidential information.

4.4. All social media use must comply with SOH's *Social Media Policy*.

GENERATIVE ARTIFICIAL INTELLIGENCE (AI)

4.5. Generative artificial intelligence (AI) platforms (such as ChatGPT, BingAI, BardAI and DALL.E) present opportunities for increased productivity across the NSW public sector but they also introduce ethical, privacy and security risks that must be considered for the appropriate use of SOH's information assets.

4.6. The NSW *Artificial Intelligence Ethics Policy* and *AI Assurance Framework* authorise the use of AI as long as it complies with the relevant legislation and aligns with the principles of community benefit, fairness, privacy and security, transparency and accountability. See SOH's *Code of Conduct* for information on the conduct and behaviour expected of SOH employees.

4.7. When using public AI tools and platforms, IT users must not disclose or input:

- Personal or health information. Such use or disclosure constitutes a data breach as defined in SOH's *Data Breach Policy*. Additionally, under SOH's *Privacy Management Policy and Plan,* it is an offence for any person employed or engaged by SOH to use or disclose any personal information about another person in the exercise of their official functions.
- Official information. This is defined in SOH's *Information Classification Policy* as information that is not publicly available.
- Any SOH databases that may contain information that cannot be shared, as outlined above, and big datasets.
- Information that would allow public AI tools to extrapolate classified or sensitive information based on the aggregation of content entered over time.

4.8. When using public AI tools and platforms, IT users must not create an account unless registration is required, and where registration is required, contact SOH's Helpdesk for guidance.

4.9. IT users must use public AI tools and platforms ethically and responsibly and:

- Be able to explain and justify their actions and decisions. Humans must remain the final decision-maker.
- Fact check and verify all outputs before using them for official purposes and reference any AI-generated content.
- Not use generative AI outputs that are unethical, irresponsible, biased, inaccurate or discriminative.
- Not use outputs that infringe on copyright or violate intellectual property rights.

5. SECURITY OF INFORMATION AND TECHNOLOGY ASSETS

5.1. IT users are responsible for the Information and technology assets assigned to them, or under their control, and must take reasonable steps to ensure that these are protected and equipment is secured against damage, misuse, disclosure, loss and theft.

5.2. SOH information must be protected in accordance with this Policy. Passwords must never be shared, written down in plain view or otherwise communicated to anyone other than the IT user associated with the system account.

5.3. IT users must follow SOH's Password Standard, available on the SOH intranet, Intouch.

5.4. IT users must always lock their Devices when they are not in active use and SOH computers (any desktop and/or laptop) must be turned off at night.

5.5. IT users accessing online services for business purposes must use their SOH identity for authentication. Personal email addresses or accounts must not be used for work purposes.

5.6. Network bridges, tunnels, proxies and related services are forbidden. IT users must not attempt to circumvent network controls or other security systems.

5.7. Requests to change the software environment of an SOH Device must be made to the Technology Help Desk.

5.8. Lost or stolen SOH Devices, or Devices containing SOH data must be reported immediately to the Technology Help Desk.

5.9. IT users must not store sensitive information on removable media without prior approval from the Chief Technology Officer (CTO).

6. REASONABLE PERSONAL USE

6.1. SOH is committed to promoting work-life balance by allowing reasonable personal use of Information and technology assets. This use is a privilege and not a right.

6.2. Use of Information and technology assets for personal financial gain is prohibited.

6.3. IT users accessing online services for personal use by means of Information and technology assets, accept all responsibility and liability for any personal loss or damages.

7. PERSONAL DEVICES

7.1. Use of personal Devices for work purposes is only permitted when SOH is able to retain control of its Information and technology assets. This includes the ability to delete stored data or deactivate services used for SOH business purposes.

7.2. SOH is not liable for lost data, financial damage, or penalties incurred on personal Devices as a result of exercising this control.

8. PURPOSE OF SURVEILLANCE

8.1. SOH monitors and collects surveillance data:

- To protect the reputation of SOH.
- To monitor compliance with rules, policies and procedures.
- To investigate claims, accidents, incidents and breaches of the law, or allegations of such, and for the purpose of any relevant legal proceedings.
- For audit and reporting purposes.

8.2. No IT user can have an expectation of privacy when using SOH Information and technology assets.

9. ACCESS TO SURVEILLANCE DATA

9.1. The CTO controls access to surveillance data that is in the scope of this Policy.

9.2. Surveillance data may be made available to SOH employees and third parties in line with the *Workplace Surveillance Act 2005 (NSW)*, and for any purpose authorised by law, for example:

- To the Chief Executive Officer; Executive Director, Building, Safety and Security; Executive Director, People and Government; Head of Security, Emergency Planning and Response; or an appropriate supervisor.
- To a law enforcement agency or other government agency.
- Where required or permitted under the *Government Information (Public Access) Act 2009 (NSW)* (see SOH Access to Information (GIPA) Policy for more information).
- Where required or permitted under the *Privacy and Personal Information Protection Act 1998 (NSW)* (see SOH Privacy Management Policy and Plan for further information).
- To meet a legal requirement (such as a subpoena).

9.3. Requests for access to surveillance data must be made in writing to the CTO, clearly outlining the reason for access and under what authority the request is being made.

10. MONITORING AND ENFORCEMENT

10.1. Surveillance data may be inspected, disclosed, monitored, and analysed by Authorised SOH users.

10.2. Internet access and email delivery may be blocked where content contravenes the objectives of this Policy, e.g. pornographic content, potential spam, or content that could compromise security of Information and technology assets. Access to blocked content must be approved in writing by the CTO.

10.3. Breach of this Policy may result in disciplinary action, including dismissal, in accordance with the *Government Sector Employment (GSE) Act 2013*, *GSE Regulation 2014* and *GSE Rules 2014* (GSE legislation). The following actions may also apply:

- Withdrawal of access to the internet, certain websites, or other privileges.
- Criminal proceedings.
- Civil proceedings.

11. RESPONSIBILITIES

11.1. All **IT users** of SOH Information and technology assets are responsible for:

- Understanding and complying with this Policy and all other information security policies, standards or procedures applicable to their role.
- Signing the acceptance statement in Appendix A of this Policy.

11.2. All **SOH employees** must complete the annual cyber security awareness training and participate in the regular phishing simulations.

11.3. All **supervisors** are responsible for ensuring that users under their supervision are aware of and comply with this Policy.

11.4. The **Information Manager** is responsible for monitoring adherence to this Policy.

11.5. The **CTO** is responsible for reporting non-compliance with this Policy to the Executive and for implementation and review of this Policy.

12. RELEVANT LEGISLATION AND POLICIES

- Cyber Security NSW generative artificial intelligence (AI) guidelines
- Government Information (Public Access) Act 2009 (NSW)

- Government Sector Employment (GSE) Act 2013 (NSW)
- NSW AI Assurance Framework
- NSW Cyber Security Policy
- NSW Artificial Intelligence Ethics Policy
- Privacy and Personal Information Protection Act 1998 (NSW)
- Surveillance Devices Act 2007 (NSW)
- Workplace Surveillance Act 2005 (NSW).

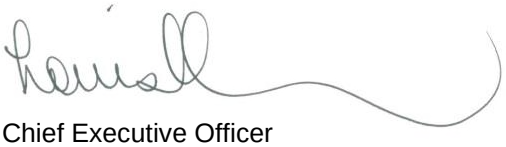
13. SOH SUPPORTING DOCUMENTS

- Access to Information (GIPA) Policy
- Code of Conduct
- Data Breach Policy
- Grievance Resolution Procedure
- Information Classification Policy
- Password Standard
- Privacy Management Policy and Plan
- Respectful Workplace Behaviour Policy
- Resolving Workplace Grievances Policy
- Social Media Policy.

Version control

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Chief Executive Officer	15/04/2022	15/04/2022	New policy
1.1	Chief Executive Officer	15/05/2024	15/05/2027	Updates to refer to the appropriate use of public generative AI platforms.

APPROVED



Chief Executive Officer

Date: 15/05/2024

Appendix A – Acceptance Statement

Acceptance

As a condition of your employment or engagement with SOH you agree to comply with the *SOH Code of Conduct* and other SOH policies, including this *Acceptable Technology Use and Surveillance Policy*. You are asked to sign this acceptance statement in order to provide a record that you have read, understood and agreed to this Policy.

If you do not understand or wish to clarify any part of this Policy, please raise this with your manager or SOH's Chief Technology Officer (CTO).

Otherwise please sign below to confirm that you have read, understood, and agree to abide by this *Acceptable Information and Technology Use and Surveillance Policy*.

Signed	
Print Name	
Business Unit	
Date	

Please return this signed form to SOH's People & Development team.