Workplace Surveillance Policy

Technology improvements have made devices which fall within the statutory definition of surveillance devices commonplace. During normal operations, Ready Group uses these devices and the information and data they generate due to the business benefits they provide. These benefits include, but are not limited to:

- Potential to deter vandalism and/or possible assailants
- Reduce the safety risks associated with workers, customers and others in the workplace
- Using data and information to defend employees against incorrect allegations
- Increasing information available when conducting investigations (e.g. code of conduct and fraud related complaints)

The Workplace Surveillance Act 2005 (NSW) (WS Act) sets out the legal requirements regarding the use of these devices and information generated by them.

The **Purpose** of this Policy is to:

- detail Ready Group's commitment to ensuring that it complies with the requirements of this legislation
- explain to employees the types of surveillance that may be carried out in the workplace and
- explain the responsibilities of management in regards to the introduction of workplace surveillance

Where there is an inconsistency between this Policy and the WS Act, the WS Act prevails.

This Policy applies to **all** employees. This Policy does not form part of any employee's contract of employment.

Workplace Surveillance

This Policy is the written notification to employees regarding Ready Group's activities that fall within the statutory definitions of surveillance. The types of workplace surveillance that Ready Group conducts include:

- Closed circuit TV camera surveillance (CCTV)
- Computer surveillance
- GPS monitoring
- Cloud based in vehicle surveillance

Nature of Surveillance

- Surveillance will be carried out in accordance with this Policy
- All forms of surveillance (Camera and Computer surveillance) will be continuous and Ready Group will carry out surveillance of any user at such times of Ready Group's choosing and without further notice to any user in accordance with the WS Act and this Policy

- Surveillance, as detailed within this Policy, will be ongoing unless specified within an amendment and subsequent approval of this Policy
- As technology improves and changes, other devices are likely to become available and will generate surveillance data and information. Where this happens, devices, information and/or data will be managed in accordance with the WS Act and this Policy

Camera Surveillance

The primary purpose of Ready Group's camera surveillance is for security and safety. Surveillance cameras are mainly at entries/exits of the yard and office, however some do exist within the offices and other spaces. The cameras at the entries/exits of the yard do not have audio capacity, the cameras within buildings are audio-visual cameras.

Ready Group will:

- ensure that surveillance cameras (including their casings or other equipment generally indicating the presence of a camera) are clearly visible where surveillance is taking place
- clearly display visible signs at each workplace entrance notifying people that they may be under surveillance

Generally, staff will be aware of and/or involved in the installation of these cameras and this Policy is further notification to staff that these cameras are used.

In vehicle camera surveillance is used to improve and monitor driver behaviour. The system sends an alert when an unsafe driver behaviour is detected. The driver is alerted as well as the Chief Operations Manager. To confirm, no audio is recorded within the vehicles.

Tracking & GPS Surveillance

The Workplace Surveillance Act also regulates all forms of tracking surveillance on employees including electronic devices which monitor an employee's geographical location such as GPS.

Computer, Internet & Email Surveillance

Use of Ready Group's computers, email and internet accounts generate vital information and data which is considered to be Ready Group's property and is managed accordingly. Ready Group may from time to time retrieve and review such information and data in accordance with this Policy.

The Act restricts computer surveillance by employers including monitoring or recording of information accessed and sent. It also regulates the surveillance of internet access by employees and prohibits the blocking of emails.

Under the Act, surveillance of an employee's computer use can only be carried out where:

- There is an existing policy on computer surveillance in the workplace and
- You have provided notice to the employee in advance and

- The employee is aware of and understands the policy

The Act also prohibits the blocking of emails sent to or by an employee. Emails can be blocked if:

- It is in accordance with the computer policy of the workplace
- The content of the email contained a virus
- The email was spam
- The email can be reasonably regarded as being menacing, harassing or offensive

Prohibited Surveillance

In accordance with the WS Act Ready Group will not:

- Conduct surveillance of change rooms and bathrooms
- Use work surveillance devices while employees are not at work, unless the surveillance is computer surveillance of the use by the employee of equipment or resources provided by or at the expense of Ready Group
- Prevent, or cause to be prevented, delivery of an email sent to or by, or access to an Internet website by, an employee of Ready Group unless;
    - It is in accordance with this Policy
    - Ready Group has (as soon as practicable) provided the employee a prevented delivery notice by email or otherwise, unless notice is not required in accordance with s17(2)-(3) of the WS Act
    - Prevent delivery of an email or access to a website merely because the email was sent by or on behalf of an industrial organisation of members, employees or an officer of such an organisation, or the website or email contains information relating to industrial matters (within the meaning of the Industrial Relations Act 1996 (NSW)).

Covert Surveillance

Ready Group will not carry out, or cause to be carried out, covert surveillance unless it is in accordance with the requirements of Part 4 of the WS Act.

Surveillance Information and Data

All employees shall at all times be compliant with Ready Group's Code of Conduct and maintain strict confidentiality of all records, information and data. Ready Group will ensure that surveillance information and records are not used or disclosed unless the use or disclosure is:

- for a legitimate purpose related to the employment of employees or Ready Group's legitimate business activities, or
- to a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence, or
- for a purpose that is directly or indirectly related to the taking of civil or criminal proceedings, or
- reasonably believed to be necessary to avert an imminent threat of serious violence to persons or of substantial damage to property.

For the avoidance of doubt, Ready Group may use or rely on surveillance records for the purposes of taking disciplinary or other appropriate action against employees or investigating a reasonable suspicion that an employee has breached their employment obligations.

Access to Surveillance Data

The Managing Director is the sole release authority for surveillance data and information. For clarity, no party may access or review CCTV footage or other surveillance data collected by Ready Group without the express permission of the Managing Director.

If an individual believes they are improperly recorded on CCTV footage held by Ready Group (ie. not in accordance with this Policy) they can exercise their access rights under privacy or freedom of information legislation, by asking to view or have a copy of the footage. They may exercise this right themselves, or through a legal representative.

All requests for access, with the exception of law enforcement agencies, for CCTV footage must be made in writing and clearly outline the reason for access to the Managing Director of Ready Group.

Installation of Surveillance Devices

Any installations of surveillance devices must be in-accordance with the WS Act, Surveillance Devices Act 2007 (NSW) and this Policy.

Policy Breach

Any employee or contractor found to be in breach of this Policy will be subject to appropriate disciplinary action, up to and including dismissal.

Definitions

Surveillance: of an employee means surveillance of an employee by any of the following means (s3 WS Act): (a) camera surveillance, which is surveillance by means of a camera that monitors or records visual images of activities on premises or in any other place, (b) 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), (c) 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 a Global Positioning System tracking device).

Surveillance information: means information obtained, recorded, monitored or observed as a consequence of surveillance of an employee.

Covert surveillance: means surveillance of an employee while at work for an employer carried out or caused to be carried out by the employer and not carried out in compliance with the requirements of Part 2 of the WS Act.

Workplace: means premises, or any other place, where members, employees and contractors work, or any part of such premises or place.

Key Responsibilities

Overall responsibility of this Policy is with the Managing Director.

Document Control
Version: 1.0
Dated: 16/10/2023
Position: Managing Director
UNCONTROLLED WHEN PRINTED