Internal Policies and Procedures

Privacy

Contents

Revision History

Date	Approver	Revision Details
		Initial CPP
May 2008	GC & CEO	Annual review - minor editing only
Feb 2012	CEO	Updated post internalisation
Dec 2016	CEO	Annual review
Dec 2017	GC	Annual review
Dec 2018	GC	Annual review
Dec 2019	GC	Annual review
Dec 2020	GC	Annual review
Feb 2022	GC	Post Implementation review

Job Functions

Abbr.	Role in Spark Infrastructure
CEO	Chief Executive Officer
GC	General Counsel and Company Secretary
HOF	Head of Finance
Tax Counsel	Senior Tax Contractor
Managers	Employees of Spark who have a supervisory or management role. Includes the CEO, GC, HOF and the Head of Renewables.

•

1. Objective and Applicable Requirements

The Privacy Act and related Australian Privacy Principles ("**APPs**") regulate the way Spark collects, uses, secures, updates and discloses Personal Information. The Privacy Act sets out the requirements for the handling of personal information about individuals. This policy sets out how Spark will comply with the Privacy Act and ensure that personal information it holds is handled appropriately. It considers:

Requirement	Description
Privacy Act	
Spark Trust Compliance Plan	Complaints

2. Applicability

This policy applies to all employees of Spark Infrastructure Group ("**Spark**"). Under this policy, "**employees**" includes contractors, consultants and other personnel who have been provided with a copy of this policy and been advised by the GC that this policy applies to them.

3. Personal Information

"**Personal Information**" is any information or opinion that is recorded and can identify a natural living person.

The following types of Personal Information are currently handled by Spark in its normal course of business:

- Details of investors who are individuals, the handling of which is outsourced to the share registrar
- Details of employees or contractors
- Details of unsuccessful job applicants or contractors

Generally, privacy legislation is not intended to prevent Personal Information about individuals acting in a business capacity ("**Business Contact Information**") from being exchanged in the normal course of business. Ordinarily, it is likely to be within individuals' reasonable expectations that information about them in their business role will be used and disclosed for generally accepted business purposes. Business Contact Information includes:

- Name
- Company the individual represents
- Title/ position description
- Work address and email
- Work phone number and mobile
- Home address and phone number
- Non–sensitive information required for corporate entertainment (e.g. hobbies, dietary requirements).

Notwithstanding the above comments, Business Contact Information is not exempt from the Privacy Act and should generally be treated in a manner consistent with other Personal Information. For example, Business Contact Information must be updated when requested by the individual. Business Contact Information does not generally include information about an individual's family.

•

Whilst most employee information is exempt from the APPs, exemptions do not apply to information about employees of other entities, unsuccessful job applicants and contractors.

All Managers are responsible for considering whether any new or changed business activity requires the handling of additional types of Personal Information or changes to the way Personal Information is handled, and if so notifying the GC so that privacy procedures can be reviewed and, if required, updated.

4. General Privacy Rules

All Managers must ensure that the following general privacy rules are adhered to, as relevant, for their areas of responsibility:

- Implement appropriate practices, procedures and systems to ensure Spark complies with the APPs and can deal with inquiries and complaints from individuals.
- Set out clearly and make available on request Spark's policies on the management of Personal Information (Privacy Policy);
- Collect only the Personal Information that is currently necessary for a legitimate business function or activity. Unnecessary Personal Information, including that obtained accidentally (e.g. emails, CV's, marketing proposals) should be promptly destroyed;
- Collect Personal Information in a fair and lawful way without unreasonable intrusiveness, intimidation or deception and not covertly. Generally Personal Information should be collected from the individual themselves or with the knowledge or consent of the individual;
- Provide a Privacy Collection Statement to the individual at or before the time of collection (or, if not practicable, as soon as practicable after the collection) of Personal Information);
- Generally, only collect sensitive information with the individual's consent;
- Only use or disclose Personal Information for the primary purpose for which it was collected unless:
    - the use or disclosure is for a related purpose (directly related if the information is sensitive information) within the individual's reasonable expectations;
    - the individual's consent is obtained;
    - the use or disclosure is required by law; or
    - another exception applies.
- Comply with the Spam Act (emails, SMS, etc), Do Not Call Register Act (telemarketing) and APP 7 in relation to direct marketing. The rules vary depending on the communication method. Express or inferred consent is required to conduct direct marketing in many cases, and individuals should be able to opt out if they don't want their details used or disclosed for direct marketing.
- Take reasonable steps to ensure that the Personal Information collected, used or disclosed is accurate, complete, relevant and up-to-date;
- Take reasonable steps to protect the Personal Information from misuse, interference and loss from unauthorised access, modification or disclosure;
- Take reasonable steps to destroy or permanently de-identify personal information if it is no longer necessary for a legitimate function or activity. Destruction of records containing Personal Information should be by secure means. Ordinarily, garbage disposal and recycling of intact documents are not secure means of destruction;
- Provide individuals with access to their Personal Information when requested. As certain exemptions and conditions may apply, Managers must refer all requests for access to Personal Information to the GC who is responsible for actioning them;
- Correct Personal Information that it is misleading or not accurate, complete or up-to-date, including where requested by the individual. As with access, several exceptions apply;

-
- Only disclose Personal Information to a third party overseas where the recipient agrees to comply with the APPs (as though itself bound), the individual consents or another exception applies. Managers must refer any proposed offshore transfers of Personal Information to the GC prior to the transfer;
- Do not use government identifiers of individuals (except ABN) as identifiers of individuals or use or disclose a government identifier unless reasonably necessary for identity verification, reasonably necessary to fulfil obligations to a relevant government agency or otherwise required or authorised by law.
- Give individuals the option of not identifying themselves or using a pseudonym, unless impracticable or required or authorised by law.

5. The Privacy Policy

The Privacy Policy summarises Spark's approach to the handling of Personal Information e.g. type of Personal Information held, purpose for collecting, holding, using and disclosing it, how it is collected and held, countries to which it is likely to be disclosed, how individuals can access and correct it and complaint processes. This Privacy Policy must be available to the public on the Spark website and in other reasonable forms on request.

The GC is responsible for:

- reviewing, and if necessary updating, the Privacy Policy annually or more often if required.
- ensuring the current Privacy Policy is included on the Spark website.

A hard copy of the Spark Privacy Policy is available from the GC if a copy is requested by a member of the public.

6. Privacy Collection Statements

Privacy Collection Statements must be provided to an individual at or before the time of collection (or, if not practicable, as soon as practicable after the collection) of Personal Information. The GC is responsible for drafting and reviewing, and if required updating, of Privacy Collection Statements for each type of Personal Information collected by Spark. Privacy Collection Statements should contain:

- the identity and contact details for Spark;
- the fact that Spark's privacy policy contains information on access, correction and complaint rights and procedures;
- the fact and circumstances of collection if not apparent;
- the purposes for which the Personal Information is collected;
- any organisations to which Personal Information of that kind is usually disclosed (including any related companies);
- any Australian law or court order that requires or authorises the personal information to be collected in the particular situation;
- the consequences (if any) for the individual if all or part of the information requested is not provided;
- whether disclosure of the Personal Information to recipients in other countries is likely, and if so, which countries if practicable to say.

Privacy Statements may be included in a prospectus, product disclosure statement, contract or form or provided as a separate statement.

•

The GC will ensure that Privacy Collection Statements are in place, including in new investor information packs issued by Spark's securities registrar relating to collection of personal information.

If Personal Information is collected from a third party, reasonable steps must be taken to ensure that the individual is or has been made aware of the matters contained in the relevant Privacy Collection Statement. In determining reasonable steps, consideration should be given to:

- whether it is possible to provide a Privacy Statement;
- whether a reasonable individual might expect a Privacy Statement to be given to them;
- how sensitive the information is;
- the cost of providing a Privacy Statement;
- the privacy consequences for the individual if a Privacy Statement is not given;
- what is accepted practice (by consumers and the industry).

Consideration should be given to the third party to provide the relevant Spark Privacy Collection Statement or include reference to Spark in their Privacy Collection Statement.

The requirement to give a Privacy Collection Statement will often not apply if information is collected from a public source (e.g. newspapers, annual reports or public registers) where the information will be handled for a purpose that is consistent with the original purpose for which the individual made their information available. This should not be taken to mean that Personal Information from the Internet and social media can be collected and used for any purpose without notifying the individual. Managers are responsible for consulting with the GC prior to the proposed collection of Personal Information from a public source.

7. Sensitive Information

Sensitive Information is Personal Information about an individual's:

- racial or ethnic origin;
- political opinions/associations;
- religious beliefs;
- trade/ professional associations/unions;
- sexual preferences/practices;
- criminal record;
- health;
- genetics;
- biometric information.

Sensitive Information can only be collected if the individual's consent is obtained or collection is required by law, required for the establishment, exercise or defence of a claim, or in other limited circumstances permitted by the Privacy Act. Managers must consult with the GC prior to the proposed collection, use or disclosure of Sensitive Information.

8. Personal Information Collected by External Service Providers

Where handling of Personal Information is outsourced (e.g. share registrar), Spark will often remain responsible for the actions of the service provider and must take reasonable steps to ensure that the Personal Information is safe in the service provider hands. Where a service provider handles Personal Information on behalf of Spark, the Manager responsible for the service provider relationship must:

- ensure the contract with the service provider allows for the protection of Personal Information disclosed to the service provider;
- ensure the service provider has adequate procedures and capability to protect Personal Information.

9. Opinion of Individuals

Personal Information includes opinions and does not need to be true. Subjective comments or opinions about individuals are a high risk because the individual may have the right to access the information or opinions could include sensitive information. Therefore, recording of opinions should be avoided unless required for a legitimate function or activity.

The basic rule when recording opinions or comments about individuals is to consider whether you would want the individual to see what you have recorded. Consideration must also be given to any potential legal action that may arise (e.g. defamation). In cases of doubt, about the most appropriate way to record an opinion or comment, the GC must be consulted.

10. Employee Records

An Employee Record is a record of personal information about an existing or past employee, e.g.

- information provided on the engagement of the employee, including CVs;
- employment contracts;
- information on the training of the employee, including academic qualifications;
- performance appraisals and information about disciplining of the employee;
- employee personal and emergency contact details.

Employee Records are exempt from the Privacy Act provided the intended use of the information relates directly to the employment relationship between Spark and the employee (past or current). Managers must ensure that Employee Records are handled with care and confidentially.

If the Personal Information is not directly related to the employment relationship, the exemption does not apply. Examples of Personal Information which would be unlikely to fall within the scope of the definition of an “employee record” are:

- an employee’s length of residence at a current or previous address;
- an employee’s credit history;
- medical assessments of an employee which do not relate directly to the inherent requirements of the employee’s employment.

-

Information about an employee's partner and family is not information about the employee themselves. Apart from family information provided as emergency contact details, no additional information about the family may be recorded.

The exemption does not apply to personal information about individuals who are not employees of the relevant entity, such as employees of related entities, or contractors, agents or unsuccessful job applicants.

Managers are responsible for ensuring that Personal Information which is not considered an Employee Record is identified and handled in accordance with this policy.

To cover the reasonable collection and use of personal information which may fall outside the employee exemption, the GC is responsible for ensuring a Privacy Collection Statement is included in the offer letter for all new employees.

11. Job Applicants and Contractors

Personal Information (such as CV's) of job applicants who do not become employees of Spark is not subject to the employee record exemption and the requirements of this policy apply. Managers are responsible for ensuring that Personal Information for unsuccessful job applicants is either destroyed or, if retained for future use, be subject to the requirements of this policy.

Care should be taken when recording notes and opinions about job applicants. No sensitive information should be recorded.

Personal information about contractors who contract as individuals (i.e. not through a company) is not subject to the employee exemption. Managers are responsible for ensuring that any Personal Information about individual contractors is subject to the requirements of this policy.

Where Spark enters into a contract with a third party such as a recruitment agency or a temp agency for the third party to provide individual's services for a fixed term, the Manager responsible for ensuring that the third party has provided a Privacy Collection Statement to the contractor.

12. Complaints

If an individual believes that Spark is in breach of its privacy obligations, they may make a complaint. This may be done by contacting Spark directly or via Spark's whistleblower service.

If the individual and Spark cannot resolve the complaint between themselves the individual may refer the complaint to the Office of the Australian Information Commissioner.

•

Appendix A – Compliance Measures

Compliance Measure	Frequency of Compliance Measure	Responsibility for Compliance Measure
For BoardRoom, ensure contract allows for the protection of Personal Information disclosed to the service provider and adequate procedures in place to protect Personal Information	Ongoing	GC
Review, and if necessary update, the Privacy Policy & ensure current Privacy Policy is included on the Spark website	As needs	GC
Review, and if required update, Privacy Collection Statements for each type of Personal Information collected by Spark	As needs	GC
Collect only the Personal Information that is currently necessary for a legitimate business function or activity. Destroy unnecessary Personal Information.	As needs	All employees
Generally, collect Personal Information from the individual themselves or with the knowledge or consent of the individual	As needs	All employees
Collect Personal Information in a fair and lawful way without unreasonable intrusiveness, intimidation or deception and not covertly.	As needs	All employees
Only collect Sensitive Personal Information with the individual's consent.	As needs	All employees
Generally, only use or disclose Personal Information for the primary purpose for which it was collected unless the individual's consent for the secondary use is obtained	As needs	All employees
Ensure Personal Information collected, used or disclosed is accurate, complete and up-to-date	As needs	All employees
Protect Personal Information from misuse and loss and from unauthorized access, modification or disclosure	As needs	All employees
Destroy or permanently de-identify Personal Information if it is no longer required	As needs	All employees
Refer all requests for access to Personal Information to GC	As needs	All employees
Correct Personal Information if notified by the individual that it is not accurate, complete or up-to-date	As needs	All employees
Refer any proposed offshore transfers of Personal Information to GC.	As needs	All employees
Do not use government identifiers of individuals (other than an ABN) as identifiers of individuals.	As needs	All employees
Ensuring Employee Records are handled with care and treated as confidential information	As needs	All employees
Ensure Personal Information which is not considered an Employee Record or relates to contractors is identified and handled in accordance with the Internal Privacy Policy	As needs	All employees
Destroy Personal Information about unsuccessful job applicants.	As needs	All employees