AdvoCard
Data Protection Policy

Background

AdvoCard is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 1998.
We need certain personal information or 'data' about our Board of Directors, personnel, volunteers, advocacy partners, AdvoCard service users and other contacts. Some information may be needed for administrative purposes, for example to pay staff wages. Other data may be needed for us to send information to people, such as meeting minutes or newsletters.
This policy aims to ensure that AdvoCard complies with the Data Protection Act 1998 and that personal information about people is collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.
The policy applies to everyone who works with AdvoCard, including employees, sessional workers, consultants, volunteers, placement students, Board members, and members of recruitment panels.
All these people will be expected to read and comply with this policy.

Policy Statement

Notification

The government's Information Commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data by the data controller. People can consult the register to find out what processing of personal data is being carried out by a particular data controller. Notification is the process by which a data controller's details are added to the register. The Data Protection Act 1998 requires every data controller who is processing personal data to notify unless they are exempt.
AdvoCard is a data controller and is registered with the Information Commissioner; registration number (). AdvoCard will only process data in accordance with their register entry.

The Eight Data Protection Principles

AdvoCard guarantees that all processing of personal data will be done in accordance with the eight data protection principles.

Principle 1:
Personal data shall be processed fairly and lawfully, and in particular shall not be processed unless certain conditions are met, (as described in Appendix 1).

AdvoCard will always obtain a person's consent to process personal information about them and explain what the information will be used for.
Any AdvoCard form that gathers information about a person will ask them to indicate consent and contain a statement explaining what the information will be used for.

Principle 2:
Personal data shall be obtained only for specific and lawful purposes and not processed in a manner incompatible with those purposes.

AdvoCard will explain what a person's personal information will be used for and will not use it for any other purpose.

Principle 3:
Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.

AdvoCard will not collect any personal information that it doesn't need.

Principle 4:
Personal data shall be accurate and, where necessary, kept up to date.

AdvoCard will review and update information as necessary to ensure that information held is accurate and up-to-date.

Principle 5:
Personal data processed for any purpose shall not be kept for longer

than is necessary for that purpose.

AdvoCard will not keep personal information for longer than we need to.
See Appendix 2: Retaining and Disposing of Information.

Principle 6:
Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.

AdvoCard understands and will the respect the rights people have regarding the information that is recorded about them.
These are outlined in Appendix 3: Rights of Data Subjects.

Principle 7:
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

AdvoCard will ensure that personal information will only be accessible to people who need to use it in the course of their work.
See Appendix 4: Security of Data.

Principle 8:
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

AdvoCard will not transfer personal information outside the European Economic Area without the explicit consent of the individual.

Appendix 1:

Principle 1 of the eight data protection principles states that personal data shall be processed fairly and lawfully, and in particular shall not be processed unless certain conditions are met, as described in below.

Personal Data:

At least one of the following conditions is met:

- The data subject has given consent.
- The processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract.
- The processing is necessary for compliance with any legal obligation to which the data controller is subject, (other than a contractual obligation).
- The processing is necessary in order to protect the vital interests of the data subject.
- The processing is necessary for official functions, e.g. the administration of justice, the exercise of any functions of the Crown, a Minister of the Crown or a government department.
- The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights of the data subject.
- The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Sensitive personal data:

At least one of the following conditions is also met:

- The data subject has given his or her explicit consent to the processing of the personal data.
- To fulfill a legal obligation in the context of employment.
- The processing is necessary in order to protect the vital interests of the data subject or another person where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject, or consent by or on behalf of the data subject has been unreasonably withheld.
- The processing is carried out in the course of its legitimate activities by any body or association which is not established or conducted for profit, and exists for political, philosophical, religious or trade-union purposes, and is carried out with appropriate safeguards for the rights and freedoms of data subjects, and relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and does not involve

disclosure of the personal data to a third party without the consent of the data subject.

- The information has been made public as a result of steps deliberately taken by the data subject.
- The processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- The processing is necessary for the administration of justice, for the exercise of any functions conferred on any person by or under an enactment, or for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
- The processing is necessary for medical purposes and is undertaken by a health professional, or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional. In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
- The processing is of sensitive personal data consisting of information as to racial or ethnic origin, is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and is carried out with appropriate safeguards for the rights and freedoms of data subjects.
- The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Appendix 2: Retaining and Disposing of Information

AdvoCard will not keep personal information for longer than we need to. Information will be kept according to AdvoCard’s Schedule for Retaining Records.
Information will be disposed of in a way that protects the rights and privacy of data subjects, i.e. paper records will be shredded, electronic records will be erased.

APPENDIX 3: Rights of Data Subjects

People have the right to access their personal information held by AdvoCard. This includes the right to inspect confidential personal references received by AdvoCard about them.
Anyone who wishes to access their personal information held by AdvoCard should request this in writing to the Director or the Chair of the Board of Directors. Any such request will normally be granted within 40 days of receipt of the written request.

People also have the following rights regarding their personal information held by AdvoCard:

- To know to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision taking processes that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Information Commissioner to assess whether any provision of the Act has been contravened.

More information on these rights can be obtained from:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
CHESHIRE
SK9 5AF

Appendix 4: Security of Data

Hard-copy personal information held by AdvoCard is stored securely in locked, non-portable storage containers, and access to storage

containers is strictly limited to people who need to see the information in the course of their work.
Electronic information will be password protected and held on computers that are password protected or on disks that are kept securely.
AdvoCard will ensure that computer passwords are kept confidential. Computers will not be left switched on unattended without password protected screen-savers, and hard-copy records will not be left where they can be accessed by unauthorised personnel.
For further information regarding security of electronic data, see AdvoCard's Information Technology Policy.

Personal information held by AdvoCard will not be disclosed to third parties under any circumstances unless:

- The person has given their consent.
- AdvoCard is legally obliged to disclose the data.
- To safeguard national security.
- For the prevention or detection of crime including the apprehension or prosecution of offenders.
- For the assessment or collection of tax duty.
- To discharge regulatory functions (e.g. health, safety and welfare of persons at work).
- To prevent serious harm to a third party.
- To protect the vital interests of the person - this refers to life and death situations.

Under these circumstances, requests for disclosure of information to a third party must be received in writing and authorised by the Director or Chair of the Board of Directors.

APPENDIX 5 - Definitions

Data Controller
Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Personal Data
Information relating to a living individual who can be identified by the information or other information held by the data controller. This includes name, address, telephone number, expression of opinion about the person, and the intentions of the data controller in respect of the person.

Sensitive Data
Relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, and criminal convictions. Sensitive data are subject to much stricter conditions of processing, (see Appendix 1).

Data Subject
Any living individual who is the subject of personal data held by an organisation.

Processing
Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data, accessing, altering, adding to, merging, deleting data, retrieval, consultation or use of data, disclosure or otherwise making available of data.

Third Party
Any individual or organisation other than the data subject, the data controller or its agents.

‘Relevant Filing System’
Is defined in the Act as, “Any paper filing system or other manual filing system that is structured so that information about an individual is readily accessible.” Personal information covered by the Act can be held in any format, for example electronic (including websites and e-mails), paper-based or photographic, from which information about a person can be discovered.