DATA PROTECTION POLICY

(2nd July 2014)

1. Context and Overview

1.1 Key details

Policy prepared by:	Mr Ben Chua
Approved by EXCO on:	2nd July 2014
Policy became operational on:	2nd July 2014
Data Protection Officer:	Mr Ben Chua

1.2 Introduction

365 Cancer Prevention Society needs to gather and use certain information about individuals.

These can include Employees, Clients (Service Users), Volunteers, Donors, Contractors, Suppliers, Business contacts and other people the organization has a relationship with may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the society's data protection standards and to comply with the Personal Data Protection Act 2012 (PDPA) of Singapore.

1.3 Why this policy exists

This data protection policy ensures 365 Cancer Prevention Society:

1.3.1 Complies with Personal Data Protection Act 2012 (PDPA) of Singapore and follow good practice

1.3.2 Protects the rights of Employees, Cancer patients, Volunteers, Donors, Suppliers, Business contacts and other people the organization has a relationship with may need to contact.

1.3.3 Is open about how to stores and processes individuals' data

1.3.4 Protect itself from the risks of a data breach

1.4 Personal Data Protection Act 2012 (PDPA)

The Personal Data Protection Act 2012 (PDPA) of Singapore describes how organisations including 365 Cancer Prevention Society must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by:

1.4.1 Consent Obligation

Only collect, use or disclose personal data for purposes for which an individual has given his or her consent.

Allow individuals to withdraw consent, with reasonable notice, and inform them of the likely consequences of withdrawal. Upon withdrawal of consent to the collection, use or disclosure for any purpose, your organisation must cease such collection, use or disclosure of the personal data.

1.4.2 Purpose Limitation Obligation

An organisation may collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent.

An organisation may not, as a condition of providing a product or service, require the individual to consent to the collection, use or disclosure of his or her personal data beyond what is reasonable to provide that product or service.

1.4.3 Notification Obligation

Notify individuals of the purposes for which your organisation is intending to collect, use or disclose their personal data on or before such collection, use or disclosure of personal data.

1.4.4 Access and Correction Obligation

Upon request, the personal data of an individual and information about the ways in which his or her personal data has been or may have been used or disclosed within a year before the request should be provided. However, organisations are prohibited from providing an individual access if the provision of the personal data or other information could reasonably be expected to:

1.4.4.1 Cause immediate or grave harm to the individual's safety or physical or mental health;

1.4.4.2 Threaten the safety or physical or mental health of another individual;

1.4.4.3 Reveal personal data about another individual;

1.4.4.4 Reveal the identity of another individual who has provided the personal data, and the individual has not consented to the disclosure of his or her identity; or

1.4.4.5 Be contrary to national interest.

Organisations are also required to correct any error or omission in an individual's personal data upon his or her request. Unless your organisation is satisfied on reasonable grounds that the correction should not be made, your organisation should correct the personal data as soon as practicable and send the corrected data to other organisations to which the personal data was disclosed within a year before the correction is made (or, with the individual's consent, only to selected organisations).

1.4.5 Accuracy Obligation

Make reasonable effort to ensure that personal data collected by or on behalf of your organisation is accurate and complete, if it is likely to be used to make a decision that affects the individual, or if it is likely to be disclosed to another organisation.

1.4.6 Protection Obligation

Make reasonable security arrangements to protect the personal data that your organisation possesses or controls to prevent unauthorised access, collection, use, disclosure or similar risks.

1.4.7 Retention Limitation Obligation

Cease retention of personal data or remove the means by which the personal data can be associated with particular individuals when it is no longer necessary for any business or legal purpose.

1.4.8 Transfer Limitation Obligation

Transfer personal data to another country only according to the requirements prescribed under the regulations, to ensure that the standard of protection provided to the personal data so transferred will be comparable to the protection under the PDPA, unless exempted by the PDPC.

1.4.9 Openness Obligation

Make information about your data protection policies, practices and complaints process available on request.

Designate one or more individuals as a Data Protection Officer to ensure that your organisation complies with the PDPA, including the implementation of personal data protection policies within your organisation. The business contact information of at least one of such individuals should also be made available to the public. Please note that compliance with the PDPA remains the responsibility of the organisation.

2. People, Risks and Responsibilities

2.1 Policy Scope

This policy applies to:

2.1.1 The office of 365 Cancer Prevention Society

2.1.2 All Staff and Board Members and Volunteers of 365 Cancer Prevention Society

2.1.3 All Contractors, Suppliers, Business contacts and other people working on behalf of 365 Cancer Prevention Society

It applies to all data that the society holds relating to identifiable individuals, even if that information technically falls outside of the Personal Data Protection Act 2012 (PDPA) of Singapore. This can include:

2.1.4 Names of individuals

2.1.5 Postal addresses

2.1.6 Email addresses

2.1.7 Telephones numbers

2.1.8 Any other information relating to individuals

2.2 Data Protection Risks

This policy helps to protect 365 Cancer Prevention Society from some very real data security risks, including:

2.2.1 Breaches of confidentiality

For instance, information being given out inappropriately.

2.2.2 Failing to offer choice

For instance, all individuals should be free to choose how the company uses data relating to them.

2.2.3 Reputational damage

For instance, the company could suffer if hackers successfully gained access to sensitive data.

2.3 Responsibilities

Everyone who works for or with 365 Cancer Prevention Society has some responsibility for ensuring data is collected, stored and handled appropriately.

Each department that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

2.3.1 The board members are ultimately responsible for ensuring that 365 Cancer Prevention Society meets its legal obligations.

2.3.2 The Data Protection Officer is responsible for:

2.3.2.1 Keeping the board updated about data protection responsibilities, risks and issues.

2.3.2.2 Reviewing all data protection procedures and related policies, in line with an agreed schedule.

2.3.2.3 Arranging data protection training and advice for the people covered by this policy.

2.3.2.4 Handling data protection questions from staff and anyone else covered by this policy.

2.3.2.5 Dealing with requests from individuals to see the data holds about them (also called 'subject access requests").

2.3.2.6 Checking and approving any contacts or agreements with third parties that may handle the society's sensitive data.

2.3.3 The IT Manager is responsible for:

2.3.3.1 Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

2.3.3.2 Performing regular checks and scans to ensure security hardware and software is function properly.

2.3.3.3 Evaluation any third-party services the society is considering using to store or process data. For instance, cloud computing services.

2.3.4 The Publicity Executive is responsible for:

2.3.4.1 Approving any data protection statements attached to communications such as emails and letters.

2.3.4.2 Addressing any data protection queries from journalists or media outlets like newspapers.

2.3.4.3 Where necessary, working with other staff to ensure publicity initiatives abide by data protection principles.

2.3.5 The Patient Care Manager and the Volunteer Management Executive are responsible for:

2.3.5.1 Handling of data is according to Personal Data Protection Act 2012 (PDPA) of Singapore.

2.3.5.2 Do not disclose the personal data to volunteers or any other people that are non-work related.

3. General staff guidelines

3.1 The only people able to access data covered by this policy should be those who need it for their work.

3.2 Data should not be shared informally. When access to confidential information is required, employees can request it from their managers.

3.3 365 Cancer Prevention Society will providing training to all employees to help them understand their responsibilities when handling data.

3.4 Employees should keep all data secure, by taking sensible precautions and following the guideline below.

3.5 In particular, strong passwords must be used and they should never be shared.

3.6 Personal data should not be disclosed to unauthorized people, either within the company or externally.

3.7 Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

3.8 Employees should request help from their manager or the Data Protection Officer if they are unsure about any aspect of data protection.

4. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager.

4.1 When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

4.1.1 When not required, the paper or files should be kept in a locked drawer or filing cabinet.

4.1.2 Employees should make sure paper and printouts are not left where unauthorized people could see them, line on a printer.

4.1.3 Data printouts should be shredded and disposed of securely when no longer required.

4.2 When data is stored electronically, it must be protected from unauthorized access, accidental deletion or malicious hacking attempts:

4.2.1 Data should be protected by strong passwords that are changed regularly and never shared between employees.

4.2.2 If data is stored on removable media (like a CD, DVD, USB drive or Thumb Drive), these should be kept locked away securely when not being used.

4.2.3 Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.

4.2.4 Servers containing personal data should be sited in a secure location, away from general office space.

4.2.5 Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

4.2.6 Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

4.2.7 All servers and computers containing data should be protected by approved security software and a firewall.

5. Data Use

Personal data is of no value to 365 Cancer Prevention Society unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

5.1 When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

5.2 Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

5.3 Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorized external contacts.

5.4 Personal data should never be transferred outside of Singapore unless it has taken appropriate steps to ensure that it will comply with the Data Protection Act in respect of the transferred personal data while such personal data remains in its possession or under its control; and if the personal data is transferred to a recipient in a country or territory outside Singapore, that the recipient is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA.

5.5 Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

6. Data Accuracy

The law requires 365 Cancer Prevention Society to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort 365 Cancer Prevention Society should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

6.1 Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

6.2 Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

6.3 365 Cancer Prevention Society will make it easy for data subjects to update the information 365 Cancer Prevention Society holds about them. For instance, via the company website.

6.4 Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

6.5 It is the Publicity Executive's responsibility to ensure databases are checked against industry suppression files every six months.

7. Subject Access Requests

All individuals who are the subject of personal data held by 365 Cancer Prevention Society are entitled to:

7.1 Ask what information the company holds about them and why.

7.2 Ask how to gain access to it.

7.3 Be informed how to keep it up to date.

7.4 Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a "Subject Access Request.

Subject Access Requests from individuals should be made by email, addressed to the Data Protection Officer at dpo@365cps.org.sg. Individuals will be asked to donate $50 per Subject Access Request. The Data Protection Officer will aim to provide the relevant data within 30 days.

The Data Protection Officer will always verify the identity of anyone making a Subject Access Request before handing over any information.

8. Disclosing Data for Other Reasons

In certain circumstances, 365 Cancer Prevention Society will disclose requested data. However, the Data Protection Officer will ensure the request is legitimate, seeking assistance from the board and from the society's legal advisers where necessary.

9. Providing Information

365 Cancer Prevention Society aims to ensure that individuals are aware that their data is being processed, and that they understand:

9.1 How the data is being used

9.2 How to exercise their rights

To these ends, the society has a privacy statement, setting out how data relating to individuals is used by the society.