Cambridge Centre
for Housing &
Planning Research

Cambridge Centre for Housing and Planning Research
Standard Operating Procedure (SOP)

Data Protection

SOP ref:	Cam/CCHPR/SOP1	**Effective date:**	10 March 2014
Version:	1.0	**Review date:**	10 March 2015

Author:	Sarah Monk Deputy Director, CCHPR	Date: 10 March 2014
Signature:	Sarah Monk	
Approved by:	Michael Oxley Director, CCHPR	Date: 25 March 2014.
Signature:	M. J. Oxley	25 March 2014

Version	Date approved	Reason for change

Background

Staff have a duty to ensure anonymity of research participants where this has been offered, to ensure that data is kept securely at all times, and to comply with the Data Protection Act.

The Data Protection Act, 1998[1] came into force in March 2000. The act applies to all personally identifiable information about living individuals. It lists eight Data Protection principles, and these have implications for the Cambridge Centre for Housing and Planning Research (CCHPR) where research is being performed that involves individuals. The Act specifies that collection and processing of data relating to research subjects must be done fairly and lawfully and in line with data subjects' rights. In addition, there are implications concerning data security, confidentiality, and possible transfer outside the European Union (EU).

The eight principles of the Data Protection Act are as follows.

Data should be:
- fairly and lawfully processed;
- processed for limited purposes;
- sufficient and relevant;
- accurate;
- not stored for longer than is necessary;
- processed in line with data subjects' rights;
- secure;
- transferred only to countries with adequate security

The purpose of this Standard Operating Procedure (SOP) is to ensure that the staff and associates of CCHPR are both aware of and comply with the requirements of the Data Protection Act.

Definitions

Personal data
Personal data identify an individual. For example, name, address, contact details, date of birth, NHS number.

Sensitive personal data
Sensitive personal data consist of information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life or offences or alleged criminal offences.

Anonymised data
Anonymised data are information which does not identify an individual. Anonymisation requires the removal of personal data, i.e. name, address, full post code and any other combination of details that might support identification.

Pseudo-anonymised (pseudonymised) data
Pseudo-anonymised data are data that has been given a unique identifier, removing the need to refer to personal data. Unlike anonymised data, pseudo-anonymisation is a reversible process; there will be a process to allow the unique identifier to be linked to the personal data.

[1] http://ico.org.uk/for_organisations/data_protection last accessed 5 March 2014

Unique identifier
A unique identifier is a code used to uniquely identify each participant in a study.

Procedure

Who?
Every individual with responsibility for collecting, processing and storing participant data must follow the guidelines contained in this standard operating procedure. This applies to the use of both paper and electronic data.

When?
This SOP covers every stage of a study where collection, processing, access and transfer of data are involved.

How?

Participation in research will be anonymous unless the interviewee gives approval to the contrary. Best practice is to obtain written consent wherever practical. Personal information about interviewees will not be held in the same place as recordings or transcripts.

In most instances subjects must give written consent for their data to be processed. Before they can do this, they must be made aware of why the data are being collected and the specific purpose(s) for which the data will be used.

Transfer of data

Staff should ensure that appropriate security measures are taken to ensure that the data are not lost or does not fall into the wrong hands.

A risk-based approach should be used which may incorporate the following:

- couriered delivery with sender/recipient signatures (postal)
- tamper-proof or tamper-evident envelopes (postal)
- sending data to a secure fax machine (fax)
- acknowledge receipt of safe arrival.

Personal data/sensitive personal data should never be sent using unencrypted email messages. Staff should note that merely adding a password to data is not the same as encrypting data.

Data collection and processing

The PI is responsible for insuring that a confidential list containing the names of all participants in a research project, allocated to unique identifiers (pseudo-anonymised) is kept securely (e.g. in a locked drawer, in a room that is looked when not in use). This allows the investigator to reveal the identity of the trial participant should the need arise. Access to this information should be restricted and on a need to know basis.

Information should be modified so that those who might see it are not aware of individual identities, as early as possible in data processing. The use of unique identifiers instead of names or other identifiable information on research material should help to achieve this. However, staff should be aware that it could be possible to marry the unique identifiers back to the personal data and that some combinations of personal data (e.g. date of birth and postcode) could lead back to the participant. Personal data should only be collected where there is a specific reason to do so.

Document storage

Where personal data are collected, these should be held in a secure place. Access to this data should be restricted to only those study personnel who require it.

All paper subject data (e.g. contact details for follow-up interviews) should be stored in a secure room, in a locked cupboard or cabinet.

Participant personal data should not be left unattended on desks, the floor, or in pigeon holes etc. and the room should always be locked when not occupied.

Electronic data must be held in a password-protected, access controlled environment. Computer equipment must be stored in a secure room, which should be locked when not occupied. No-one should be able to access participant data unless authorised to do so. Care should be taken not to leave subject information visible on an unattended PC monitor. Special care should be taken where an unauthorised person may be in a position to view the data. CCHPR and associated staff should use a password protected screensaver whenever the computer is left unattended.

Where personal data is being recorded, this will be done using encrypted recording devices. When interviews are transcribed this will be done on CCHPR premises or transferred securely to a transcriber meeting the requirements of the research client.

Data gathered in research will be handled in a way that complies with agreed procedures for safe storing and archiving of data, and destroying data where appropriate. Data storage and management must comply with //Data Protection legislation <http://www.admin.cam.ac.uk/univ/information/dpa/>

Where data are likely to be transferred outside the EU, the Data Protection Act requires that steps must be taken to ensure that a standard of security such as would apply in the EU will be maintained once the data pass outside of the EU.

Document Disposal

Care must be taken when disposing of any documentation containing personal data. Such documentation should be shredded or disposed of by being placed in confidential waste bins or black bags marked up as 'confidential waste' and disposed of by Estates Department. Portering Services will collect confidential waste from departments. Confidential electronic information should be wiped from the hard drives of computers as soon as it is not longer required. Please note that just pressing the delete button does not delete a file from the hard drive. When wiping documentation from the hard drive advice should be taken from the IT team, email address LE IT Support landecon-computing@lists.cam.ac.uk.

Confidentiality

Data collected for research purposes, and secondary data that can identify individuals is to be treated as confidential. Staff may not disclose personal information to any other agency or individual.

Training

All staff handling data should complete the Cambridge University on-line course on Data Protection http://www.training.cam.ac.uk/event/100058

Reporting security incidents

Break-ins, attempted break-ins, probes for vulnerabilities and other security incidents in the University of Cambridge should be reported to CamCERT as soon as they are discovered. The preferred method of contact is by email to cert@cam.ac.uk. Mail to this address is monitored frequently during normal working hours and intermittently at other times. You should also contact CamCERT if you think that your password has been obtained by someone else or you suspect that someone has been misusing your email. The Director of CCHPR and the Land Economy IT team should also be notified as soon as possible.

CamCERT may pass details of a security incident to JANET-CSIRT for investigation, follow up, to assist in another investigation or simply for the records.

Reporting incidents where an intruder is suspected of having broken in to the system

- The system should be disconnected from the network as soon as possible, preferably immediately the problem is discovered. This applies across the board, including to servers - remember that the system may well be being used to attack other machines. It should not be switched off or restarted because valuable evidence can be lost.
  - if the machine is your responsibility you should also tell your Institutional Computer Officer as other systems in the institution may also be vulnerable to the attack.
  - if it is not your machine contact the system manager, either you or the system manager should also tell the Institutional Computer Officer.
- Send details to cert@cam.ac.uk. Remember to leave details of
  - the machine name and/or IP address (number)
  - any information you have about the incident
  - where you can be reached - remembering that the machine has just been disconnected.
- If the machine is yours and you do not feel that you are competent to investigate the machine yourself, ask your Institutional Computer Officer or CamCERT for advice

Reporting probes for security vulnerabilities

CamCERT welcomes reports of probes from system managers of machines on the CUDN; probes, attempted and actual break-ins should be reported to cert@cam.ac.uk, with an extract from the log including:

- the name and/or IP address (number) of the probed machine
- the name and IP address of the attacking machine
- the port probed
- the time of the probe
- an indication whether the machine is NTP synchronised.

Staff signatures

All staff must sign the attached statement and keep a copy. The top copy will be kept by the administrator. Staff must re-read and re-sign each time the SOP is modified.

STATEMENT BY STAFF

This is Version 1.0 dated 10 March 2014.

I HAVE READ THE CCHPR STANDARD OPERATING PROCEDURE FOR RESEARCH AND CONSULTANCY PROJECTS WHERE OFFICIAL DATA AND/OR PERSONAL INFORMATION IS USED.

I AGREE TO COMPLY WITH THE REQUIREMENTS OF THIS DOCUMENT.

Signed...

Name (print) ....

Date...