Community Action Hampshire – trading as Action Hampshire and Action Portsmouth

DATA PROTECTION POLICY

All references to Action Hampshire in this document should be deemed to cover and include Action Portsmouth.

This Policy should be read in conjunction with Action Hampshire's Cyber Security, Information Governance Policy, Disciplinary Procedure (within Staff Handbook) and relevant confidentiality clause in contract/volunteer agreement.

This Policy applies to all team members who have access to Action Hampshire's data. Team members include staff, volunteers, trustees and consultants.

Introduction

Action Hampshire is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 1998. Action Hampshire processes information about its staff, volunteers, organisations, clients, funders and other individuals it has dealings with for a range of administrative purposes (e.g. to recruit and pay staff, disseminate information, administer projects and comply with legal obligations to funding bodies and government). In order to comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

All "processing" of personal data (including collection, holding, retention, destruction and use of personal data) is governed by the Data Protection Act 1998. The Act applies to all personal data - whether it is held on a computer or similar automatic system or whether it is held as part of a manual file. Personal data is defined as data which relate to a living individual who can be identified –
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
and can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Personal data can either be 'ordinary personal data' or 'sensitive personal data.' "Sensitive personal data" "Sensitive personal data" is information about an individual's:

- Racial or ethnic origin;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);

- Physical or mental health or condition;
- Sex life;
- Commission or alleged commission of any criminal offence; and
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

Sensitive personal data will not be held on an employee's personal file without his or her express consent - unless held in compliance with Action Hampshire's legal obligations (for example under health and safety legislation) or to protect the employee's vital interests (for example under the Equality Act 2010).

Under the 1998 Act, all organisations that process personal information are required to notify the Information Commissioner's Office. Action Hampshire as Data Controller is registered with the Information Commissioner.

Data Protection Principles

The Act 1998 requires that eight data protection principles be followed in the handling of personal data. These are that personal data must:

- be fairly and lawfully processed;
- be processed for limited purposes and not in any manner incompatible with those purposes;
- be adequate, relevant and not excessive;
- be accurate;
- not be kept for longer than is necessary;
- be processed in accordance with individuals' rights;
- be secure; and
- not be transferred to countries without adequate protection.

Action Hampshire will make every effort to ensure that it adheres to these principles and:

- observes fully the conditions regarding the fair collection and use of information
- meets its legal obligations to specify the purposes for which information is used
- collects and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- ensures the quality of information used
- ensures that the information is held for no longer than is necessary
- ensures that the rights of people about whom information is held can be fully exercised under the Act (i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information)
- takes appropriate technical and organisational security measures to safeguard personal information

- ensures that personal information is not transferred abroad without suitable safeguards.

Responsibilities

In the course of your work, you may come into contact with and use confidential personal information about people, such as names and addresses or even information about customers' circumstances, families, health and other private matters. This policy helps you ensure that you do not breach the Data Protection Act 1998, which provides strict rules in this area. If you are in any doubt about what you may or may not do, seek advice from your line manager. If you are in doubt and cannot get in touch with him/her or our data protection officer (Rosie Taylor), do not disclose the information concerned.

All team members are responsible for ensuring that:

- any personal data that they hold is kept securely
- the Office Manager is informed of all instances where data is lost, accidentally given to the wrong person or organisation or any other breach occurs.
- personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure may become a disciplinary matter, and may be considered gross misconduct in some cases. Action Hampshire will make every effort to ensure that personal information is

- kept in a locked filing cabinet, drawer, or safe. If it is computerised, personal information should be encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up.
- data should not be stored for any length of time on memory sticks. When a memory stick is needed to temporarily store data, an encrypted memory stick should be used. These are available from the Office Manager.
- team members should make every effort to ensure that data relating to Action Hampshire is not stored on, or transferred to, any personal computerised devise or equipment. If, in certain circumstances, this is deemed necessary, team members should contact the Office Manager who will request Senior Management approval and, should this be granted, they should ensure that any information is password protected.
- if the data is being sent electronically, any passwords should be sent in a separate email or telephoned.
- the most secure place to store data relating to Action Hampshire is on the shared drives on the server, which can be accessed remotely, so the need to store data on personal devices should, in any case, be minimal.

Trustees, associates and consultants must follow the same guidelines. They should refer any queries about the security of the IT equipment they are using to the Office Manager.

Requests for information in respect of Action Hampshire customers/clients

If you receive requests for information that may be classed as personal data (see definition in Introduction) or identifies a third party under the Data Protection Act you should normally obtain the permission of the individual who is the subject of the data before releasing it. You should check with your manager if you are unsure what types of data might be classed as personal and also the context of the request. All requests for the passing on of information should be recorded in the 'Record of Information Requests' form in the Data Protection folder on the network.

Staff Records and Subject Consent

Action Hampshire holds personal data about you. You have consented in your employment contract to the data being used. If this data changes, you should let us know so that our records can be updated.

All staff are responsible for:

- checking that any information that they provide to the organisation in connection with their employment is accurate and up to date.
- informing the organisation of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently. The organisation cannot be held responsible for any errors unless the employee has informed it of such changes.

In relation to the retention of records, the organisation follows the retention periods recommended by the Information Commissioner in its Employment Practices Data Protection Code.

You should therefore treat the following as guidelines for retention times in the absence of a specific business case supporting a longer period.

Application form	Duration of employment
References received	1 year
Payroll and tax information	6 years
Sickness records	3 years
Annual leave records	2 years
Unpaid leave/special leave records	3 years
Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
References given/information to enable references to be provided	5 years from reference/end of employment

Summary of record of service, e.g. name, position held, dates of employment	10 years from end of employment
Records relating to accident or injury at work	12 years

In many cases, Action Hampshire can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act (and to which special rules apply), express consent must be obtained. Agreement to the organisation processing some specified classes of personal data are a condition of employment for staff.

Subject access

An employee may request details of personal information which we hold about him or her under the Data Protection Act 1998. A small fee of not more than £10 may be payable. If an employee would like a copy of the information held on him or her, they please write to your manager. The requested information will normally be provided within 40 days.

If an employee believes that any information held on him or her is incorrect or incomplete, then they should write to or email their manager as soon as possible. The organisation will promptly correct any information found to be incorrect.

Any data protection queries should be addressed to your line manager or our Data Protection Officer – Rosie Taylor.