

1. Scope

Australian News Channel (ANC) has surveillance on its premises in the interests of ensuring the security and protection of its property, employees, clients and members of the public. ANC is committed to meeting its obligations under the applicable workplace surveillance legislation, or any other legislation which may address surveillance or monitoring in the workplace.

The policy describes the circumstances in which ANC conducts workplace surveillance of its employees, namely, telephone, camera, computer and tracking surveillance.

The policy outlines how, when and why ANC is carrying out surveillance. Relevant workplace surveillance legislation may deal with surveillance of employees by means of cameras, computers or tracking devices and requires that employees are notified as to the nature of that surveillance.

This policy should be read in conjunction with all other ANC policies, including the Code of Conduct, Privacy and Using Technology Safely policies.

Definitions

“ANC’s Technology Systems”: means all technology resources or applications provided for use by ANC and includes the corporate computer network and associated equipment, file servers, networks, information technology hardware, internet and intranet facilities, telephone systems, voicemail, email as well as ANC Issued Technology Equipment.

“ANC Issued Technology Equipment”: includes desktop and laptop computers, business applications and data, electronic storage media (for example, USB drives, removable hard disks, CDs), information technology hardware or software, mobile phones, smart phones, tablet devices or PDAs, and other system equipment and devices provided by ANC.

“employees”: means all full-time, part-time, fixed term and casual employees employed by ANC. It also includes contractors, contributors, consultants, interns, work experience students and volunteers providing a service to ANC.

2. Types of Surveillance

Surveillance is conducted by the following means:

- Telephone surveillance – which is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a fixed or mobile telephone or any other device that sends or receives telephone calls or messages (including, but not limited to, outgoing or incoming calls, text or instant messages and “apps” downloaded)
- Camera Surveillance – which is surveillance by means of a camera that monitors or records visual images or activities on premises or in any other place
- Computer Surveillance – which is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including but not limited to, the sending and receipt of emails and the accessing of internet websites) and
- Tracking surveillance - which is surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as global positioning system tracking device).

3. Notification

Employees will be notified of this policy in accordance with relevant workplace surveillance legislation, which may include by email, hard copy and/or by referral to a common drive on ANC's computer network or ANC's intranet.

All new employees will be given written notification of surveillance activities at ANC before they commence their employment (or engagement) – which could include providing them with a hard copy of this policy upon commencement. Any such notification will also refer to this policy. ANC will also periodically remind employees of the surveillance activities and will refer employees to this policy.

Any changes to this policy, or the nature of any surveillance, will be notified to employees by email, provided with access to the amended policy and/or on noticeboards at ANC's premises not less than 14 days before any change takes effect.

4. Use and Disclosure of Surveillance

ANC will not use or disclose surveillance other than:

- For any legitimate purpose related to an employee's employment (or engagement for services)
- For the legitimate business activities or functions of ANC, including internal inquiries and investigations of alleged unlawful activities or activities that are alleged to be in breach of any ANC policy or code of conduct or in breach of an employee's duties at ANC

- When ANC reasonably believes that there is an imminent risk of substantial damage to property or serious violence to any person and/or
- To provide information to a law enforcement agency in relation to criminal or civil proceedings.

5. ANC Surveillance

Telephone Surveillance

- ANC monitors the input and output of telephone (both fixed line and mobile) devices provided by ANC for use by employees.
-
- ANC may access ANC-owned telephones, telephone logs and other telephone records and backups to ensure the security, confidentiality, availability and integrity of ANC's telephone systems.

Camera Surveillance

ANC operates security cameras within its premises where required to ensure the safety and security of employees and to visitors who visit ANC's premises.

Camera surveillance involves the use of visible cameras and/or camera casings. Camera footage may be accessed and used to investigate any instances that in the reasonable opinion of ANC warrant investigation, including, but not limited to, assault, theft or damage to property. Such records may also be required by law to be provide to other parties, such as court or to the police.

Where security cameras are in place, ANC's premises will display notices in a prominent and visible position regarding the existence of cameras at the premises.

Due to the nature of ANC's business, at any time we are in the vicinity of an authorised ANC filming for its business (be it at any ANC premises or outside of the premises), we may be recorded by a camera. Relevant information may be accessed in the course of a workplace investigation relating to misconduct or determining whether there has been a breach of ANC's policies.

Computer Surveillance

The use of ANC Issued Technology Equipment (which includes computers, laptops and other electronic devices) and associated ANC's Technology Systems is governed by ANC's Using Technology Safely policy.

From time to time, ANC may investigate alleged breaches of the law or ANC policies by using its ANC Issued Technology Equipment and/or ANC's Technology Systems. These may include cyber bullying, theft or other inappropriate workplace conduct/behaviour. These investigations could involve accessing the employee's computer, other electronic devices and/or electronic records. For employees such

investigations may involve misconduct or serious misconduct and are managed in accordance with ANC's policies.

ANC undertakes computer surveillance and monitors employee use of ANC Issued Technology Equipment (which includes computers, laptops and other electronic devices) in the following areas:

- Any electronic device connected to ANC's Technology Systems, regardless of who owns the device
- ANC retains logs, backups and archives of computing activities, which may be audited. Such records are the property of ANC and are subject to State and Federal laws and may be used as evidence and
- Monitoring may include, but is not limited to, storage volumes, download volumes, external hard drives, databases, data storage devices, browsing/download history (and site content), applications installed, device location and access point to network.

Email and Internet

Our emails are not routinely read or monitored. However, emails are records of ANC and should be managed accordingly and will be accessible in that context. An email may also be the subject of an application under privacy legislation.

ANC may access and monitor the use of email and internet systems in the following ways:

- ANC monitors email server performance and retains logs, backups and archives of emails sent and received through the ANC server. Even where the user has deleted an email, ANC may still retain archived and/or back-up copies of the email. Only employees authorised by ANC may examine such records
- ANC retains logs, backups and archives of all internet access and network usage. These records may be audited, are subject the State and Federal laws, and may be used as evidence. While individual usage is not routinely monitored, unusual or high volume activities may warrant more detailed examination
- For the purposes of producing the email in response to a legal requirement or other lawful investigation
- For the purpose of determining whether, as part of an investigation by ANC, there has been unacceptable use of email or internet
- For the purposes of determining whether there has been a breach of ANC's policies in the use by the employee of ANC's resources and
- For the purposes of investigating allegations of misconduct or to provide materials to an external investigative authority that is lawfully investigating possible criminal conduct.

Scope of Surveillance

ANC monitors employee use of all ANC Issued Technology Equipment. To avoid any doubt, this includes workstations, laptops, servers, telephone and mobile devices, ipads and/or tablets, email and network services, all devices connected to ANC's Technology Systems (even if the actual device is not owned by ANC) and connections to the internet services (including fixed, Wi-Fi and 3G/4G).

Tracking Surveillance

Tracking devices come in many forms and can be fixed (for example, to a vehicle) or handheld. The devices can be used to provide operational and/or safety information related to the exercise of a function of ANC.

ANC provides and makes available, for use by employees, equipment and devices that may have the functionality to monitor and record geographical location or movement. For example:

- Mobile telephones, laptops, tablets and similar devices
- Access and security cards into ANC premises
- ANC-owned vehicles with global positioning systems (GPS) installed
- Fuel cards issued for ANC-owned vehicles and
- Wired and wireless data point connections installed in ANC premises.

The primary purpose of the provision of the equipment and devices may not be to monitor or track the location or movement of individual employees (apart from a GPS, which primary function is to monitor or record geographical location or movement). However, any available and relevant information may be accessed and used by ANC for a legitimate purpose as provided by this policy. For example, in the course of a workplace investigation relating to misconduct or determining whether there has been a breach of ANC's policies.

For the purposes of GPS surveillance, ANC will install visible signs in all ANC-owned vehicles fitted with tracking devices to inform all vehicle users that surveillance tracking is being carried out.

Tracking surveillance is continuous and ongoing, and is in place as at the date of approval of this policy.

6. Prohibited Surveillance

ANC will not carry out any prohibited workplace surveillance, as set out below:

- Surveillance of employees in a change room, toilet facility or shower or other bathing facility in the workplace
- Surveillance of employees using work surveillance devices when employees are not at work, except as permitted under the applicable workplace surveillance legislation and ANC policies

- Blocking emails or internet access of an employee, except as permitted under the applicable workplace surveillance legislation and ANC policies, including the section “*Blocking of email or internet use*” in this policy and
- Any *covert surveillance* (which is surveillance other than that requiring notification in accordance with the applicable workplace surveillance legislation) by ANC without a covert surveillance authority issued under the applicable workplace surveillance legislation.

7. Blocking of Email or Internet Use

ANC is prohibited from blocking an employee from accessing the internet or sending or receiving emails unless:

- ANC acts in accordance with its policies relating to email or internet access that have been notified to the employee in advance in such a way that it is reasonable to assume the employee is aware of and understands the relevant policy. For example, refer to ANC’s Using Technology Safely policy and
- If the ANC intends to prevent delivery of an email, ANC gives the employee notice (which can be by email) that delivery of the email will be blocked.

However, if ANC intends to prevent delivery of an email, ANC is *not* required to give the employee notice that the delivery of an email will be blocked if:

- ANC regards the content of the website or email, including any attachment, as menacing, harassing or offensive, for example, pornographic, gambling or terrorist websites
- The email is or contains a commercial electronic message, as defined in the [Spam Act 2003 \(Commonwealth\)](#)
- The content or attachments of the email would or might result in unauthorised interference with, or damage to, ANC Issued Technology Equipment and/or ANC’s Technology Systems
- The sender of the email has been identified as having previously sent malicious content to the organisation and/or
- ANC is not aware (and cannot reasonably be expected to be aware) of whether an employee has sent that email or of the identity of any other person who has sent that email.

8. Our Obligations

We all must comply with all applicable laws and ANC policies relating to the use of all communications, information technology and electronic resources.

Cameras in mobile telephones, either owned by the employee or supplied by ANC, are not to be used, under any circumstances, to record images of any persons without their knowledge or consent in ANC’s workplace or at any other work related event.

Mobile telephones and any other recording devices (whether or not supplied by ANC) must not be used under any circumstances to record a conversation, meeting or otherwise without the written consent of the person being recorded.

However, as detailed above in this policy, we acknowledge and consent to the filming and/or recording in the circumstances when in the vicinity of any authorised ANC filming and/or recording for its business (be it at any ANC premises or outside of the premises).

9. Further Information

This policy replaces all pre-existing ANC policies, standards or guidelines that are related to workplace surveillance. It does not form part of any contract of employment or override the terms of any contract, award or registered agreement which might also apply to employment with ANC. The policy may also be varied or rescinded from time to time.

10. Policy Version and revision information

Title	Workplace Surveillance
Version	1.0
Date of Issue	November 2017
Policy Owner	General Manager, Human Resources/Head of Legal
File Name	Workplace Surveillance