1. POLICY

This policy guides how Family Emergency Accommodation Townsville (FEAT) implements, monitors and uses workplace surveillance. This Policy enhances the safety and security of workers, clients, visitors and our assets, and maintains compliance with organisational policies and the Information Privacy Act 2009 (QLD) ("IP Act") and Information Privacy Principles (IPP's). As a contract provider to government, our organisation is also required to follow guidelines issued by the Office of the Information Commissioner (QLD) in relation to camera surveillance.

FEAT does not operate or control any camera surveillance at the properties which we manage. Any such surveillance conducted is the responsibility of the relevant body corporate or building owners.

When our workers are attending our properties, we do not expect our clients to utilise surveillance inappropriately or in a manner which breaches the privacy or dignity of individuals and will address any concerns raised with us.

This Policy applies to all staff, contractors, clients and visitors at FEAT premises and applies to all premises owned or leased by the organisation, and the use of any external or third-party contractors involved in surveillance.

2. DEFINITIONS

Personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

3. PRINCIPLES

Workplace surveillance at FEAT adheres to the following principles:

- Compliance with legislated requirements as outlined in this Policy and our Privacy Policy;
- Respect for privacy and dignity, avoiding undue intrusion without justifiable reasons;
- Informing workers about the purpose, nature and scope of surveillance activities;
- Secure storage of images, ensuring access is restricted to authorised personnel;
- Ensuring individuals are aware that they may be recorded, e.g. through signage;
- Ensuring there is clear legal basis for the access or release of images to any person;
- Providing details of who to contact and how an individual can lodge a complaint; and
- Recognition of an individual's right to lodge a complaint concerning our workplace surveillance activities.

4. TYPES OF WORKPLACE SURVEILLANCE

Surveillance used at FEAT occurs in several forms, including:

- **Closed Circuit Television (CCTV) Cameras**: installed in various locations throughout the workplace including car park, front and rear building entry, Boardroom and Rooms 1 – 4.
- **Organisational Systems**: We scan and monitor appropriate use of organisational computers, networks, internet, phones and emails and all devices.

Cameras will not be installed in areas where there is a reasonable expectation of privacy, including bathrooms or changing rooms.

5. NOTIFICATION AND CONSENT

Staff Notification: Staff are informed of our workplace surveillance methods via this Policy and provide their consent to such surveillance via their employment contract.

Contractor Notification: Contractors are notified via the Contractor Management Handbook and provide their consent to such surveillance via acknowledgement of the Handbook.

Visitor Notification: Signs are displayed in areas under camera surveillance to notify any visitors to our premises of the presence of cameras. This Policy is publicly available on our website, as is our Privacy Policy.

Consent: By entering the workplace, staff, contractors, clients and visitors acknowledge and consent to being monitored by surveillance systems in areas where such surveillance is in place.

6. USE OF SURVEILLANCE DATA BY FEAT

Our organisation uses workplace surveillance to:

- protect organisational assets, intellectual property and confidential information;
- provide an enhanced level of security for our workers, clients, visitors and assets;
- deter and/or detect unlawful activity on its premises, such as with a CCTV system;
- prevent and investigate allegations of misconduct or unlawful behaviours not limited to violence, bullying, harassment, sexual harassment, discrimination, theft, fraud;
- ensure compliance with work, health and safety duties, by being able to track the whereabouts of our workers when conducting outreach work;
- facilitate an effective response to requests for access to camera surveillance data; and
- ensure compliance with our organisational policies and procedures.

7. CAMERA SURVEILLANCE DATA HANDLING

In operating workplace surveillance, FEAT will capture personal information as camera footage (data) which may discern identifiable features of an individual.

To maintain confidentiality, integrity and availability of the surveillance data, the following procedures are in place:

Storage and Retention: All routine camera surveillance data will be stored securely for a maximum of 30 days. After this period, data will be overwritten, unless the surveillance records are required to be maintained for any purpose as outlined in this Policy, in which case they will be retained until the conclusion of the business.

Where an ongoing record is required to be kept, the contents of the data will be transcribed into a written format.

Where data is provided for law enforcement investigations, it must be retained for a period of 12 months after the recording is provided to the agency. If there is any need to retain the documentation for longer, it will be transcribed into written format.

Access and Security: Surveillance data can only be accessed live from FEAT premises or via the cloud. Only the General Manager and Finance & Office Manager and any appointed investigator have authorised access to surveillance data via encrypted passwords and two-step verification. Access to surveillance data is restricted and is not accessible by unauthorised staff, nor by clients or visitors.

Cloud-based Computing: Information kept on FEAT's computer systems, including camera surveillance data is kept in the cloud, which operates from Australia. When transferring personal information outside of Australia, FEAT will ensure:

- The individual agrees to the transfer;
- The transfer is authorised or required under a law; or
- FEAT is satisfied on reasonable grounds that the transfer is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; or

  Two or more of the following conditions apply—

- FEAT reasonably believes that the recipient of the personal information is subject to a law, binding scheme or contract that effectively upholds principles for the fair handling of personal information that are substantially similar to the IPPs or, if the agency is a health agency, the NPPs;
- the transfer is necessary for the performance of FEAT's functions in relation to the individual;
- the transfer is for the benefit of the individual, but it is not practicable to seek the agreement of the individual, and if it were practicable to seek the agreement of the individual, the individual would be likely to give the agreement;
- FEAT has taken reasonable steps to ensure that the personal information it transfers will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the IPPs or, if the agency is a health agency, the NPPs, i.e. by entering into a contract with the cloud services vendor which provides for the same level of privacy protections as are required in Australia.

Audit Trail: The Finance & Office Manager maintains the *Camera Surveillance Register*, which is an audit trail of who accesses surveillance data, including the time, date and reason for access. It also includes details of any necessary release of camera surveillance data. Only those authorised under this Policy have access to this Register.

In addition to the above register, any files (i.e., evidence, correspondence) relating to a request or complaint will be kept in secure files only accessible by authorised officers. These files will be destroyed in accordance with our retention and disposal requirements.

8. USE AND DISCLOSURE OF CAMERA SURVEILLANCE DATA

Use: The use of camera data may include live monitoring, reviewing footage after an incident, examining data as evidence, archiving data for later use, making copies, or manipulating it.

Restricted Purposes: The use of surveillance data will be limited to the purposes outlined within this Policy and will not be used for other purposes unless required by law or with the explicit consent of the individuals recorded.

Requests from Law Enforcement or Other Agencies: On a case-by-case basis, as approved by the General Manager, we may release surveillance data to law enforcement agencies such as QLD Police Service, Crime & Misconduct Commission, Corrective Services, Work, Health & Safety and other law enforcement or appropriate agencies (e.g. Department of Housing) if the personal information is 'reasonably necessary' for a law enforcement or agency activity, or where we receive a subpoena to do so.

Individuals are advised that in the above disclosures, FEAT is not required to notify the individual of such release. Once the data is released to the authorities, it may become a public record, and if an individual wishes to access the data, they must do so via the relevant authority.

9. REQUESTING ACCESS TO VIEW OR RECEIVE SURVEILLANCE DATA – THIRD PARTIES

Any person requesting (the requestor) to view or receive a recording of surveillance data must make their request in writing marked Private & Confidential to the General Manager, at the address outlined further below.

As outlined in this Policy, requestors are advised that routine surveillance data will only be retained for a period of 30 days. If such data has not been withheld as part of an investigation or as required by law, such data will not exist beyond 30 days of being captured. Where we are required to keep the data for longer, we will do so as outlined in this Policy.

To assist us in understanding what the request relates to and whether the request aligns with the requirements of this Policy; and that access is permitted under privacy laws, we ask for the following information to be provided:

- Full Name of the requestor
- Contact details of the requestor (address and telephone)
- Sighting of Photo ID, or where this is not possible provision of a Certified Copy of Photo ID (which will be destroyed at completion of the request)
- Reason/s for the request, and whether the request is to view live data or to receive a copy of recorded data
- Any legal basis for the request, and how the surveillance data will be used
- The exact (or approximate) time and date the data was captured
- Any evidence (if applicable) available to support the request

Upon receiving a written request as outlined above, the following will occur:

- The requestor will receive written acknowledgement of the request within three (3) business days, together with a copy of this Policy and the Privacy Policy.
- An investigation into the request will be undertaken, determining the basis of the request and determination as to whether FEAT can allow access.
- The requestor will receive a written outcome as to whether their request is granted, within 30 days of the written complaint being received by FEAT (or earlier if deemed necessary by FEAT), and under any specific circumstances.
- Where access is granted to view live surveillance data, this will only occur under supervised conditions, meaning that the viewing will be managed and supervised at all times by an authorised officer. In such cases the requestor is not permitted to record, film or photograph any images.

Where access **is granted** for the release of surveillance data, this will preferably be provided in person to the requestor, with the requestor being required to sign and acknowledge receipt of the data and their responsibilities in relation to the data. A signed copy is to be provided to the individual.

Where access **is not granted** to either view or receive recorded data, the reasons for the refusal will be outlined in the written outcome. If the individual is not satisfied with the response, they are within their rights to escalate the matter to the Privacy Commissioner or Office of Information Commission, as relevant.

The General Manager (or authorised delegate) must ensure that the details of the request are entered into the *Camera Surveillance Register*.

10. ACCESS TO VIEW OR RECEIVE SURVEILLANCE DATA – EMPLOYEES

Bearing in mind the nature of the work which our employees undertake, we recognise that in situations which have resulted in a threat to the life, health, safety or welfare of our workers, that we may expedite the process of allowing access to viewing surveillance data in the interests of the individuals concerned, and/or the investigation process.

Authorised officers remain responsible for assessing and determining the appropriate actions to be taken, and for ensuring these are approved actions and are documented in the *Camera Surveillance Register*.

However, where an employee wishes to receive a recording of surveillance data, they must follow the procedure outlined in the section above.

In the instance where FEAT (or an appointed investigator) is conducting an investigation into disciplinary or related workplace matters, and where such data is relied upon as part of disciplinary action or the investigation, the person/s subject to discipline or investigation will be offered the opportunity to view the data under supervised conditions.

If any other person requests access to surveillance data, where the data only shows that individual,

and the General Manager considers that the release of such information is consistent with the objectives and requirements of this Policy, then the individual may be allowed to view the data in a supervised sitting. No individual may record, photograph or video the information under any circumstances.

If there are other identifiable people in the footage, it may not be possible to allow the data to be viewed unless the data can be securely redacted or images pixelated to protect the identity of those persons, or without the explicit consent of the other persons who are identifiable in the data. In these circumstances, any costs arising from having the data redacted will be borne by the requestor.

11. MAKING A COMPLAINT TO FEAT

Any individual who believes their privacy may have been breached by FEAT in regard to the collection, storage and security, use or disclosure of workplace surveillance data, can lodge a written privacy complaint under this Policy marked ***Private & Confidential*** to:

General Manager
Family Emergency Accommodation Townsville
9 Carlton Street
Kirwan
QLD 4817

Or via email: generalmanager@feat.org.au

To assist us in understanding what the complaint relates to and how we might be able to resolve the complaint, we ask for the following information to be provided:

- Full Name of complainant
- Contact details of the complainant (address and telephone)
- Certified Copy of Complainant Photo ID (which will be destroyed at completion of complaint)
- Brief description of the complaint
- Legal or other basis as to why the complaint is being made
- Any evidence available to support the complaint
- Outcome sought by the complainant

Please note, that it may be necessary for the General Manager (or delegate) to make contact with the complainant to gather additional information or to ascertain particulars of the complaint.

Upon receiving a written complaint as outlined above, the following will occur:

- The complainant will receive written acknowledgement of the complaint within three (3) business days, together with a copy of this Policy and the Privacy Policy.
- An investigation into the complaint will be undertaken, determining the basis of the complaint and confirming whether breaches to policy or legislation have occurred.
- The complainant will receive a written outcome of the complaint within 30 days of the complaint being received by FEAT (or earlier if deemed necessary by FEAT).

The General Manager (or their authorised delegate) must ensure that the details of the complaint are entered into the *Camera Surveillance Register*.

It must be recognised that while anonymous complaints may be made and will be investigated to the extent possible, FEAT will may be able to investigate and determine.

12. MAKING A COMPLAINT ABOUT FEAT

If any individual believes that FEAT has violated their privacy via workplace surveillance activities, they can file a complaint with the Privacy Commissioner or Office of the Information Commissioner (QLD). However, we request that complaints be directed to us initially to allow us the opportunity to address them.

13. BREACH OF POLICY

Any unauthorized access, use or disclosure of surveillance data may result in disciplinary action, up to and including termination.

14. AVAILABILITY OF THE POLICY

This policy is available on the FEAT Company website (http://www.FEAT.com.au).
Alternatively, you can request a copy in person, by phone (07) 4772 1450 or email, reception@feat.org.au and we will provide a hardcopy or send it to you by your preferred method (email or physical mail).

Other related policies and procedures

Related Policies	• Privacy Policy • Work Health & Safety Policy
Forms of other organisational documents	• Camera Surveillance Register • Manager Guidelines (Internal Document)

Review Processes

Policy review frequency:	**Responsibility for review:**
Two-year review or as required	Manager
Review Process: Staff may submit amendments to the Manager for consideration at any time. The Manager will consider the amendments and update the Policy as required. The Management Committee will ratify changes to the Policy.	
Documentation and Communication: the Manager will ensure redundant versions of this policy are removed from the electronic and paper-based files and that staff and all other relevant people are advised of the updates through training/staff meetings.	