CARES Data Protection Procedures and Guidance v. 1 Sept 2019

1. Purpose of document

This document should be read in conjunction with the CARES Data Protection Policy.

This document indicates the standard operating procedures adopted by CARES to comply with the requirements of data protection law in Singapore and overseas. In the event that a situation is not covered by these guidelines, CARES will consult the Personal Data Protection Commission (PDPC) website and guidance material for best practice.

This document is reviewed at least once every three years by the CARES Governing Board, but as an operational document may be updated in between reviews provided such updates are in compliance with the law and CARES Data Protection Policy.

Any questions on CARES' approach to data protection should be directed to the Data Protection Officer (DPO) at dataprotectionofficer@cares.cam.ac.uk.

2. Consent, Purpose and Notification obligations

CARES will seek consent for its standard personal data collections via the following routes. All Data Protection Notices will (at minimum) state the purpose for which the data is collected and give details of how individuals may withdraw consent if desired.

Personal data collection	**Process for obtaining consent**
Job application data from job applicants	Deemed consent for initial response to job advertisement. Job applicants requested to sign Data Protection Notice for Job Applicants when submitting the Job Application Pro-forma.
Personal files for current employees, including payroll and staff claims	Employees to sign Data Protection Notice for Employees at commencement of employment
Personal data to facilitate travel bookings	Explanation of purpose during email correspondence with travellers. Provision of information after such explanation deemed consent.
CCTV for security and compliance with lab licensing legislation	Publically displayed notice
Photography/videography for display on website or in other material	Displayed notices at all registration points for events where photography/videography will take place. Signed consent notices for photo shoots.
Contact information for registration at CARES events	Notice at registration point and specific opt-in for CARES mailing list
Contact information for CARES mailing list	Notice at sign up point and unsubscribe options included in mailings

For all new data collection scenarios, CARES will consult the best practice guidelines provided by PDPC and develop a specific standard operating procedure (SOP) prior to data collection commencing.

If individuals wish to withdraw consent at any time, they may make a request by contacting dataprotectionofficer@cares.cam.ac.uk . If CARES does not require the data for compliance with higher laws (eg. employment or immigration law) then CARES will comply with the request and cease using the personal data within 10 business days. For all withdrawal of consent requests, CARES will immediately review whether the data needs to continue to be stored; if no legal compliance or other legally compatible reason for continuing to store the data is found the default will be to delete such data.

3. Access and Correction Obligation

Procedure for Dealing with Access Requests

Any requests received in CARES for access to an individual's personal data shall be forwarded to dataprotectionofficer@cares.cam.ac.uk immediately.

The Data Protection Officer (or an authorised delegate) will proceed as follows on receipt of a request:

1. Log the request and the date received in the CARES Data Protection Access Log.
2. Verify the identity of the individual raising the request. In the event of the request being raised by a third party, the DPO will also verify the right of the third party to act for the individual concerned. If the identity cannot be verified or the third party cannot provide evidence that they are permitted to act for the individual concerned, then the request will be rejected.
3. If necessary, the DPO will clarify the specifics of the request with the requestor to facilitate a prompt response.
4. The DPO will verify that the data requested is not subject to legal privilege or any of the other Fifth Schedule exemptions. If previous requests have been received from the same requestor or if the request is repetitive, the DPO will consider whether exemption applies.
5. If the request is a complex one but not overly burdensome, the DPO will inform the requestor of the schedule of fees. Requests for personal data that the requestor can self-access (step 5 below) will not be charged for. All other requests will be charged based on staff time to complete (standard rate of SGD30/hour) and consumables utilised. The DPO will provide an estimate for acceptance by the requestor prior to work starting. The estimate and the eventual calculation of actual charges will be recorded in the CARES Data Protection Access Log.
   If the DPO assesses that the burden or expense of providing access would be unreasonable for CARES, then the DPO will consider whether exemption applies.
6. If the information requested can be accessed by the individual via CARES' ERP system, intranet or other system for which the requestor is entitled to a log-in, the DPO will ensure the requestor understands how to access (and if needed, correct) their data.

7. For any personal data held that the requestor cannot access via CARES systems, the DPO will give a timeline for response to the requestor and then seek help from CARES HR Executive or others to compile the data held by CARES.
8. The DPO will review the personal data held to ensure that providing it to the requestor will not:
    a. threaten the safety or physical or mental health of an individual other than the individual who made the request
    b. cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request
    c. reveal personal data about another individual
    d. reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his/her identity
    e. be contrary to the national interest
9. The DPO will supply the personal data and (if requested) the ways in which it has been used or disclosed during the preceding year (excluding disclosures to law enforcement). If no relevant personal data can be found, the DPO will inform the requestor of this. If an exemption applies and the request is rejected, the DPO will inform the requestor of this.
10. The DPO will record the response, the response date and any other notes in the CARES Data Protection Access Log. If any exemption applies and the request is therefore rejected, this will also be recorded in the Data Protection Access Log. Data relating to rejected requests should be filed with the Data Protection Access Log for at least 30 days after the rejection in case of PDPC appeal enquiry.

If the steps above are not completed within 30 days of receipt of the request, the DPO will notify the requestor by day 30 of the anticipated response timeline.

<u>Procedure for Dealing with Correction Requests</u>

Any requests received in CARES for correction of an individual's personal data shall be forwarded to dataprotectionofficer@cares.cam.ac.uk immediately.

The Data Protection Officer (or an authorised delegate) will proceed as follows on receipt of a request:

1. Log the request and the date received in the CARES Data Protection Correction Request Log.
2. Verify the identity of the individual raising the request. In the event of the request being raised by a third party, the DPO will also verify the right of the third party to act for the individual concerned. If the identity cannot be verified or the third party cannot provide evidence that they are permitted to act for the individual concerned, then the request will be rejected.
3. The DPO will verify that the data requested is not subject to legal privilege or any of the other Sixth Schedule exemptions.

4. The DPO will arrange for the correction to be made to CARES records and for a correction to be sent to any third party organisations to whom the personal data was disclosed in the preceding year.
5. The DPO will update the requestor that the correction has been made or the reason for rejection of the request.
6. The DPO will record the response, the response date and any other notes in the CARES Data Protection Correction Request Log. If any exemption applies and the request is therefore rejected, this will also be recorded in the Data Protection Correction Request Log. Data relating to rejected requests should be filed with the Data Protection Correction Request Log for at least 30 days after the rejection in case of PDPC appeal enquiry.

If the steps above are not completed within 30 days of receipt of the request, the DPO will notify the requestor by day 30 of the anticipated response timeline.

4. Accuracy Obligation

The following principles will apply in CARES:

- Whenever possible, CARES will collect personal data in writing directly from the individual concerned
- At least once annually CARES will review the personal data it holds and consider whether updated copies should be requested
- At least annually CARES will send email reminders to all staff on which it holds personal data to update on any changes to personal data

5. Protection Obligation

CARES has implemented the following measures to protect the personal data it holds and will review its protection arrangements at least annually to ensure they are robust and utilising best practice.

- All staff employment contracts, student agreements and visitor agreements contain confidentiality clauses
- CARES data protection policy and guidelines available via the CARES intranet
- Information posters reminding staff of obligations
- Staff with responsibility for handling personal data required to take the PDPC E-Learning programme at least annually and where relevant, the University of Cambridge e-learning programme
- Staff with no specific job responsibility for handling personal data encouraged to use the PDPC e-learning for professional development and reminded via internal newsletters on responsibilities
- Lock offices where personal data hard copies are held when unoccupied and restrict access to keys
- Restrict access to soft copy personal data through use of passwords and personally assigned log-ins. Encourage employees to set a short screen lock on their computers.
- Use of shredder to destroy documents containing personal data

- Where possible transmit soft copy personal data through secure link to CARES file storage system, rather than email attachment. If email attachment must be used, then password protect the file and send the password separately.
- Regular review of soft copy personal data held and full deletion of any data no longer required
- Installation of anti-virus software on all CARES computers and regular updates of anti-virus software.

6. Retention obligation

CARES will review personal data held annually and delete any personal data not required. In addition, the following retention deadlines will apply:

Accounting records and supporting documentation to accounting records	Statutory retention limit or five years, whichever is longer.
Job application data from job applicants who do not receive a job offer	Retain for maximum of 12 months after interview to ensure successful candidate passes probation, then destroy personal data of unsuccessful candidates.
Personal files for current employees, including payroll and staff claims	Retain for period of employment and for five years after end date of employment or current relevant statutory requirement, whichever is longer
Personal files for ex-employees, including payroll and staff claims	Retain for five years after end date of employment or current relevant statutory requirement, whichever is longer
Personal data to facilitate travel bookings	Retain until travel (and any associated insurance claims) have been completed and then destroy passport copies and other non-financial documentation. For regular travellers, obtain consent to keep travel documents on file. Retain financial documentation securely for statutory accounting retention period.
CCTV for security and compliance with lab licensing legislation	Retain for 30 days after footage is taken and then destroy.
Photography/videography for display on website or in other material	Review annually and delete any old photos no longer required for publicity or archive purposes
Contact information for registration at CARES events	If individuals do not consent to be added to the CARES mailing list for future events, destroy personal data within 30 days of the event.
Contact information for CARES mailing list	Review mailing list annually

7. Transfer limitation obligation

CARES will ensure that all service providers to whom it needs to transfer personal data for are under obligation to protect the personal data transferred to an equivalent standard as PDPA, even if those providers are not based in Singapore. CARES will do this by:

- Including requirement to protect personal data in service contracts where relevant
- Checking certification of providers is of an equivalent or greater standard than required under PDPA
- Checking the receiving organisation is subject to laws of equivalent or greater strength than PDPA
- Obtaining direct consent from the individual to whom the personal data relates if necessary

8. Accountability obligation

In order to properly discharge its data protection responsibilities, CARES has put in place the following infrastructure:

- CARES has an appointed Data Protection Officer, who may be contacted on dataprotectionofficer@cares.cam.ac.uk. The role of the Data Protection Officer is detailed in the CARES Data Protection Policy.
- The CARES Data Protection Policy and this guidelines document are available to staff and students via the CARES Intranet.
- The CARES website carries brief information on CARES' approach to data protection (relevant to members of the public) and contact details of the Data Protection Officer
- Staff with responsibility for handling personal data or management responsibility required to take the PDPC E-Learning programme at least annually and where relevant, the University of Cambridge e-learning programme
- Staff with no specific job responsibility for handling personal data encouraged to use the PDPC e-learning for professional development and reminded via internal newsletters on responsibilities