Newcastle Coal
INFRASTRUCTURE GROUP

Privacy

Policy

DOCUMENT NO:	PCUL.POL.05.01
NEXT REVIEW DATE:	01-09-2024
REVIEW FREQUENCY:	3 years
DOCUMENT OWNER:	Lauren Ross
DOCUMENT APPROVER:	Chief Executive Officer

KEY ELEMENTS

- This Policy & Procedure applies to all employees of NCIG, as well as contractors, consultants, and visitors.
- Decisions in relation to the collection, use, disclosure, and protection of Personal Information must be made in line with the Australian Privacy Principles.
- Individuals can make a complaint about breaches to this Policy & Procedure to the People and Culture Manager, and/ or the Australian Information Commissioner.
- Employees, contractors, consultants, and visitors will also be subject to workplace surveillance.

TABLE OF CONTENTS

1. PURPOSE

To describe processes for the collection, use, disclosure and protection of personal information and workplace surveillance monitoring conducted by the Newcastle Coal Infrastructure Group Pty Ltd ('**NCIG**'). This Procedure is based on the Australian Privacy Principles of the Privacy Act 1988 (Cth), and the Workplace Surveillance Act 2005 (NSW).

2. SCOPE

This Policy and Procedure applies to all NCIG employees and includes all operations managed by NCIG. Contractors, consultants and visitors are also expected to comply with this Policy and Procedure.

3. ROLES AND RESPONSIBILITIES

3.1 Executive Leadership Team

- Actively promote and support the implementation of this Policy & Procedure;
- Ensure that this Policy & Procedure is aligned with relevant NCIG policies and values;
- Monitor the effective implementation of this Policy & Procedure;
- Treat any breach of this Policy & Procedure in a fair and consistent manner.

3.2 People and Culture Team

- Update this Policy & Procedure in line with review dates;
- Ensure the adequacy of this Policy & Procedure and to ensure it meets legislative requirements;
- Ensure this Policy & Procedure is aligned with relevant NCIG policies and kept up to date with relevant industry best practice;
- Monitor the effective implementation of this Policy & Procedure; and
- Disperse this Policy & Procedure to all workers and encourage questions and feedback.

3.3 Leader

- Ensure this Policy & Procedure is communicated with their teams;
- Ensure any issues or queries raised by an employee in relation to this Policy & Procedure are dealt with promptly and in a fair and consistent manner; and
- Know who to escalate a request for Personal and/ or Sensitive Information to and instruct their team accordingly.

3.4 Employee

- Follow Policy & Procedures as outlined in this Policy & Procedure;
- Recognise what is classified as Personal and/ or Sensitive Information; and
- Be accountable for the way in which you escalate a request for Personal and/ or Sensitive Information from an external or internal party.

4. POLICY & PROCEDURE

4.1 Personal Information

The Privacy Act regulates personal information of individuals. '*Personal information*' is any information, or an opinion, about an identifiable person or an individual who is reasonably identifiable. This definition includes whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not. 'Recorded' covers not only traditional means of data storage such as paper files but also electronic records.
Common examples are an individual's name, signature, address, telephone number, email address, date of birth, medical records, bank account details, employment details and commentary or opinion about an identified person.

By law, organisations are required to have in place systems relating to the collection, storage, use and disclosure and handling of personal information that reflect due regard for the protection of personal information. NCIG has established practices for collecting and dealing with personal informationand will continue to maintain those standards to minimise the risk of misuse, loss and unauthorised access, modification, or disclosure of such information.

4.2 Collection of Personal Information and Sensitive Information

If NCIG collects Personal Information:

- It will do so only when the information is reasonably necessary for one or more functions or activities of NCIG;
- It will be collected using lawful and fair means and not in an unreasonably intrusive way;
- The information will be collected directly from the individual concerned where it is reasonable and practicable to do so; and
- The information will only be collected from a third party where it is not practicable to collect the information directly from the individual.

Unless the collection of Sensitive Information is required or permitted by law, NCIG will not collect Sensitive Information unless it has obtained the individual's consent to its collection. '*Sensitive Information*' is defined in the Privacy Act to mean information or an opinion relating to an individual's ethnic or racial origin, political opinions, membership of a political association, religious beliefs, professional or trade union membership, criminal record, health, genetic information and biometric information or sexual orientation. '*Health information*' is defined broadly to include information or an opinion about the health or a disability of an individual.

NCIG will at, before the time, or as soon as practicable after collecting Personal Information from an individual, take all reasonable steps to ensure that the individual is notified or made aware of:

- NCIG's identity and contact details;
- The purpose for which NCIG is collecting Personal Information;
- The identity of other entities or persons to whom NCIG usually discloses Personal Information to;
- That NCIG's Privacy Policy & Procedure contains information about how the individual may complain about a breach of the Australian Privacy Principles and how NCIG will deal with a complaint; and
- Whether NCIG is likely to disclose Personal Information to overseas recipients and if so, the countries in which such recipients are likely to be located and if practicable, to specify those countries.

4.3 Use and Disclosure of Personal Information

NCIG will not disclose or use any Personal Information about an individual for a purpose (the secondary purpose) other than the primary purpose of the collection of the information unless:

- The secondary purpose is related to the primary purpose for which the information was collected, and, if the Personal Information is Sensitive Information, directly related to the primary purpose of collection, and the individual would reasonably expect NCIG to use or disclose the information for the secondary purpose;
- The use or disclosure is required or authorised by or under law, or a court/tribunal order;
- It is unreasonable or impracticable to obtain the individual's consent to the use or disclosure and there are reasonable grounds to believe that disclosure is necessary to prevent or lessen a serious and imminent threat to the life, health or safety of the individual concerned or a serious threat to public health or public safety;
- NCIG has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to NCIG's functions or activities has been, is being or may be engaged in and NCIG reasonably believes that the disclosure or use is reasonably necessary in order for NCIG to take appropriate action in relation to the matter;

- NCIG reasonably believes that the use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been missing and the use or disclosure complies with any applicable rules made by the Privacy Commissioner;
- The use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim or for the purposes of a confidential alternative dispute resolution process;
- The disclosure or use is reasonably necessary to allow an enforcement body to enforce laws, protect the public revenue, prevent serious improper conduct, or prepare or conduct legal proceedings; or
- The individual has consented to the use or disclosure.

Where NCIG intends to disclose Personal Information to another person or organisation, the individuals concerned will be made aware at the time of collection that their Personal Information will be disclosed and to whom.

4.4 Collected Data Security

NCIG will take all reasonable steps to protect Personal Information (including Sensitive Information and Health Information) in its possession from misuse, interference, loss, unauthorised access, modification, or disclosure, including by:

- Storing paper or electronic documents containing Personal Information in secure hardware and software systems;
- Maintaining physical and software protection over paper and electronic data stores and premises, by way of locks and security systems;
- Maintaining computer and network security via the use of firewalls, email and internet monitoring systems, as well as security features that involve user identification and passwords that control access.
- Ensuring that Personal Information is kept no longer than is necessary for the purposes for which it may lawfully be used;
- Ensuring that Personal Information is disposed of securely and in accordance with any other requirements for the retention and disposal of such information;
- Ensuring that where Personal Information is to be destroyed by an outside organisation, reasonable safeguards protect the information and prevent unauthorised access, disclosure, use, loss or modification;
- Limiting access to Personal Information to authorised persons only; and
- Training its employees on their obligations with respect to Personal Information

During the course of operations, photographic pictures may be taken, including individual pictures. Persons not wishing their individual photographs to be taken and/or published, should advise the photographer and People and Culture Manager in writing on commencement of employment.

4.5 Access and Correction

Where NCIG holds Personal Information about an individual, the individual may, upon request,access that information unless:

- the request is frivolous or vexatious; or
- it would have an unreasonable impact on the privacy of others; or
- there is an exemption under the Privacy Act 1988 (Cth) which allows NCIG to not disclose the information.

In the event of NCIG being advised that Personal Information held about an individual is considered by that individual not to be accurate, complete, or up to date, then NCIG will take reasonable steps to correct the information. Individuals are encouraged to contact their manager if they believe the information held by NCIG about them is not accurate, complete, or up to date.

If NCIG refuse to correct the Personal Information as requested by the individual, NCIG will give written notice that sets out:

- The reasons for the refusal, except to the extent that it would be unreasonable to refuse;
- The mechanisms available to complain about the refusal; and
- Any other matter prescribed by the regulations.

4.6 Exceptions

Certain acts and practices of an organisation in relation to the privacy of Personal Information are exempt from privacy legislation. Staff or employee records (the terms and conditions of employment of the employee, salary or wages, and performance or conduct etc) are exempt from privacy legislation.

NCIG will provide appropriate security measures for the handling, storing and disposal of such records in accordance with relevant legislation.

4.7 Workplace Surveillance

NCIG conducts continuous workplace computer and camera surveillance on an ongoing basis, in accordance with the NCIG Internet/Email Policy and the Workplace Surveillance Act 2005 (NSW).

NCIG monitors and records usage of electronic systems and equipment and accesses information contained on our electronic systems (this includes but is not limited to):

- Emails;
- Internet use;
- Documents created or accessed;
- Telephone logs; and
- Satellite navigation systems.

Camera surveillance is carried out by means of video cameras to monitor the safety and security of NCIG's property, assets, and resources.
The records produced as a result of this surveillance may be used by NCIG for various purposes including investigating alleged misconduct, disciplinary action and any other legitimate business purpose.
Covert surveillance will only be carried out in accordance with the Workplace Surveillance Act 2005 (NSW) in circumstances where NCIG believes there may be unlawful activity.

The records produced as a result of any covert surveillance will only be used or disclosed by NCIG for a "relevant purpose" as provided in the Workplace Surveillance Act. This includes for example, use or disclosure for a purpose that is directly or indirectly related to: establishing whether or not an employee is involved in unlawful activity while at work; taking disciplinary action or legal proceedings against an employee as a consequence of any alleged unlawful activity while at work; establishing security arrangements or other measures to prevent or minimise the opportunity for unlawful activity while at work.

4.8 Breach

In the event that an individual believes his or her privacy has been breached, they should make a written complaint to the People and Culture Manager. The People and Culture Manager will then notify the Company Secretary and commence proceedings for an internal review.

A Review Panel, comprising the Chief Executive Officer and either of the Company Secretary or the People and Culture Manager (together with any other persons they deem as being appropriate) will conduct an internal review of the alleged breach.

Once a review has been completed, NCIG will notify the applicant of the following:

- The findings of the review;
- The reasons for the finding;
- The action proposed to be taken;
- The reasons for the proposed action; and
- The applicant's right to have the findings and reasons for the findings reviewed by the australian information commissioner.

The Australian Information Commissioner receives complaints under the Act. Complaints can be made:

- Online http://www.oaic.gov.au/privacy/making-a-privacy-complaint
- By telephone 1300 363 992
- By fax +61 2 9284 9666
- In writing
    - Office of the Australian Information Commissioner
      GPO Box 5218
      Sydney NSW 2001
    - Office of the Australian Information Commissioner
      GPO Box 2999
      Canberra ACT 2601

In the event that an individual believes there has been a breach in privacy and it is not appropriate to make the complaint to the People and Culture Manager, additional reporting avenues are available under the NCIG Whistleblowing Policy.

5. REFERENCES

- Australian Privacy Principles of the Privacy Act 1988 (Cth)
- Workplace Surveillance Act 2005 (NSW)
- NCIG Internet/ Email Policy
- NCIG Whistleblowing Policy

6. REVISION HISTORY

DATE	REVISION NO.	DESCRIPTION OF CHANGE	PERSONS INVOLVED
18/05/2009	1	Initial NCIG Document	J Thomas
28/07/2009	2	Policy reviewed by J Thomas/ Technicians	J Thomas/ Technicians
30/04/2013	3	Formatting updated only	A Hill
21/10/2016	4	Formatting updated using Style Guide	Kate Eliza David
25/5/2018	5	Compliance updates	Casey Samuels / A Johansen
6/11/2019	6	Review and formatting updates	Casey Samuels
02/09/2021	7	Policy Review New Template Updated Roles and Responsibilities References added to NCIG Whistle Blowing policy	L Ross / N Payne