IMS 25	Privacy Policy	SKG Services

Overview

SKG Services recognises the importance of privacy and is committed to ensuring the privacy of information pertinent to our company, our employees and our clients. The company is bound by the *Privacy Act* 1988 and the National Privacy Principles.

This policy is to ensure that any service, information, or property deemed to belong to clients - physical, intellectual- both written and electronic is respected by all SKG Services staff and sub-contractors engaged for cleaning, and security activities is aware of this key requirement and always respects it. All staff and sub-contractors are inducted in the requirements of this policy and are charged with the responsibility of reporting to management any breeches that may occur during cleaning, and security work. The policy forms the basis of SKG Services' Code of Integrity Conduct for cleaners, security officers, and management personnel, and operates in conjunction with safety inductions. Cleaners, and Security Officers are not allocated to contract sites until they have been fully inducted in both areas.

SKG Services 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 staff and sub-contractors. As with safety issues the company requires 100% compliance to this code and any deliberate breech or unreported accidental breech may result in instant dismissal and possible legal action if client property – physical and intellectual has been 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 etc are then recorded in the company's data base systems and hard copy records and retained in accordance with the standard and prevailing legislation.

Site staff is 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 staff integrity of operations in commercial, educational, health, public authority, recreation, retail, and residential locations.

Key requirements

- Inducted in the requirements for cleaning 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 staff property.
- Handle property only as part of the cleaning or security process and return it to its normal place – e.g., books on bookshelves, magazines on foyer tables, cutlery to kitchen draws,
- 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 staff, 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 staff,
- 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 staff is 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 respond fully regarding cleaning or security work issues to supervisors and client representatives,
- Report any breakage, damage, spillage or un-necessary movement 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,
- Reporting any of the above incidents to supervisors make a note in the cleaners or security report book – recording time and circumstances of the incident,
- Report breeches of these rules by other cleaners or security staff immediately to supervisors,

Exposure to Types of Information

The company collects information in the form of:

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

Some of the types of information we collect are as follows:

CLIENT INFORMATION

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

EMPLOYEE INFORMATION

- Employee and prospective employee 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 2 reference checks from previous employers. Referees are nominated by the applicant
- Sensitive information including membership of a trade association and criminal record

Cleaners 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

Use and Disclosure of Information

Company management supplied by clients during the course of contract delivery and for employees, during the recruitment and employment process, will use information of a personal or private nature provided to the company. The information will only be distributed internally to the relevant Managers that are involved in the contract or supervision of cleaners. The information will be treated in the strictest confidence.

The company enters into agreements to provide cleaning services which may result in particular persons having access to client information. They shall only ever have access to the information for the purpose of providing the cleaning services and 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 is terminated, or an employee the company, the 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.

SKG Services has a need to collect personal information about persons who are intending to be employed as cleaners or security staff from existing cleaners or guards who need to update new information (e.g., Drivers Licence Renewal, change of address or change of employment status).

The information collected may also include Criminal and WWCC details as SKG places cleaners and security guards in offices, schools, and health facilities.

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

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

Further all SKG Services' staff sign a Code of Integrity Conduct that covers all aspects of the business including non-devolving 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 cleaning personnel. Clients are requested where practical to maintain a clear desk policy.

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

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

Cleaners 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 your personal and private information secure. Only senior managers have access to this information.

Clients and employees 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 and Access and Storage, handling & protection

As indicated above SKG 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 resources staff 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 and the Office is protected by a Security Alarm System.

Trans-border data flows

SKG does not use or rely on or request any overseas documents that staff or potential staff may offer in support of work application or continuation of employment or other personal details. SKG accepts only Australian documentation when requesting information from staff or potential staff 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's handling procedure and Compliance monitoring regime

SKG Services acknowledges that there will be occasions when staff past and present may lodge a complaint re their personal data held in the office and senior management always responds to such complaints. If the complaints relate to updating of personal data the staff member is informed that they must provide the updated information to continue working as a cleaner, security officer, supervisor, manager, or administrator.

If the complaint relates to information that may have been provided to SKG's clients, then the staff member will be informed that such provision of information is in the contract requirements and must be provided. Examples of this situation may apply to cleaning bank branches or cleaning in schools.

At no time will SKG Services divulge personal data to anyone or any organisation other than for the purposes of retaining our contracts for cleaning, and security.

SKG Services management conducts regular checks of both hard copy documents and softcopy records to ensure that no breech of information security has occurred – SKG Services' Business Procedures – "Document and Records" and "Improvement" provide the guiding principals for the way in which monitoring is carried out and this aspect of the business operations is subject to ISO auditing (full privacy provisions apply to the company's auditors).

Disposal/de-identification practises

SKG Services responds in 2 ways for the disposal of personal data – for softcopy the record is deleted from the softcopy 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.

For hardcopy records of personal data all disposal activities involve shredding and removal to a security and locked bin to be removed by a recognised Sensitive Document Disposal Company.

Management of data breaches, malicious attacks & data breach response plans

To date SKG Services has not had any breeches of security in respect of personal data being compromised or leaked inadvertently.

To respond to any future breeches SKG Services senior management will take the following steps – for softcopy breeches – restore data in a different location on the Office Server, change passwords immediately. In the case of hardcopy breeches locks on filing cabinets will be changed and for both types of breeches additional training of staff on the requirements of the Privacy Act will be put in place.

If SKG Services experiences malicious attacks or ransom demands the system is immediately shutdown and the company's IT consultant is called in to relocate data onto a different server and checks to determine the extent of confidential data that has been hacked or compromised. The necessary authorities will also be informed of the breech.