SGH Policy for Handling Personal Information

1. Purpose

This policy sets out how SGH Ltd ("SGH") and SGH employees, must handle personal information in accordance with the *Privacy Act 1988* (Cth) (Privacy Act).

2. Scope

This Policy applies to all employees within SGH and its related bodies corporate. This Policy may be amended from time to time.

This policy must be read in conjunction with SGH's *Privacy Statement* available at: https://www.sghl.com.au/privacy-policy/.

3. Policy Statements

3.1 Privacy Compliance Officer

SGH has a Privacy Compliance Officer who oversees privacy compliance and to whom any queries or concerns should be directed.

The SGH Privacy Compliance Officer can be contacted at: The SGH Privacy Officer
SGH Ltd
Level 30, 175 Liverpool Street
Sydney NSW 2000 SGH_Privacy_Officer@sghl.com.au

3.2 What is Personal Information?

The Privacy Act defines personal information as *'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not.'* Essentially, personal information is information that identifies a person or from which an individual could reasonably be identified.

3.3 What types of personal information does SGH collect?

During the provision of SGH's products and services, SGH may collect personal information.

Generally, the kinds of personal information SGH collects are:

- Contact and identification information such as a name, company name, business street and postal address, business telephone and facsimile number, business email address or other personal contact details;
- Professional information including job responsibilities;
- Consumer credit information (in connection with an application for commercial credit and provided the collection of the consumer credit information is expressly consented to) including:
  - Identification information; and
  - Consumer credit liability information including information about credit accounts and credit limits.
  - Repayment history information;

- Information about credit defaults;
- Credit eligibility information, which is information about an individual that SGH obtains from a credit reporting body such as Equifax or Dunn & Bradstreet together with information SGH derives from such information based on its own analysis; and
- Any other information lawfully obtainable within the Australian credit reporting system.

In some circumstances SGH may also hold other personal information provided by an individual.

3.4 What are SGH's obligations under the Privacy Act?

SGH is required to handle personal information in accordance with the Privacy Act and the 13 Australian Privacy Principles (APPs) set out in the Privacy Act.

In order for SGH to comply with its obligations under the Privacy Act and the APPs, SGH's employees are required to collect, store, use and disclose personal information they may come into contact with, or have access to, in the course of their employment in accordance with the Privacy Act and the APPs.

The ways in which employees can do this are set out in more detail below with reference to each of the APPs.

3.5 Collection, Anonymity and Notification (APPs 1, 2, 3 and 5)

To the extent practicable, individuals should be given the option of remaining anonymous or using a pseudonym when dealing with SGH (e.g., when an individual is making general enquiries), unless it is required or authorised by law to deal with individuals who have identified themselves.

Where personal information is required to be collected:

- Personal information must only be collected where it is reasonably necessary for one or more of SGH's functions or activities and where collection is fair and lawful;
- Personal information should, as far as is reasonably practicable, be collected directly from the individual about whom it relates; and
- The individual, about whom SGH is collecting personal information, must be made aware of (either before or at the time of collection or as soon as reasonably practicable after collection):
  - SGH's privacy policy (which is available on SGH's website or must otherwise be provided to the individual in a suitable form) or otherwise of the information contained within it;
  - If the personal information is not being collected from the individual directly, that the personal information is being collected and from whom the personal information is being collected; and
  - Any law or court order under which the collection of the personal information is required.

3.6 Sensitive information

In most circumstances, SGH will not need to collect 'sensitive information' about an individual to whom it provides goods or services. Therefore, unless absolutely necessary in the circumstances, there should be no collection or retention by SGH of personal information about an individual's racial or ethnic origin, political opinions or associations, religious or philosophical beliefs or affiliations, trade or professional memberships, sexual orientation or practices, criminal record, health or genetic information.

SGH may undertake health and/or criminal record checks in relation to candidates for jobs within SGH. However, such information must only be collected and handled by relevant managers and Human Resources personnel and subsequently destroyed when it is no longer required.

In circumstances where SGH's first-aid and medical staff are required to collect health information about an individual in the event of a workplace incident, SGH must handle this information for the purposes of, and in accordance with, its occupational health and safety obligations.

3.7 Collection of unsolicited personal information (APP 4)

In the event personal information is received by SGH in circumstances where SGH did not solicit the collection of that information, an assessment must be made as to whether SGH could have otherwise collected that personal information in accordance with the Privacy Act (i.e., had the personal information been solicited by SGH) and:

- If a determination is made that SGH could have collected the personal information, the personal information must subsequently be handled in accordance with the APPs; or
- If a determination is made that SGH could not have collected the personal information, the personal information must be destroyed or otherwise de-identified (unless the information is contained in a Commonwealth record or it is otherwise unlawful or unreasonable to do so).

3.8 Use and Disclosure (APP 6)

Personal information must only be used or disclosed by SGH for the primary purpose for which it was collected. The purposes for which SGH collects personal information include:

- Internal research on SGH's website users' demographics, interests and behaviours to better understand and serve SGH's customers;
- Accounting, billing and other internal administrative purposes; and
- Identifying and informing individuals of products and services that may be of interest to them from SGH or selected third parties.

Personal information may also be used or disclosed by SGH for a 'secondary' purpose where:

- The individual would reasonably have expected their personal information to be used or disclosed for that secondary purpose and the secondary purpose is related to the primary purpose for which the personal information was originally collected;
- The individual consented to the secondary use or disclosure;
- The use or disclosure is required or authorised by law; or
- A prescribed public interest exception applies under the Privacy Act.

Personal information should only be disclosed to third parties or other external service providers where it is necessary in order for SGH to provide its products or services. This may include disclosing personal information to SGH subsidiaries, SGH's subcontractors and third parties engaged to perform administrative or other services for the purposes of:

- Regulatory and compliance purposes;
- Updating of credit information to credit reporting agencies;
- Resale and valuation services; or
- Underwriting, assessing and administering insurance risk and claims.

Such disclosures must always be on a confidential basis.

Any other disclosures must only occur with the relevant individual's consent or where it is required or authorised by law or court order.

3.9 Use of personal information for direct marketing purposes (APP 7)

Personal information cannot be used by SGH for direct marketing purposes unless:

- The personal information is collected from the individual directly and the individual would reasonably expect their information to be used by SGH for direct marketing and:
- SGH has provided an 'opt-out' in the marketing communication; and
- The individual has not previously made an opt-out request.
- The personal information is collected from the individual and the individual would not reasonably expect their information to be used by SGH for direct marketing, or the information is otherwise collected from a third party, and:
- SGH has obtained the individual's consent (unless impracticable);
- SGH has provided an 'opt-out' in the marketing communication;
- SGH has provided a prominent statement in the marketing communication, or otherwise made the individual aware, that the individual may request to opt-out; and
- The individual has not previously requested to opt-out.

3.10 Overseas disclosures (APP 8)

SGH may disclose personal information to overseas recipients for administrative or other business management purposes.

If personal information is required to be disclosed by SGH to an overseas recipient, such disclosure can only occur if steps have been taken, that are reasonable in the circumstances, to ensure the overseas recipient does not breach the APPs in relation to the personal information disclosed. Such steps are likely to include ensuring the overseas recipient has entered into an express contractual obligations to comply with the APPs when handling personal information disclosed to it by SGH and undertaking due diligence into the overseas recipients personal information handling processes.

However, this requirement will not occur where:

- SGH reasonably believes the overseas recipient is subject to a law, or binding scheme, that is at least substantially similar to the apps;
- The individual provides informed consent to the disclosure, which requires:
- The individual to be expressly informed that if he/she consents to the overseas disclosure, SGH will be relieved of its obligation to ensure the overseas recipient is subject to a substantially similar privacy protection framework; and
- The individual subsequently provides his/her consent.
- The overseas disclosure is authorised or required under an Australian law or court/tribunal order; or
- A prescribed public interest reasons applies.

Accordingly, personal information must not be disclosed to an overseas recipient except in accordance with the employee's duties, as expressly instructed and through the processes established and authorised in the course of employment.

3.11 Adoption of government identifiers (APP 9)

No government identifier (such as a Medicare, tax file or driver licence number) should be adopted as an internal SGH identifier for an individual.

3.12 Integrity of personal information (APP 10)

SGH must take steps that are reasonable in the circumstances to ensure that personal information that is held, used and disclosed by SGH is accurate, complete, up to date and, having regard to the purpose for any use or disclosure, relevant to that use or disclosure.

Accordingly, when disclosing personal information for a specific purpose, care must be taken to ensure only personal information relevant to that specific purpose is disclosed, notwithstanding that it may be only one piece of personal information otherwise available.

3.13 Security of personal information (APP 11)

SGH must take steps reasonable in the circumstances to ensure that personal information:

- It holds is protected from misuse, interference and loss and from unauthorised access, modification or disclosure; and
- Is destroyed or permanently de-identified when no longer required by SGH (unless the information is contained in a commonwealth record or it is otherwise unlawful or unreasonable to do so).

Accordingly, employees should not access, copy, disclose or remove personal information unless relevant to and necessary for specific duties in the course of their employment. Also, employees are required to comply with all security and confidentiality processes implemented by SGH from time to time, to ensure the security of personal information held by SGH.

Where an employee becomes aware of an actual or potential security breach in relation to SGH's handling of personal information, they must notify their direct manager and the SGH Privacy Compliance Officer immediately.

3.14 Access to personal information (APP 12)

Individuals have a right to request access to their personal information held by SGH.

A request by an individual to access their personal information held by SGH should be referred to the SGH Privacy Compliance Officer, unless otherwise responding to such a request falls within an employee's duties and express instructions in the course of their employment.

Following a request for access to personal information:

- Proof of identity of the person making the request must be obtained to ensure that personal information is only provided to the correct individual and that the privacy of others is protected;
- Reasonably specific details about the information subject to the request must be obtained;
- Where the provision of access is to attract a fee, the individual must be notified of the fee (which cannot be more than the cost to SGH in providing access in accordance with the request); and
- A response to the request should be provided within 30 days and if this is not possible, the individual should be informed of the anticipated time frame in which the request will be addressed.

Access should be granted unless denying access is required or authorised by law or providing access would otherwise:

- In SGH's reasonable belief, pose a serious threat to the life, health or safety of any individual or the public;
- Unreasonably impact on the privacy of others;
- Be in response to a frivolous or vexatious request;
- Prejudice negotiations between the individual and SGH;
- Disclose information relating to legal proceedings that would not be discoverable;
- Prejudice an investigation into suspected unlawful conduct or serious misconduct within SGH;

- Be unlawful;
- Reveal information to do with a commercially sensitive decision making process; or
- Prejudice enforcement-related activities.

Where a request for access is refused by SGH, the individual must be provided with written reasons for the refusal and details of complaint mechanisms available to the individual.

Notwithstanding a refusal by SGH to provide access in the manner specifically requested, where possible, the individual should be provided with access in a manner that meets the needs of both SGH and the individual.

3.15 Correction of personal information (APP 13)

Individuals have a right to request correction of their personal information held by SGH.

A request by an individual to correct their personal information held by SGH should be referred to the SGH Privacy Compliance Officer, unless otherwise responding to such a request falls within an employee's duties and express instructions in the course of their employment.

If SGH receives a request for correction or it is otherwise satisfied that, having regard to the purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, SGH must take such steps as are reasonable in the circumstances to correct the personal information, having regard to the purpose for which the personal information is held.

SGH must respond to a request for correction of personal information without charge and within 30 days (and if this is not possible, the individual should be informed of the anticipated time frame in which the request will be addressed).

On request of the individual, if SGH has previously disclosed personal information of the individual to a third party, SGH must also take such steps as are reasonable in the circumstances to notify the third party of the correction, unless it would be unlawful or impracticable to do so.

Where a request for correction is refused, the individual must be provided with written reasons for the refusal and details of the mechanisms through which the individual can complain.

If, following SGH's refusal of a request to correct personal information, an individual requests SGH to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, SGH must take such steps as are reasonable in the circumstances to do so.

3.16 Eligible Data Breaches

Incidents where data containing Personal Information is lost or compromised must be appropriately investigated, contained, reported and managed in compliance with the Notifiable Data Breach provisions of Part IIIC of the Privacy Act. Please refer to SGH's Personal Data Breach Procedure document for further guidance and information.

4. Responsibilities

4.1 SGH Employees

- Comply with this Policy and the Privacy Act.
- Report breaches of this Policy and the Privacy Act.

4.2 Company Secretary

- Act as Privacy Compliance Officer.
- Handle complaints regarding the handling of Personal Information.
- Handle requests for Personal Information.

4.3 All General Managers and Directors

- Ensure that their respective departments have the systems, processes, templates and tools in place to ensure compliance with this Policy and the Privacy Act when accessing, storing, using and handling Personal Information.

5. Reporting

All breaches of this procedure and the Privacy Act must be reported to the Company Secretary.

6. Complaints and Further Information

Where an employee receives a complaint about SGH's handling of personal information, the complaint must be referred to the SGH Privacy Compliance Officer who will deal with the complaint.

7. Accountabilities

Compliance to Procedure: Employees.

Implementation & Review: Company Secretary, and General Managers.

Approval of Procedure: Company Secretary.

Monitoring: Company Secretary.

Interpretation and Advice: Company Secretary.

8. Related Documents

This Policy should be read in conjunction with the following internal documents (i.e. internal documents such as policies, procedures, forms):

- Personal Data Breach Procedure

This Policy should be read in conjunction with the following legislative or compliance guidelines (if required):

- *Privacy Act 1988 (Cth)*

9. Definitions

Employee: SGH's directors, officers, executive team, managers and all other employees and contractors.