Title:	Acceptable Information and Technology Use and Surveillance Policy
Policy Number:	SOH146
Effective Date:	16 June 2017
Authorisation:	Chief Executive Officer
Authorisation Date:	15 June 2017
Superseded Policy:	*SOH116 Information Systems and Security Policy*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 information and technology assets are valuable and must be protected and used appropriately. This Policy sets out:

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

Notice to employees

1.2. This policy is notice to all employees of workplace surveillance, as required by the *Workplace Surveillance Act 2005*. Surveillance by authorised Opera House 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 the Opera House and all users of those assets.

3. DEFINITIONS

3.1. **Authorised Opera House 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** – any item used for business communication e.g. a computer whether desktop or laptop, mobile phone, tablet, desk phone, television or two-way radio.

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

3.4. **Supervisor** – employees, contractors, consultants and persons otherwise engaged to undertake work on behalf of the Opera House, with management responsibilities.

3.5. **Surveillance data** – for the purposes of this policy is any information collected by or on behalf of the Opera House about a user's behaviour on Opera House information and technology assets, e.g. web browsing history, radio transmission, email content, online chat content or information about the physical movement of devices.

3.6. **Users** – Opera House employees, contractors, consultants, and persons otherwise engaged to undertake work on behalf of the Opera House, who access information and technology assets managed by or on behalf of the Opera House.

4. ACCEPTABLE USE

4.1. Use of Opera House 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 the Opera House's reputation. This includes communications that may:

- be misleading or deceptive;
- result in discrimination, victimisation or harassment;
- reasonably be found to be offensive, obscene, threatening, abusive or defamatory; or

- lead to civil liability or criminal penalty.

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; and
- Unauthorised use of confidential information.

4.3. All social media use must comply with the *SOH Social Media Policy*.

5. SECURITY OF INFORMATION AND TECHNOLOGY ASSETS

5.1. 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, loss and theft.

5.2. Sensitive 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 user associated with the system account.

5.3. Users accessing online services for business purposes must use their Opera House identity for authentication. Personal email addresses or accounts must not be used for work purposes.

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

5.5. Requests to change the software environment of an Opera House device must be made to the Technology Help Desk.

5.6. Lost or stolen Opera House devices, or devices containing Opera House data must be reported immediately to the Technology Help Desk.

6. REASONABLE PERSONAL USE

6.1. The Opera House 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. 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 the Opera House is able to retain control of its information and technology assets. This includes the ability to delete stored data or deactivate services used for Opera House business.

7.2. The Opera House 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. The Opera House monitors and collects surveillance data:

- to protect the reputation of the Opera House;
- 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; and
- for audit and reporting purposes.

8.2. No user can have an expectation of privacy when using Opera House information and technology assets.

9. ACCESS TO SURVEILLANCE DATA

9.1. The Chief Technology Officer (CTO) controls access to surveillance data.

9.2. Surveillance data may be made available to Opera House employees and third parties in line with the *NSW Digital Information Security Policy* (DISP), and for any purpose authorised by law, for example:

- To the Chief Executive Officer; Director of Safety, Security and Risk; Director, People and Culture; 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 (see the SOH Access to Information (GIPA) Policy for more information);
- Where required or permitted under the Privacy and Personal Information Act 1998 (NSW) (see the SOH Privacy Management Policy and Plan for further information); or
- 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 Opera House 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; and
- Civil proceedings.

11. ROLES AND RESPONSIBILITIES

11.1. All **users** of Opera House 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; and
- Signing the acceptance statement at Appendix A of this Policy.

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

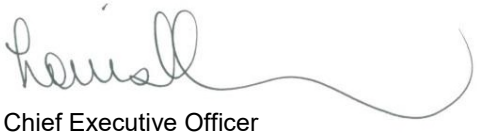
11.3. The **Information Manager** is responsible for monitoring adherence to this Policy.

11.4. The **Chief Technology Officer** is responsible for reporting non-compliance with this Policy to the Executive and for implementation and review of this Policy.

12. RELEVANT LEGISLATION AND SUPPORTING DOCUMENTS

Workplace Surveillance Act 2005
Surveillance Devices Act 2007
NSW Digital Information Security Policy (DISP)
SOH Access to Information (GIPA) Policy
SOH Bullying and Harassment Policy
SOH Code of Conduct
SOH Privacy Management Policy and Plan
SOH Records Management Policy
SOH Social Media Policy

APPROVED



Chief Executive Officer

Date: 15 June 2017

Appendix A – Acceptance Statement

Acceptance

As a condition of your employment or engagement with the Sydney Opera House you agree to comply with the Opera House Code of Conduct and other Opera House 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 the Chief Technology Officer.

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

Signed	
Print Name	
Department	
Date	

Please return this signed form to the People & Culture department.