Ascending Hope Community Services

Personal Data Protection Act: Internal Policy and Guidelines

Use of this document

Title	Personal Data Protection Policy and Guidelines
Department Owner	Personal Data Protection Office
Department(s) Applied To	All Business Units and Departments within the organisation
Position Applied To	All positions dealing with personal data
Regulatory Requirements	Personal Data Protection Act 2012

Table of Contents

1. Introduction 4
2. Scope 4
3. What is personal data? 4
4. Roles and Responsibilities 5
5. Guidelines 6
5.1 Collection, Use and Disclosure of Personal Data 6
5.2 Maintenance of Data Quality 8
5.3 Granting Access to Personal Data 8
5.4 Granting Correction of Personal Data 9
5.5 Protection of Personal Data 10
5.6 Anonymisation of Personal Data 11
5.7 Retention and Disposal of Personal Data 11
5.8 Handling Feedback and Complaints 12
5.9 PDPA Awareness 13
5.10 Dealing with Business Partners 13
5.11 Reporting of Breaches (to be read with the Information Security Incident Management Plan, and Policy) 13
5.12 Compliance Review Programme 14
5.13 Contacting DPO 14
Appendix A: Personal data of the Organisation's Staff. 15
Appendix B: Personal data of the Organisation's patients. 16
Appendix C: Personal data of the Organisation's donors 17
Appendix D: Personal data of the Organisation's volunteers 18
Appendix E: Application for Withdrawal of Consent Form 19
Appendix F: Application for Access to Personal Data Form 20
Appendix G: Application for Correction of Personal Data Form 22
Appendix H: Sample Tables for Data Retention and Disposal 23
Appendix I: Disposal methods 24
Appendix J: Data Processing Agreement Template 26

1. Introduction

1.1 The Personal Data Protection Act 2012 (**PDPA**) established a new overarching Singapore regime for the protection of personal data and seeks to ensure that organisations comply with a baseline standards of protection for personal data of individuals.

1.2 There are two key parts of the PDPA:

- Protection of an individual's "**personal data**", i.e. data, whether true or not, about an individual which can be identified from that data or other information available or accessible by that organisation. The protection covers personal data stored in electronic or non-electronic form.
- Establishment of a Do Not Call Registry (**DNC Registry**) for individuals to opt-out from receiving certain types of marketing messages.

1.3 Ascending Hope Community Services (**Organisation**) is committed to compliance with the PDPA. All staff are to familiarise themselves with the guidelines in this document as it describes the responsibilities in connection with any personal data that may be collected, used and disclosed as an employee of the Organisation.

1.4 The purpose of this document is to provide instructions for the collection, use and disclosure of personal data in compliance with the PDPA.

1.5 Failure to comply with the guidelines in this document could expose the Organisation to enforcement action by the Personal Data Protection Commission ("PDPC"), including the imposition of financial penalties. There may also be negative publicity from any breach that is made public. Compliance with this document will help the Organisation avoid such negative consequences.

2. Scope

2.1 This document applies to all employees (whether on a part-time, temporary or full-time basis), interns and trainees (**Staff**) working at or attached to the Organisation who are granted access to and/or process personal data on behalf of the Organisation. Violation may result in disciplinary action including termination of employment and/or termination of contract.

2.2. This document may be updated from time to time. Staff should familiarise themselves with the guidelines in this document and any of its subsequent versions. This document is not intended to supersede or override other policies relating to the handling of personal data. Therefore, please continue to observe all other policies pertaining to the handling of personal data as well as any applicable confidentiality or secrecy obligations.

3. What is personal data?

3.1 Please regard any data which you can relate to a specific identifiable individual, whether such individual is identifiable from the data itself or from other information

which is reasonably available to the Organisation, as being "**personal data**". The only exception to this is the following information provided to you in your business capacity, which you collect, use and disclose in your business capacity or for a business purpose of the:

- Name
- Position name or title
- Business telephone number
- Business address
- Business electronic mail address
- Business fax number
- Other similar information provided to you in your business capacity (e.g. such as contained on business cards you collect or provided pursuant to contracts signed between an entity and a third party)

3.2 By way of example, all of the following is personal data:

- Full name
- NRIC/passport number
- Photograph or video image of an individual
- Name and address or phone number

3.3 Please seek the assistance of the DPO if you are unsure whether any specific information is "personal data".

3.4 Further general information on PDPA is available at http://www.pdpc.gov.sg/.

4. Roles and Responsibilities

The roles and responsibilities of relevant parties are detailed below:

4.1 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is the main contact person for and has oversight responsibilities on all PDPA related matters. These include:

a) Overseeing and implementing Data Protection Programme to comply with the requirements of the PDPA.
b) Maintaining the currency of Personal Data Protection Policy and Guidelines, and communicating them to staff.
c) Reviewing internal protocols, systems and processes relating to personal data.
d) Working with relevant Business Units (BUs) to evaluate business specific operation and risks.
e) Maintaining records of queries/complaints and the results of PD related incidents.
f) Monitoring and conducting regular compliance assessment and alert management of any risk that may arise with personal data usage.
g) Liaising with Personal Data Protection Commission (PDPC) on PDPA related matters, as and when necessary.
h) Providing regular status updates to the Management.

4.2 Staff

Staff is required to:

a) Be familiar with Personal Data Protection Policy and know the requirements of PDPA.
b) Comply with the Personal Data Protection Policy and Guidelines with regards to the personal data that they are handling.
c) Ensure that personal data is collected for a legitimate purpose and with consent of the individual.
d) Understand the importance of protecting personal data that has been collected, and undertake all necessary security measures to safeguard such data.
e) Ensure the personal data is disposed properly when it is no longer required.

5. Guidelines

This set of guidelines is intended to provide guidance to staff and facilitate them in complying with the requirements of the PDPA.

5.1 Collection, Use and Disclosure of Personal Data

Collection of Personal Data

5.1.1 The Organisation may collect personal data through various channels from:

a) actual or prospective customer or staff
b) job applicants
c) individuals otherwise involved in, connected with or impacted by the Organisation's business activities

5.1.2 Staff should collect personal data that are consistent with the purposes listed in the Personal Data Protection Policy.

5.1.3 Staff should only collect personal data that is necessary for its functions and activities.

5.1.4 Staff should only collect personal data by lawful and fair means and not in an unreasonably intrusive manner.

5.1.5 Staff should ensure that individuals are aware that the Organisation is collecting personal data about them and that the information is collected without intimidation and deception.

5.1.6 As a good practice, staff should obtain consent in writing or recorded in a manner that is accessible for future reference. Wherever possible, consent should be obtained upfront in application forms.

5.1.7 Notification should be provided to individuals as follows:

a) Where personal data is collected on a form, include a statement about the purpose on the form.

b) Where personal data is collected using a cookie, web bug or other means, include a statement about the website.
c) Where personal data is collected over the phone, use an automated message to advise individuals about this (where practicable to do so).

Withdrawal of Consent

5.1.9 Individuals are allowed to withdraw consent in respect to the collection, use or disclosure of their personal data provided that the purpose for which the use of data provided have not been submitted to the relevant authorities. The following requirements are to be complied with:

a) Individual must give reasonable notice of the withdrawal to the Organisation.
b) On receipt of the notice, the Organisation must inform the individual of the consequences of withdrawing consent and the processing time required for the withdrawal.
c) The Organisation must not prohibit an individual from withdrawing consent, only if it does not affect any legal consequences arising from such withdrawal.
d) Upon withdrawal of consent, the Organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data.

5.1.10 Individuals can put up a request for withdrawal of consent in writing to the DPO. Withdrawal requests could be made by completing the "Application for Withdrawal of Consent" form (Refer to Appendix E) at our Main Office, or mailed to our office at 37 Jalan Pemimpin #07-03 Singapore 577177 (Attn to: DPO)

5.1.11 The counter staff receiving the form should request for a form of identification (e.g. NRIC, Driving License, etc.) for a visual check of the provided information to verify that the request is legitimate. No recording (e.g. copying, photocopying, taking pictures, scanning, etc.) should be done to the NRIC or Driving License.

5.1.12 The completed and verified consent withdrawal form should be forwarded to the DPO for review and subsequent processing.

Use & Disclosure

5.1.13 The Organisation's use and disclosure of the personal data collected should be consistent to the original purpose it was intended for.

5.1.14 If the personal data is intended for another purpose (i.e. differing from the original purpose), a new set of consent is to be obtained from the individual again.

5.1.15 Prior to using or disclosing any personal data, you must:

- Check that the personal data you are using or disclosing is listed in Appendices A, B, C, and D; and
- Confirm that the purpose for which you are using or disclosing that personal data is listed in the corresponding "permitted purposes" column in Appendices A, B, C, and D.

5.1.16 Staff should seek assistance from the DPO if they are unsure whether a use or disclosure falls within the original consent.

Exceptions

5.1.17 There are exceptions whereby consent is not required for collection, use and disclosure of personal data. Please refer to the respective schedules within the Personal Data Protection Act for more details:

a) Second Schedule – Collection of Personal Data without Consent
b) Third Schedule – Use of Personal Data without Consent
c) Fourth Schedule – Disclosure of Personal Data without Consent

5.1.18 Staff should note that even if an exception applies such that consent need not be sought, the exception does not override existing laws and requirements.

5.2 Maintenance of Data Quality

5.2.1 Staff shall take reasonable steps to ensure the accuracy and the completeness of personal data collected. These will include:

a) Verification of personal data collected against supporting documents.
b) Training staff on the processes to verify and correct information provided.
c) Granting access to personal data only to authorised staff on a need-to-know basis to maintain integrity of data.
d) Sending regular reminders to staff, patients, and stakeholders to update their personal data with Ascending Hope Community Services if there are any.

5.3 Granting Access to Personal Data

5.3.1 Individuals may only make a request for access to their personal data via Ascending Hope Community Services' Office.

5.3.2 Access requests can be made by completing the "Application for Access to Personal Data" form (Refer to Appendix F) made available Ascending Hope Community Services' office.

5.3.3 The counter staff receiving the form should request for a form of identification (e.g. NRIC, Driving License, etc.) for a visual check of the provided information to verify that

the request is legitimate. No recording (e.g. copying, photocopying, taking pictures, scanning, etc.) should be done to the NRIC or Driving License.

5.3.4 The completed and verified access form should be forwarded to the DPO for review and subsequent processing.

5.3.5 The DPO should determine if access should be granted and as necessary:

a) Consider whether to impose a fee for providing access, and are to advise the requestor of that fee accordingly.
b) If the access request is made on behalf of another individual, ensure that evidence of consent is obtained from the said individual whose personal data it belongs to. This can be done via calls made directly to the individual in question.
c) Provide the requestor with only the requested information.
d) If applicable, provide the individual with reasons for refusing the access. Exceptions for refusing access request is stated in the Fifth Schedule of the PDPA.

5.3.6 Once the request has been completed, the DPO will update the completion status for closure.

5.4 Granting Correction of Personal Data

5.4.1 Individuals may make a request to update their personal data via Ascending Hope Community Services' office.

5.4.2 Correction requests could be made by completing the "Application for Correction of Personal Data" form (Refer to Appendix G) made available at Ascending Hope Community Services' office.

5.4.3 The counter staff receiving the form should request for a form of identification (e.g. NRIC, Driving License, etc.) for a visual check of the provided information to verify that the request is legitimate. No recording (e.g. copying, photocopying, taking pictures, scanning, etc.) should be done to the NRIC or Driving License.

5.4.4 The completed and verified correction form should be forwarded to the DPO for review and subsequent processing.

5.4.5 The DPO which handles such requests should determine if corrections should be granted and as necessary:

a) Make necessary correction(s).
b) Notify the individuals when the correction request is completed.
c) If applicable, provide the individual with reasons for refusing the correction request. Exceptions for refusing correction request is stated in the Sixth Schedule of the PDPA.

5.4.6 Once the request has been completed, the DPO will update completion status for closure.

5.5 Protection of Personal Data

5.5.1 Personal data collected should be treated as confidential information. It should be protected in a secure manner, and access to such data by authorized staff should be granted on a restricted and need to basis.

5.5.2 Organisation should consider adopting security measures that are reasonable and appropriate in their own circumstances. For example, take into consideration the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.

5.5.3 Security measures may take various forms as follows:

I. Administrative Security
   a) Requiring employees to be bound by confidentiality obligations in their employment agreements
   b) Implementing and communicating policies and procedures (with disciplinary consequences for breaches) regarding confidentiality obligations.
   c) Conducting regular training sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data.
   d) Ensuring that only the appropriate amount of personal data is held, as holding excessive data will also increase the efforts required to protect personal data.

II. Physical Security
   a) Restricting employee access to confidential documents on a need-to-know basis.
   b) Encouraging a clean desk policy.
   c) Putting in place access control measures and security alarm systems to detect unauthorised access.
   d) Proper disposal of personal data (and related documents) that are no longer required.

III. Computer and Network Security
   a) Ensuring computer networks are secure.
   b) Installing appropriate computer security software (including virus checking) and using suitable computer security settings.

c) Adopting appropriate access controls (i.e. User passwords, screen saver passwords and limiting access to shared network drives to authorised personnel).
d) Using right level of email security settings when sending and receiving confidential emails.
e) Ensuring that IT service providers are able to provide the requisite standard of IT security.

IV. Personnel Security
a) Granting system access only to personnel who need the functions or information to carry out their duties.

5.5.4 All staff should be familiar and comply with requirements and obligations under the IT Policy and the Employee Handbook for details of the Organisation's Code of Conduct.

5.6 Anonymisation of Personal Data

5.6.1 All staff handling personal data should consider the need to anonymise the personal data collected under their care where practicable.

5.6.2 In the case where individuals need not be identified for the purposes in question, it is good practice to collect data in an anonymised form or to anonymise the data prior to disclosure to another party.

5.7 Retention and Disposal of Personal Data

5.7.1 All staff should note that under the PDPA, it prohibits the organisation from retaining personal data indefinitely without legal or business reasons. The organisation must not keep personal data "just in case" it may be needed for other purposes that have not been made known to the individual concerned.

5.7.2 The data is to be disposed of/destroyed when it is no longer required for any legal or business purposes after 6 years, in accordance to the document retention requirements from the Companies Act.

5.7.3 Staff must:
- Conduct regular checks on personal data retained (at least once a year)
- Inform DPO upon destruction or anonymisation of personal data
- Comply with all instructions by the DPO in respect of the personal data which is no longer retained

5.7.4 Calculation of retention periods can be done by grouping documents into categories and allocating retention periods accordingly. The retention period of a document or category should be calculated by:

- Determining the minimum length of time that the relevant law or regulation requires the data to be retained (e.g. PHMC Regulations, MOH's 2015 Guidelines for the Retention Periods of Medical Records);
- Determining the commercially prudent length of time that the document is required for normal operations or business purposes;
- Determining whether the documents are likely to be needed for purposes other than the normal operations or business purposes, such as supporting a potential litigation or arbitration case, an employment or contract dispute or supporting business continuity plans and then determining a prudent length of time to retain the data; and
- Using the longer of each of these three periods.

Refer to Appendix H for how retention periods should be documented.

5.7.5 The related departments will be responsible for gathering the information to calculate the retention periods for each category of documents, and consult Legal/legal counsel and the DPO where necessary.

5.7.6 When the retention periods for data have expired and the data is no longer required, the data will be destroyed using the methods in Appendix I.

5.8 Handling Feedback and Complaints

5.8.1 This section provides the process that staff can undertake to facilitate the handling of any feedback, or complaints from staff or the public in regards to matters pertaining to personal data protection.

5.8.2 All feedback/complaints should be provided via email to the DPO: admin@ascendinghope.org

5.8.3 The DPO will endeavour to respond to the reply within 15 working days. Where a request requires more time, the DPO will acknowledge the individual's request with the approximate time of resolution.

5.8.4 All personal data requests relating to queries, access and correction will be handled by the DPO. The DPO will keep the requests for at least one (1) year from the date of completion of the request.

5.8.6 All complaints in relation to personal data matters should be directed to the DPO, who shall respond to the said complaint.

5.8.7 All enquiries from the media shall be referred to the DPO to respond to the said enquiries.

5.9 PDPA Awareness

5.9.1 Awareness building programme shall be carried out from time to time, when necessary, to allow staff to be familiar with obligations under the PDPA and understand their roles in complying with the PDPA.

5.9.2 All new staff will be made aware of obligations under the PDPA through the onboarding process by HR.

5.10 Dealing with Business Partners

5.10.1 When staff have an engagement with business partners which involve collection or disclosure of personal data, the following key points are to be noted:

a) Staff are to ensure and verify that business partners have proper policies and proper protection measures in place to facilitate compliance with the PDPA via a Data Processing Agreement (refer to Appendix J for a template).
b) Staff are to ensure that business partners understand that it must not use any personal data for non-permitted use and to provide contractual provision for enforcement of requirements.
c) Legal advice is to be sought (where required) where contracts with business partners involve the collection/use/disclosure of personal data.

5.11 Reporting of Breaches (to be read with the Information Security Incident Management Plan, and Policy)

5.11.1 In the event of a breach of personal data security (e.g. loss or unauthorised disclosure of personal data by staff), it is vital to ensure that it is dealt with immediately and appropriately to minimize the impact of the breach and prevent a recurrence.

5.11.2 If a staff becomes aware of an actual, potential or suspected breach of personal data security, staff must report the incident to the DPO immediately.

5.11.3 The staff shall:

a) Report the incident immediately to the DPO.
b) Record the relevant details of the incident and communicate on a need-to-know basis to relevant staff so that prompt and appropriate actions can be taken to resolve the incident.

5.11.4 DPO will then review and ensure that the incident is appropriately addressed and closed.

5.12 Compliance Review Programme

5.12.1 Regular internal review process should be conducted to ensure that the personal data protection requirements are compiled within the Organisation. A compliance assessment exercise will be initiated at least once every two years by the DPO with the various staff to support an ongoing compliance with the PDPA programme.

5.13 Contacting DPO

5.13.1 If you have any query or feedback in regard to the PDPA, you may contact the DPO via email at admin@ascendinghope.org

Appendix A: Personal data of the Organisation's Staff.

Type of Personal Data	Purpose
Personal data of employees	• For managing or terminating the employment or other relationship between the Organisation and the employee • To evaluate the employee • To fulfil internal audit requirements • For payroll arrangement • To arrange for employment benefits/privileges to be offered to the employee • To use employee's details or those nominated contact on business continuity/disaster recovery contact list • To confirm the employee's contact in the context of security clearances authorisation granted • To make disclosures as permitted or required by applicable law such as in connection with investigations • To respond to queries the employee or the employee's authorised representatives may have to manage disputes • To apply for insurance policy
CCTV Footage	• To maintain security of the Organisation's office premises

Appendix B: Personal data of the Organisation's beneficiaries.

Type of Personal Data	Purpose
Personal data of beneficiaries	• Performing obligations in the course of or in connection with the provision of services • Verification of identity • Responding to, handling, and processing queries, requests, applications, complaints, and feedback • Processing of billing • For processing of booking appointments • Processing of grant, subsidy, or financial assistance applications • Complying with any applicable laws, regulations, codes of practice, guidelines, or rules, or to assist in law enforcement and investigations conducted by any governmental and/or regulatory authority • Transmitting to any unaffiliated third parties including our third party service providers and agents, and relevant governmental and/or regulatory authorities, whether in Singapore or abroad, for the aforementioned purposes • Any other purposes which Ascending Hope Community Services may inform beneficiaries of in writing from time to time, but for which Ascending Hope Community Services will seek beneficiaries' separate consent

Note: Use of data for the purposes include disclosure between the Organisation, to third parties who provide services to the Organisation and further collection, use or disclosure by such parties of such data for such purposes. If you are establishing a new method of disclosure or if you are unsure whether you may use such data, please seek assistance from the DPO.

Appendix C: Personal data of the Organisation's donors

Type of Personal Data	Purpose
Personal data of donors	• Verification of identity • Responding to, handling, and processing queries, requests, applications, complaints, and feedback • Complying with any applicable laws, regulations, codes of practice, guidelines, or rules, or to assist in law enforcement and investigations conducted by any governmental and/or regulatory authority • Transmitting to any unaffiliated third parties including our third party service providers and agents, and relevant governmental and/or regulatory authorities, whether in Singapore or abroad, for the aforementioned purposes • Any other purposes which Ascending Hope Community Services may inform patients of in writing from time to time, but for which Ascending Hope Community Services will seek donors' separate consent

Note: Use of data for the purposes include disclosure between the Organisation, to third parties who provide services to the Organisation and further collection, use or disclosure by such parties of such data for such purposes. If you are establishing a new method of disclosure or if you are unsure whether you may use such data, please seek assistance from the DPO.

Appendix D: Personal data of the Organisation's volunteers

Type of Personal Data	Purpose
Personal data of volunteers	• Assessing of suitability of volunteer • Verification of identity • Responding to, handling, and processing queries, requests, applications, complaints, and feedback • For processing of booking appointments • Complying with any applicable laws, regulations, codes of practice, guidelines, or rules, or to assist in law enforcement and investigations conducted by any governmental and/or regulatory authority • Transmitting to any unaffiliated third parties including our third party service providers and agents, and relevant governmental and/or regulatory authorities, whether in Singapore or abroad, for the aforementioned purposes • Any other purposes which Ascending Hope Community Services may inform patients of in writing from time to time, but for which Ascending Hope Community Services will seek volunteers' separate consent

Note: Use of data for the purposes include disclosure between the Organisation, to third parties who provide services to the Organisation and further collection, use or disclosure by such parties of such data for such purposes. If you are establishing a new method of disclosure or if you are unsure whether you may use such data, please seek assistance from the DPO.

Appendix E: Application for Withdrawal of Consent Form

WITHDRAWAL OF CONSENT FORM	
PERSONAL DETAILS	
Name :	
NRIC No. (last 3 digits and alphabet):	
Address :	
Email :	Telephone / Mobile No :
REMARKS (If any)	
IMPORTANT INFORMATION	
Please attach a copy of : (a) a valid power of attorney authorising you to make this withdrawal of consent if you are making this withdrawal request in respect of another person's personal data, or (b) a written and acknowledged documentation granting you permission to act on behalf of the individual. Please note that to process this withdrawal request, the information in this form may need to be given to third parties or our affiliated companies. By default, your request will be treated as a full withdrawal of your consent concerning your personal data (i.e. for its collection, use and disclosure). Please indicate clearly in the Form if you do not wish to withdraw your consent for us to (i) collect; or (ii) use; or (iii) disclose, any of your data. The Data Protection Officer will contact you via email if more information is required to process your request. Upon sending your request, please allow us 30 working days from receipt of your request for processing. During this period, you may continue to receive correspondence from us. We will be entitled to act on this request without reconfirming that you wish to proceed with your request. Please present your NRIC / Driving License for visual verification of your identity at the point of submitting this form to our Counter Staff. We will not make or store any copies of your NRIC / Driving License.	
Signature :	Date :

Appendix F: Application for Access to Personal Data Form

APPLICATION FOR ACCESS TO PERSONAL DATA FORM	
ABOUT THIS FORM	
(a) This form enables us to locate the personal data that you require. Please provide all the requested information. You may attach additional pages in your response. (b) Please note that you may only apply for access to your own personal data. You may not apply for access to another person's personal data unless you are the parent or legal guardian of a child. If you are requesting access on behalf of another person, you must provide proof of your authority to do so. (c) We may charge you a fee to process your request. Processing of your request will begin only after payment is received. (d) We will respond to your request within 30 business days. (e) We may deny access in certain limited circumstances. If we refuse access, this will be pursuant to the provisions of the Personal Data Protection Act, its subsidiary legislation or other guidance provided by the Personal Data Protection Commission. (f) Please note that to process this request, the information in this form may need to be given to third parties or our affiliated companies.	
PERSONAL DETAILS	
Name :	
NRIC No. (last 3 digits and alphabet):	
Address :	
Email :	Telephone / Mobile No :
INFORMATION REQUESTED	
(Please attach additional pages if needed) Name of Data Subject (if different from person requesting): _____ Location, date and time data was captured:	
IMPORTANT INFORMATION	

(a) If you are collecting this information on behalf of someone else, please provide written evidence of the identity of the individual who has authorised you to collect the information as well as proof of your own identity. We reserve the right to contact the other individual. Evidence may include a valid Power of Attorney, or written and acknowledged documentation granting you permission to act on behalf of the individual.

(b) Please present your NRIC / Driving License for visual verification of your identity at the point of submitting this form to our Counter Staff. We will not make or store any copies of your NRIC / Driving License.

DECLARATION

I confirm that this application relates to personal data about me.

Signature : Date :

Appendix G: Application for Correction of Personal Data Form

APPLICATION FOR CORRECTION OF PERSONAL DATA FORM	
ABOUT THIS FORM	
(a) This form has been prepared to assist you in applying to correct personal data about you. (b) Please provide all of the requested information, attaching additional pages if you require more spaces for your response. (c) Please note that you may only apply to correct your own personal data. You may not apply to correct another person's personal data unless you are the parent or legal guardian of a child. If you are requesting to requesting corrections on behalf of another person, you must provide proof of your authority to do so. (d) We will try to respond to your request for correction promptly, in most cases within 10 business days. (e) We are permitted and/or required to refuse to make the correction in certain limited circumstances. If we refuse to make the correction, this will be pursuant to the provisions of the Personal Data Protection Act, its subsidiary legislation or other guidance provided by the Personal Data Protection Commission.	
PERSONAL DETAILS	
Name :	
NRIC No. (last 3 digits and alphabet):	
Address :	
Email :	Telephone / Mobile No :
CORRECTION REQUESTED	
(Please specify the personal data and the relevant correction you are requesting to be made) (Please attach more pages where necessary)	
IMPORTANT INFORMATION	
(a) If you are collecting this information on behalf of someone else, please provide written evidence of the identity of the individual who has authorised you to collect the information as well as proof of your own identity. We reserve the right to contact the other individual. Evidence may include a valid Power of Attorney, or written and acknowledged documentation granting you permission to act on behalf of the individual. (b) Please present your NRIC / Driving License for visual verification of your identity at the point of submitting this form to our Counter Staff. We will not make or store any copies of your NRIC / Driving License.	
DECLARATION	
I confirm that this application relates to personal data about me (or about a person that has authorised me to make this application on their behalf). Signature : Date :	

Appendix H: Sample Tables for Data Retention and Disposal

Type of Record	Minimum Retention Period	Reason for Length of Period

File ID	Retention		Storage Location	Disposal Method	Signature
	Start	End			

Appendix I: Disposal methods

#	Medium	Method
1	CD-ROMs, DVDs & Tapes	• Destroy CD-ROMs, DVDs or tapes by cutting them up with scissors or using devices that are designed to shred them.
2	USB, Hard drives	• The hard drive must either be physically destroyed or software tools must be used to remove the data. • All USBs and storage devices must be cleaned and cleared of all traces before re-using. • Alternatively the USBs and hard drives should be degaussed. • Note that degaussing can make the media inoperable, so this method is not recommended if the media needs to be reused.
3	Multi-Functional Devices (MFDs)	• Ascending Hope Community Services staff to escort and witness the formatting of MFD, hard disk by the vendor. • The vendor should then transfer the disk to a degaussing plant for degaussing and should issue a certificate of degaussing to Ascending Hope Community Services.
4	Data in shared folders	• Ascending Hope Community Services to implement a clean folder policy and at periodic intervals perform an inventory for all files containing personal data and delete old data that is longer required (especially unstructured files)
5	Data in applications	• Ascending Hope Community Services to perform an inventory for data stored in the applications on a periodic basis and compare with the retention schedules and delete data that is not required from the applications
6	Voice Recordings	• All recordings of phone calls in which consent is obtained, should be retained as long as Ascending Hope Community Services intends to use and disclose this data or 7 years after the business relationship ends with the individual, whichever is earlier. • All other recordings of phone calls to be deleted from the system after 24 months. • Ascending Hope Community Services to perform an inventory of the voice recordings downloaded into a shared folder or any other location and delete recordings that are no longer required
7	Video Image	• All recordings to be deleted from the system after xx months • Ascending Hope Community Services to perform an inventory of the video recordings downloaded into the shared folder or

#	Medium	Method
		any other location and delete recordings that are no longer required
8	Hardcopy documents	• Hardcopy Documents that are “restricted”, “confidential” or “internal” shall be shredded. • Other Hardcopy Document may be destroyed using other methods. • The destruction of Hardcopy Documents that have been archived and shredded must be recorded and the record must identify the documents destroyed, who authorized the destruction and the date the documents were destroyed.

Appendix J: Data Processing Agreement Template

DATA PROCESSING AGREEMENT

This Personal Data Processing Agreement ("**DPA**") is concluded between

Ascending Hope Community Services
An organisationincorporated under the laws of Singapore with its registered office at Ascending Hope Community Services, 37 Jln Pemimpin, #07-03, Singapore 577177, represented by Eva Ng, Executive Director ("**AHCS**" or "**Customer**")

and

[ORGANISATION]
with its registered office at [ADDRESS], represented by [NAME, POSITION] **("Company ABC"** or "**Contractor**")

(each individually the "**Party**" and together the "**Parties**")

to reflect the Parties' agreement with regard to the processing of personal data under the contracts concluded between **AHCS** and [Company ABC] in accordance with the requirements of the Personal Data Protection Act 2012 ("PDPA").

BACKGROUND

AHCS utilizes the services consisting in [xxx] [please add the services where Company ABC will process **Customer Personal Data** as the Controller] ("**Services**") under the contracts concluded between AHCS and Company ABC (individually "**the respective contract**", collectively the "**contracts**").

While providing the Services, the Service Provider will have access to personal data as will be submitted by **AHCS** to Company ABC (the "**Personal Data**") and thus will process certain categories of Personal Data as a "**Data Intermediary".**

Company ABC (when acting as Data Intermediary) agrees to comply with the following provisions with respect to Personal Data provided or made accessible by **AHCS** and processed by Company ABC in connection with provision of Services.

1. DEFINITIONS, SUBJECT MATTER, NATURE AND PURPOSE OF PROCESSING

1.1. Terms used in this DPA shall have following meaning:

- "**Contractor"** means [name of the Contractor]
- "**Customer**" means [name of the Customer]

- "**Data Intermediary"** as defined by Section 2(1) of the PDPA as an organisation that processes data on behalf of another organisation but does not include an employee of that other organisation
- "**Customer Personal Data"** means Personal Data which the Customer discloses to the Contractor, or which the Contractor processes on behalf of the Customer, including: [Refer to clause 1.5]

1.2. Within this DPA and during provision of the Services, **AHCS** is in the position of Customer and Service Provider acts in the capacity of Contractor.

1.3. Subject matter, nature and purpose of the processing: provision of Services.

1.4. Duration: for the term of the provision of Services.

1.5. Types of Personal Data and categories of data subjects: [please insert> e.g. first and middle names, surnames, date of birth, personal identification numbers, address, citizenship, business contact data and any information provided for the purpose of provision of the Services by **AHCS** or by the data subjects (relevant staff members, representatives, contractors and clients directly).]

2. OBLIGATIONS OF CONTRACTOR

2.1 Compliance with PDPA. The Contractor shall comply with all its obligations under the PDPA at its own cost.

2.2 Process, Use and Disclosure. The Contractor shall only process, use or disclose Customer Personal Data:
(a) strictly for the purposes of [fulfilling its obligations and providing the services required] under this Agreement;
(b) with the Customer's prior written consent; or
(c) when required by law or an order of court, but shall notify the Customer as soon as practicable before complying with such law or order of court at its own costs.

2.3 The Contractor shall immediately notify the Customer when the Contractor becomes aware of a breach of any of its obligations in this agreement.

2.4 The Contractor shall indemnify the Customer and its officers, employees and agents, against all actions, claims, demands, losses, damages, statutory penalties, expenses and cost (including legal costs on an indemnity basis), in respect of:
(a) the Contractor's breach of this agreement; or
(b) any act, omission or negligence of the Contractor or its subcontractor that causes or results in the Customer being in breach of the PDPA.

2.5 Where the Customer provides Customer Personal Data to the Contractor, the Customer shall make reasonable effort to ensure that the Customer Personal Data is accurate and complete before providing the same to the Contractor. The Contractor

shall put in placeadequate measures to ensure that the Customer Personal Data in its possession or control remain or is otherwise accurate and complete. In any case, the Contractor shall take steps to correct any errors in the Customer Personal Data, as soon as practicable upon the Customer's written request.

3. OBLIGATIONS OF CUSTOMER

3.1 Customer has the primary responsibility to ensure that consent of Data Subjects is obtained for the use of Personal Data in situations where such consent is required by the Act or the PDPA

3.2 Contractor acknowledges that it is responsible for its own compliance with all applicable data protection laws and that the Contractor does not determine the purpose for which or the manner in which the Personal Data shall be collected and processed.

3.3 Customer guarantees that the Personal Data transferred to the Contractor is collected, processed and transferred in accordance with applicable data protection legislation in respect of for example the legal grounds for processing and the requirement to provide data subjects with certain information.

4. PERSONAL DATA AND CONFIDENTIAL INFORMATION PROTECTION

4.1. The Contractor acknowledges and agrees that:

(a) it may use Personal Data solely and exclusively for the limited purpose of providing the Services to Customer,

(b) it shall limit access to Personal Data solely to its personnel and personnel of third parties approved according to Article 5 who have a need of such access in connection with the performance of the Services and have committed themselves to confidentiality, and grant that access in accordance with the security controls as set out in Article 7;

(c) it shall not disclose or transfer the Personal Data to any third parties, unless necessary and approved by Customer in advance and in writing;

(d) it shall reproduce the Personal Data only to the extent necessary for the Approved Use;

(e) it shall implement and maintain appropriate technical and organizational measures for Personal Data against unauthorized or unlawful processing and against accidental loss or destruction of, or damage to Personal Data, whereas specific requirements for data security are set out in Article 7. Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to the harm that might result from unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of Personal Data to be protected;

(f) state-of-the-art physical security measures shall be in place over the servers storing Personal Data as well as the logical controls requiring authentication before gaining access to Personal Data;

(g) it shall comply with Customer requests, as soon as possible, for access to, correction of, and destruction of Personal Data in the the Contractor's possession.

5. PERSONAL DATA TRANSFERS/SUBPROCESSING

5.1. The Contractor shall only subcontract processing of Personal Data in accordance with the general written authorisation set out in the section 5.2. and shall ensure that it has a written contract with any further contractors (sub-contractors) it engages to process Personal Data. That contract must impose obligations on the sub-contractor equivalent to those in this DPA and the Contractor shall ensure that such contractors (sub-contractors) complies with those obligations. The further Contractors or sub-contractors in the context of this section 5.1. are solely the Subcontractors approved by the Customer in the respective contract/DPA or otherwise.

5.2. The Customer provides a general authorisation to the Contractor to engage the Subcontractors and if necessary also other third parties to act as further Contractors (sub-Contractors) of the Personal Data. The Contractor shall give the Customer prior notice of any intended engagement of a third party as a further Contractor (sub-Contractor). If the Customer objects to that engagement of a third party, the Customer may (within 30 days of such change) escalate to the Contractor for discussion its objection.

5.3. The Contractor shall not transfer Customer Personal Data to a place outside Singapore without the Customer's prior written consent. If the Customer provides consent, the Contractor shall provide a written undertaking to the Customer that the Customer Personal Data transferred outside Singapore will be protected at a standard that is comparable to that under the PDPA. If the Contractor transfers Customer Personal Data to any third party overseas, the Contractor shall procure the same written undertaking from such third party.

6. PERSONAL DATA RETENTION AND ARCHIVING

6.1 The Contractor shall not retain Customer Personal Data (or any documents or records containing Customer Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of this Agreement.

6.2 The Contractor shall, upon the request of the Customer:
(a) return to the Customer, all Customer Personal Data; or
(b) delete all Customer Personal Data in its possession,

and, after returning or deleting all Customer Personal Data, provide the Customer with written confirmation that it no longer possesses any Customer Personal Data. Where

applicable, the Contractor shall also instruct all third parties to whom it has disclosed Customer Personal Data for the purposes of this Agreement to return to the Contractor or delete, such Customer Personal Data.

7. DATA SECURITY MEASURES

7.1. Contractor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of the varying likelihood and severity of the rights and freedoms of natural persons, implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and shall ensure that any of its employees or agents or other persons who it provides access to the Personal Data are obliged to keep it confidential.

7.2. In order to adhere to requirements in paragraph 7.1, the Contractor shall implement the technical and organizational measures to safeguard the personal data collected from **AHCS** .

7.3 The Contractor shall only permit the authorised personnel set out in [Schedule A1] to access Customer Personal Data on a need to know basis.

8. RIGHTS OF THE DATA SUBJECT

8.1 The Contractor shall provide the Customer with commercially reasonable assistance in relation to any request made by a Data Subject or by Customer for access to that person's Personal Data, to the extent legally permitted and to the extent the respective Data Subject or Customer do not have access to such Personal Data through its use of the Services. The Customer shall pay the Contractor for any reasonable costs incurred in providing such assistance within 45 days of receiving an invoice for such costs.

8.2 The Contractor shall not disclose the Data Subject's Personal Data to a third party other than at the written instruction of the respective Data Subject, unless otherwise required by law.

9. SEVERABILITY

In the event any clause of the DPA is considered to be invalid, unlawful, non-enforceable or null and void, this will not result in the invalidity, unlawfulness, non-enforceability or nullity of the entire DPA. In this case, the Parties are released from all rights and responsibilities ensuing from such a clause, but only in as far as this stipulation is invalid, non-enforceable or null and void. In this event, the Parties will use their best efforts to replace such a clause by a

valid clause that has the nearest possible economic and legal meaning and/or significance, as the invalid, non-enforceable or null and void clause.

10. CLOSING PROVISIONS

This DPA shall enter in force at the moment when the Processing of Personal Data commences (Effective Date) and shall survive valid and applicable thorough the duration of the Personal Data Processing. Unless provided otherwise in previous sentence this Data Processing Agreement expires also with the termination of the last of the respective contract between **AHCS** and Company ABC.

Each of the Customer and the Contractor has caused this DPA to be signed by its duly authorized representative and become effective as of the Effective Date written below.

Ascending Hope Community Services		**Company ABC**	
Signature:	_____	Signature:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____