Bringing spaces to life.

Privacy Policy

South Australia.
10 Marlow Road
Keswick 5035

New South Wales.
Unit 4, 42-50 Violet Street
Revesby 2212

Queensland.
Unit 6, 2 Aliciajay Circuit
Luscombe 4207

Victoria.
26 Tarmac Way
Pakenham 3810

Big Screen Video

T - 1300 244 727
info@bigscreenvideo.com.au
bigscreenvideo.com.au

1. Introduction

In the performance of our Company's business activities, we are required to collect, hold and use and/or disclose personal information relating to individuals including our employees, customers, contractors and suppliers.

This document sets out our Policy in relation to the protection of personal information as defined under the Privacy Act 1988 (Cth) "the Act", which includes the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) and the Australian Privacy Principles "APP". The APPs regulate the handling of personal information.

2. Scope

This policy applies to all employees, customers, contractors and suppliers and other workers engaged by the Company and who have access to personal information while performing their duties.

3. Definitions

3.1 What is personal information?

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 material form or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.

3.2 What is not personal information?

An employee record is exempt from the APPs. However, employees (such as those engaged in a management or human resource capacity) will have access to employee records and must ensure that the information is handled confidentially and for a proper purpose only. Employee records are only permitted to be collected, used and disclosed where the act of doing so is directly related to the employment relationship only.

4. Information Collected and Held

The Company only collects and holds information that is necessary. If this information contains sensitive information (as defined below) we will also ensure that we have obtained consent to collect this information.

The information we collect may depend on the individual's relationship with the Company. For example:

- Candidates – if a candidate is seeking employment with the Company, we may collect and hold information including name, address, email address, contact numbers, drivers license, employment history, references, resume, medical history, emergency contact, taxation details, qualifications and payment details.
- Customers – the Company may collect and hold information including name, address, email address, contact number, identification, and other sensitive information.
- Supplier – the Company may collect and hold information about name, address, email address, contact number, business records, billing information and information about goods and services supplied by the supplier.
- Referee – if a person is a referee of a candidate being considered by the Company for employment, we may collect and hold name, contact details, current employment information and professional opinion of the candidate.
- Sensitive information - the Company will only collect sensitive information where an individual consent and the information is reasonably necessary for one or more of the Company's functions or activities. Sensitive information includes, but is not limited to, union membership, criminal record, health information, philosophical beliefs.

4.1 How Information Is Collected and Held

The Company, and employees acting on behalf of our Company, must only collect personal information by lawful and fair means.

The Company collects personal information in several different ways, including:

- Through application forms for employment
- By email, phone or in person
- Through transactions

- Through our Company website
- Through lawful surveillance, such as security cameras
- By technology that is used to support communications
- Through publicly available information sources
- Through direct marketing database providers

Personal Information collected through publicly available sources will be managed in accordance with the APPS and as soon as practicable, the Company will either notify the individual or otherwise take all reasonable steps to ensure that the individual is made aware of the following:

- That the Company has collected personal information from someone other than the individual, if the individual is unaware of the information collected.
- The identity and contact details of the Company.
- That collection of personal information is required by Australian law, if it is.
- The purpose for which the Company collects the personal information.
- The consequences if the Company does not collect some or all of the personal information.
- Any other third party to which the Company may disclose the personal information collected by the Company.
- The Company's Privacy Policy contains information about how and individual may access, seek correction or complain about a breach of the APPS; and
- Whether the Company is likely to disclose personal information to overseas recipients, and the countries in which those recipients are likely to be located.

Unsolicited personal information is personal information that the Company receives which it did not solicit. Unless the Company determines that it could have collected the personal information in line with the APPs or the information is contained within a Commonwealth record, it must destroy the information to ensure it is de-identified unless the Company determines that it is acceptable for the Company to have collected the personal information.

5. Use and Disclosure of Personal Information

The main purposes for which the Company pay use or disclose personal information may include:

- Recruitment
- Training and events
- Customer service management
- Surveys and general research
- Business relationship management

The Company may also collect, hold and use and/or disclose personal information in an individual consents or if required or authorised under law.

6. Direct Marketing

The Company may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing. For example, advising a customer about new goods and/or services being offered by the Company.

The Company may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose; and

An individual can opt out of receiving direct marketing communications from the Company by contacting the Privacy Officer in writing or if permissible, accessing the Company's website and unsubscribing appropriately.

7. Disclosure of Personal Information

The Company may disclose personal information for any of the purposes for which it was collected, as indicated under the relevant clauses above, or where it is under a legal duty to do so.

Disclosure will usually be internally and to related entities or to third parties such as contracted service suppliers.

If an employee discloses personal information to a third party in accordance with this policy, the employee must take steps as are reasonable in the circumstances to ensure that the third party does not breach the APPS in relation to the information.

8. Access to Personal Information

Individuals may request access to the personal information that is held by the Company by putting the request in writing and sending it to the Chief Operating Officer. The Company will respond to any request within a reasonable period, and a charge may apply for giving access to the personal information where the Company incurs any unreasonable cost in providing the personal information.

There are certain circumstances in which the Company may refuse access to personal information. In these circumstances, the Company will provide written notice to the individual which sets out the reasons for the refusal and the mechanisms available to make a complaint.

9. Correction of personal information

If the information held by the Company is inaccurate, out of date, incomplete, irrelevant or misleading, it must take steps as are necessary to correct the information.

If an individual makes a request in writing to correct the information, the Company must take reasonable steps to correct the information and respond within a reasonable time.

There are certain circumstances in which the Company may refuse to correct the personal information. In these situations the Company will give the individual written notice stating the reason for the refusal and the mechanisms available to make a complaint, as outlined in this Policy.

If the Company corrects personal information that has been previously supplied to a third party and an individual requests the Company to notify the third party of the correction, the Company will take all reasonable steps to do so, unless impracticable or unlawful to do so.

10. Integrity and Security of Personal Information

The Company will take steps to ensure that the personal information that it collects is accurate, up-to-date, and complete.

Employees must take all reasonable steps to protect the personal information from misuse, interference, loss and from unauthorised access, modification, or disclosure.

If the Company no longer needs the information for any purpose for which the information may be used or disclosed and the information is not contained in any Commonwealth record and the Company is not required by law to retain the information, it will take steps to ensure that it is destroy or de-identified.

11. Data Breaches and Notifiable Data Breaches

A 'Data Breach' occurs where personal information held by the Company is accessed by, or is disclosed to, an unauthorised person, or is lost. An example of a Data Breach may include: Illegal hacking;

- Lost or stolen laptops, phones, tablets or USB storage devices;
- Lost or stolen paper records or documents containing personal information;
- Employees mistakenly providing personal or payroll information to the wrong recipient;
- Unauthorised access to personal information by an employee;
- Employees providing confidential information to the Company's competitors;
- Credit card information lost from insecure files or stolen from garbage bins.

If you are aware of or reasonably suspect a Data Breach, you must report the actual or suspected Data Breach to the Chief Operating Officer as soon as reasonably practicable and not later than 24 hours after becoming aware of the actual or suspected Data Breach.

A ‘Notifiable Breach’ occurs where there is an actual Data Breach and:

- A reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual (including harm to their physical or mental well-being, financial loss, or damage to their reputation); or
- In the case of loss (i.e. leaving an unsecure laptop containing personal information on a bus), unauthorised access or disclosure of personal information is likely to occur as a result of the Data Breach, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual (including harm to their physical or mental well-being, financial loss, or damage to their reputation).

A Notifiable Data Breach does not include a Data Breach where the Company has been successful in preventing the likely risk of serious harm by taking remedial action.

Notification – Subject to any restriction under the Act, if the Company is aware of a Notifiable Data Breach, the Company will, as soon as practicable, prepare a statement outlining details of the breach and notify the individual whose personal information was part of the Data Breach and notify the Office of the Australian Information Commissioner.

12. Anonymity and Pseudonymity

Individuals have the option of not identifying themself or using a pseudonym when dealing with the Company in relation to a particular matter. However, this does not apply where the Company is required or authorised to do so by law or where it is impracticable for the Company to deal with individuals who have not identified themselves or who have used a pseudonym.

In some cases, the Company may not be able to respond to the request or provide goods or services where the individual does not provide their personal information when requested.

13. Complaints

Individuals have a right to complain about the Company's handling of personal information if the individual believes the Company has breached the APPs.

Individuals should direct their complaints to the Chief Operating Officer in writing in the first instance. The Company will provide a response within a reasonable period.

Individuals who are dissatisfied with the Company's response to a complaint, may refer the complaint to the Officer of the Australian Information Commissioner.

14. Breach of this Policy

Employees deemed to have breached this policy may be subject to formal disciplinary action.

Revision History							
Version	**Approved By**	**Approval Date**	**Effective Date**	**Reviewed By**	**Review Date**	**Sections Modified**	**Review Due**
1.0	Chief Operating Officer	13/04/2022	14/04/2022	HR Coordinator	24/10/2024	Addresses & Formatting	24/10/2025