

IBMS 25	Privacy Policy	
----------------	-----------------------	--

Overview

SKG, ICC and their related subsidiaries (known as “the Group”) recognises the importance of privacy and is committed to ensuring the privacy of information relevant to our company, our workers and our clients. The company is bound by the Privacy Act 1988 (as amended by Act No 74, 2012) and the National Privacy Principles.

This policy is to ensure that any service, information, or property deemed to belong to clients, physical, intellectual, and both written and electronic, is respected by all the Group workers and sub-contractors engaged for cleaning and security activities and that all parties are aware of this key requirement and always respect it. All workers and sub-contractors are inducted in the requirements of this policy and are charged with the responsibility of reporting to management any breaches that may occur during cleaning, security, maintenance or construction work. The policy forms the basis of the Group’s Code of Integrity Conduct for all workers and operates in conjunction with safety inductions. Workers are not allocated to contract sites until they have been fully inducted in both areas.

The Group prides itself on delivering a first-class quality service to all clients and to achieve this, it always relies on the informed responsibility of its workers and sub-contractors. As with safety issues, the company requires 100% compliance to this code and any deliberate breach or unreported accidental breach may result in instant dismissal and possible legal action if client property, physical and/or intellectual, is compromised.

Contract contents are divulged on a strictly “need to know basis” for the satisfactory implementation of the work, selection of teams, access to client premises, inductions and commencement of work. The details of contracts and any concessions are recorded in the company’s data base systems and hard copy records are retained in accordance with the standard and prevailing legislation.

Site workers are trained in the requirements of this policy and all other requirements via our safety and work procedures induction processes.

Training involves identifying the key requirements for respecting privacy and worker integrity of operations in all locations.

Key Requirements

- Workers must be inducted in the scope of work requirements as per contract specification for the site
- Respect client property in all formats – fixtures, furniture, ornaments, books, files, electronic equipment (data contents), consumables, stored items at sites and client employee property
- Handle property only as part of the required process and return it to its normal place e.g., books on bookshelves, magazines on foyer tables, cutlery to kitchen drawers
- Do not open files on desks, do not read open documents on desktops, do not read notes on calendars or white boards
- Do not turn on computer terminals, do not use a terminal if it has been left on by client employees, do not use machines e.g., copiers, faxes, printers, do not use client telephones or other devices
- Do not handle equipment accessories e.g., CD’s or memory sticks
- Do not use client consumables e.g., pens, pads, coffee, milk or food from kitchen areas
- Do not handle clothing that may be left by client employees
- Do not leave security doors unlocked or open while working on site
- Do not permit entry by unauthorised persons to the site
- Do not accept any deliveries to clients when client employees are not present
- Do not mention to others anything you have accidentally read, heard, or noticed
- Do not engage in any activity at sites that may cause any of the above situations to occur
- When sites are inspected, ensure cleaning or security issues are reported to supervisors and client representatives
- Report any breakage, damage, spillage, unnecessary or accidental usage of any of the above items to supervisors as soon as possible
- Report any unauthorised entry to supervisor and client
- Report any unauthorised deliveries to supervisor and client
- When reporting any of the above incidents to supervisors, ensure it is documented appropriately, recording time and circumstances of the incident
- Report breaches of these rules by other workers to supervisors immediately.

IBMS 25	Privacy Policy	
----------------	-----------------------	--

Exposure to Types of Information

The company collects information in the form of:

- Client requirements and contact details of client personnel where required by contract
- Worker information provided by the worker to assess their suitability for employment and for ongoing employment with the company.

Some of the types of information we collect are:

CLIENT INFORMATION

- Building plans and schedules of service requirements with details of relevant contact persons
- Client contact numbers for emergency contacts
- Security information.

WORKER INFORMATION

- Worker and prospective worker information, including the applicant's name and address, contact details such as phone numbers and email addresses, skills and employment history details
- A minimum of two reference checks from previous employers. Referees are nominated by the applicant
- Sensitive information including membership of a trade association and criminal records.

Workers on client sites may be exposed to the following:

- Documents left unattended on desks and other surfaces
- Storage areas left unlocked or required to be accessed for the purposes of cleaning
- Information displayed on computer screens
- Information displayed on workplace notice boards
- Sensitive conversations.

Use and Disclosure of Information

Company information supplied by clients during the course of contract delivery, and for workers during the recruitment and employment process, may include information of a personal or private nature. The information will only be distributed internally to the relevant managers that are involved in the contract or supervision of workers. The information will be treated in the strictest confidence.

The company enters into agreements to provide cleaning, security, maintenance or construction services which may result in select persons having access to client information. They shall only ever have access to the information for the purpose of providing the relevant services and they must not use this information for other purposes. To do so would be considered theft or fraudulent behaviour. Confidentiality and privacy statements are signed at contract commencement by relevant management personnel.

Once the contract or a worker of the company is terminated, information will be held and stored in a secure location for a period of six (6) months, after which time it will be shredded, or otherwise de-identified before we dispose of it.

The Group has a need to collect personal information about persons who are intending to be employed, and from existing workers who may need to update their information (e.g., Drivers Licence Renewal, change of address or change of employment status).

The information collected may also include Criminal and WWCC information as the Group places personnel in offices, government departments, schools, defence and health facilities.

The information collected may also be from other people including referees, previous employers, professional registration authorities and educational institutions, who may provide the Group with sensitive data that the Company may use to assess the suitability of candidates to be placed in or continue working in various positions.

The Group does not divulge any personal data collected unless it is required by clients to operate the business and outside of this, any information sought by government agencies must be requested via a subpoena.

IBMS 25	Privacy Policy	
-----------------------	------------------------------	--

Furthermore, all the Group workers sign a Code of Integrity Conduct that covers all aspects of the business including non-divulging of confidential information.

Access to Information in the Delivery of Services

Our goal is to take all reasonable steps to ensure that personal and private information on client premises remains secure and out of visual contact of workers. Clients are requested where practical to maintain a clear desk policy.

Workers are trained and instructed to not touch or clean desks or other surfaces where paperwork is present. Only surfaces free of paperwork will be cleaned unless otherwise instructed by the client.

Workers are trained not to read information on desks, computer screens or other information displayed in the workplace except for Emergency Signage and Instruction.

All workers are made aware of the Privacy Act and the consequences of a breach of the Act should they read or otherwise make note of information that is not the property of the company.

Personal Information Security

The company is committed to keeping all personal and private information secure. Only senior managers have access to this information.

Clients and workers may have access to our system for a planned audit of the Privacy Policy only in relation to the information held on their behalf.

Use, Access, Storage, Handling and Protection of Personal Data

As indicated above, the Group only uses personal data for what it is intended for – to provide evidence of suitability for employment or continued employment. Access to sensitive personal data is restricted to senior management and human resource workers and all materials stored on computers is only accessed via password entry (which is changed on a regular basis) while hard copies are stored in lockable filing cabinets. The head office is protected by a Security Alarm System.

Trans-border Data Flows

The Group does not use, rely on or request any overseas documents that workers, or potential workers, may offer in support of work application or continuation of employment, apart from Government issued identification documentation, such as a passport. The Group only accepts Australian documentation when requesting information from workers or potential workers and we do not provide any received information to overseas entities. Any overseas documents are either returned to the person concerned or shredded with their approval.

Complaint Handling Procedure and Compliance Monitoring Regime

The Group acknowledges that there will be occasions when workers, past and present, may lodge a complaint re their personal data held in the office and senior management will always respond to such complaints. If the complaint relates to the updating of personal data, the worker is informed that they must provide the updated information to continue working in their role.

If the complaint relates to information that may have been provided to the Group's clients, then the worker will be informed that such provision of information is a contractual requirement and must be provided. Examples of this situation may apply to accessing bank branches, secure government sites or schools.

At no time will the Group divulge personal data to anyone or any organisation other than for the purposes of retaining our contracts.

The Group management conducts regular checks of both hard copy documents and soft copy records to ensure that no breach of information security has occurred. The Group's Business Procedures "Document and Data Control Process", "Customer Property Process" and the "Quality Management Plan" provide the guiding principles for the way in which monitoring is carried out. This aspect of the business operations is subject to ISO auditing (full privacy provisions apply to the company's auditors).

Disposal/De-identification Practices

The Group responds in two ways for the disposal of personal data. For soft copies the record is deleted from the soft copy folder and a second check is made to ensure that further information is not stored elsewhere on the office server and if found, this will also be deleted.

IBMS 25	Privacy Policy	
----------------	-----------------------	--

For hard copy records of personal data, disposal activities involve shredding and removal to a secure and locked bin to be destroyed by a recognised Secure Document Disposal Company.

At any time, a client may request to review the information that is collected and shared with our workers or service providers on a need to know basis.

At termination of contract, or whenever required, clients are to contact the contract/operations manager to request any information that is stored on the client, be identified and where required, removed, subject to legislative requirements in relation to data retainment.

Management of Data Breaches, Malicious Attacks and Data Breach Response Plans

To date the Group has not had any breaches of security in respect of personal data being compromised or leaked inadvertently.

To respond to any potential future breaches, the Group senior management will take the following steps. For softcopy breaches, restore data in a different location on the Office Server and change passwords immediately. In the case of hard copy breaches, locks on filing cabinets will be changed and for both types of breaches, additional training of workers on the requirements of the Privacy Act will be carried out.

If the Group experiences malicious attacks or ransom demands, the system will be immediately shut down and the company's IT consultant called in to relocate data onto a different server with checks to determine the extent of confidential data that has been hacked or compromised. The necessary authorities will also be informed of the breach.

Unauthorised Disclosure of Internal or Client Data

The Group strictly prohibits the release or sharing of internal company data or client information to anyone who is not authorised to receive it.

This applies to all forms of data, including emails, documents, images, audio or video recordings, and any other information collected, stored, or transmitted in the course of the Group's operations.

If such information is accidentally or deliberately provided to an unauthorised party:

1. **Immediate Notification** – The worker must notify their supervisor and senior management immediately upon discovering the disclosure.
2. **Containment** – Where possible, recall or request secure deletion of the data and confirm the outcome in writing.
3. **Investigation** – Senior management will assess the scope of the disclosure, determine if it constitutes a reportable data breach under the Privacy Act 1988, and document findings.
4. **Corrective Actions** – May include re-training, process amendments, or disciplinary action in cases of negligence or misconduct.

Any unauthorised disclosure — deliberate or accidental — may result in disciplinary action up to and including termination of employment and may trigger legal obligations to notify affected individuals and the Office of the Australian Information Commissioner (OAIC).

Unauthorised Surveillance or Recording

Under the Surveillance Devices Act 2007 (NSW), it is illegal to record a private conversation without the consent of all parties involved, unless an exception applies. In most circumstances it is not only inappropriate to secretly record conversations in the workplace, but in some states within Australia, it may also be a criminal offence.

If the Employer becomes aware of any unauthorised recordings, each case will be dealt with on its own merits and action may be taken as appropriate. This may include disciplinary action, up to and including termination, and potentially criminal charges being laid.

For the avoidance of any doubt, the Group directs that it is essential that you disclose the fact that you are recording any meeting or conversation and seek consent from each participant prior to commencing any recordings, by audio, video or any other digital means.