PEER ACTION
FOR EVERYONE AFFECTED BY HIV

PEER ACTION DATA PROTECTION POLICY

1. Introduction and purpose of the policy

Peer Action is required to maintain certain personal data about past and current members, contractors, volunteers, trustees, and providers for the purposes of satisfying operational and legal obligations. We recognise the importance of the correct and lawful treatment of personal data. The types of personal data that Peer Action may require include information about: a current, past and prospective member, contractors, volunteers, trustees, and providers; suppliers and others with whom it communicates.

This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998. Peer Action fully endorses and adheres to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation, and storage of personal data. Employees and any others who obtain, handle, process, transport, and store personal data for Peer Action must adhere to these principles.

Peer Action is concerned with respecting the rights of individuals when processing their personal information. This can be achieved by being open and honest with them about the use of information about them and by following good data handling procedures.

2. Legal Definitions used in the Data Protection Act

Data includes computerised and manual filing systems that are structured by reference to individuals and readily accessible, for example, card indexes, case file records.

Data controller is Peer Action in its capacity as a collector of information. Any person who handles Personal Data information on behalf of Peer Action is bound by the legal requirements of the Data Protection Act. Any such person does not act as an individual, but as a representative of the data controller. (***Peer Action is exempt from the legal requirement of registration with the Information Commissioner about the data it holds, it however retains a voluntary registration to comply with wishes of Funders)***

Data Subject is an individual about whom data is held. Data subjects at Peer Action can include:

- Service users or members
- Carers of service users
- Organisation contact persons

Donors (individuals or organisations)

Employees and prospective employees through recruitment

Trustees and volunteers

Personal Data means data about a living individual who can be directly identified from that data i.e. name and address, National Insurance or NHS number etc. This specifically precludes information such as phone numbers or emails details which being transient do not necessarily identify a person. – Peer Action will however treat such details as if they were Personal Data.

Processing means virtually everything from data collection, updating, correcting, storage, and use to data destruction. There is probably nothing that can be done to personal data that would be outside the scope of the Act.

Sensitive Data means personal data that includes information about:

Racial or ethnic origin of the person.

Their religious beliefs or other beliefs of a similar nature

Their physical or mental health or condition

Their sexual orientation

Their gender identity

Their HIV status

Their political opinions

Whether they are a member of a trade union

Their criminal record.

Finance Data means any data pertaining to monies generated or expended by the work of Peer Action through donation or fundraising or running events.

Explicit consent is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Notification Notifying the Information Commissioner about the data processing activities of Peer Action as certain activities may be exempt from notification.

Information Commissioner - The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Disclosure Peer Action may share data with other agencies such as the local authority, funding bodies and other voluntary agencies. The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Peer Action to disclose data (including sensitive data) without the data subject's consent. These are:

Carrying out a legal duty or as authorised by the Secretary of State

Protecting vital interests of a Data Subject or other person

The Data Subject has already made the information public

Conducting any legal proceedings, obtaining legal advice or defending any legal rights

Monitoring for equal opportunities purposes – i.e. race, disability or religion

Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

3. Related Peer Action policies

Confidentiality

4. Legal background for this Policy

Data Protection Act 1998

Medical Reports Act (1988)

5. Principles of the Data Protection Act

The principles of this Policy are as follows:

Personal data should be processed fairly and lawfully

Data should be obtained only for one or more specified and lawful purposes

The data should be adequate, relevant, and not excessive

It should be accurate and where necessary kept up to date

Any data should not be kept for longer than necessary

Personal data should be processed in accordance with the individual's rights under the act

Data should be kept secure

Personal data should not be transferred outside the European Economic Areas unless the country offers adequate data protection

6. Compliance with these Principles

Peer Action will, through appropriate management, strict application of criteria and controls:

Observe fully conditions regarding the fair collection and use of information,

Meet its legal obligations to specify the purposes, for which information is used,

Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,

Ensure the quality of information used,

Take appropriate technical and organisational security measures to safeguard personal information,

Ensure that personal information is not transferred abroad without suitable safeguards,

Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,

Set out clear procedures for responding to requests for information.

Ensure that the rights of people about whom information is held, can be fully exercised under the Act. (*These are:*

The right to be informed that processing is being undertaken,

The right of access to one's personal information

The right to prevent processing in certain circumstances and

The right to correct, rectify, block, or erase information that is regarded as wrong information

The right to take action for compensation (see Compensation below) if the individual suffers damage by any contravention of the Act by the data controller

The right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.)

6.1 Data Collection

Informed consent

Informed consent is when a Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data and then gives their consent.

It is not strictly necessary to gain the consent of members before recording information about them, whether the data is Personal Data or Sensitive Personal Data and consent is not necessary for Personal Data where it is your legitimate interests to hold the information, and holding it doesn't harm the data subject.

There are some circumstances when you need consent to use people's data. For 'sensitive personal data', consent may be required. In other circumstances it is good practice to get consent whenever possible.

Peer Action will ensure that data is collected within the boundaries defined in this policy. When collecting data, Peer Action will ensure that:

The Data Subject clearly understands why the information is needed and what it will be used for, and what the consequences are should they decide not to give consent to processing

As far as reasonably possible, that the data subject grants explicit consent, either written or verbal for data to be processed, is competent enough to give consent and has given so freely without any duress

The Data subject has received sufficient information on why their data is needed and how it will be used

All Data Subjects will be given an 'Information for Members' leaflet outlining data collection and storage

Where sensitive data is to be requested from other agencies, Data Subjects will be asked to sign a Consent Form

6.2 Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers. Information will be stored for only as long as it is needed and will be disposed of appropriately. Peer Action retains member records for 7 years.

Paper records

Folder files may be kept where appropriate, necessary or required by law, in such circumstances these should be kept secure in a locked and secure area, room or cabinet are under lock and key with personal contact details and case notes held separately. This information is only accessible to Peer Action trustees, contractors and volunteers on a need to know basis. Information held on members is relevant to services they are accessing and any individual work that is being conducted with them.

Computer security

Peer Action does NOT have its own computers use for storing or handling of Data, nor any data stored on its own computers. Peer Action has its files stored on a protected DropBox that can only be accessed by authorised people and is password protected. The members of this list are regularly checked and updated and passwords changed on a regular basis (and immediately upon anyone leaving the group).

Steering Members and Trustees who access Peer Action Information are required to ensure that they have secure password protection on any and all of their devices they use to access Peer Action Data and services. Should authorised users keep local copies of non-sensitive files on their computers (e.g. for editing before updating the official version) this should be saved only to a password protected local volume).

Data-sensitive files on the DropBox drive are protected from unauthorised access by file passwords. Members accessing these files MUST NOT at anytime remove such password protection.

Should a user sell, dispose of, loan, repair or otherwise any computer, mobile device, Memory Sticks & removable media that has been used to access Peer Action Data at anytime during the devices lifetime – then the user must undertake to remove all passwords, links, documents etc. relating to Peer Action upon its disposal – preferable by means of a clean erase (format) and reinstall of the devices basic software.

Memory Sticks & removable media

Memory Sticks and removable media may be used for the transfer of work related documents, They must be password protected and not be used to back up work present

on any of Peer Action's computers or Cloud storage. The only case where unprotected documents are permitted on unprotected Memory Sticks & removable media is where such documents are for public release.

Any work related documents saved on a memory stick and removable media must be kept to a minimum in order to ensure that if the memory stick is lost data is not compromised.

Any loss of a Memory Sticks & removable media or mobile computer devices connected to the Peer Action Website, Facebook Page or DropBox must be reported immediately to the Trustees and appropriate action (such as wiping remotely such mobile devices and changing associated user passwords) must be done as soon as practicable.

Back Up

All of Peer Action's computers are backed up regularly by our cloud provider and additionally by the Chair of the Trustees or nominated person in order to preserve information produced and to safe guard from any loss of data from any hardware malfunction. All work related back up will be on an external hard drive, which is, password protected and held by the Chair of Trustees or nominated person.

It is Peer Action's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation which has been passed on/sold to a third party.

6.3 Data Access and accuracy

All Data Subjects have the right to access the information Peer Action holds about them. (There are certain exemptions to this laid out in the Data Protection Act i.e. employee redundancy plans, confidential references from an employer or information that may identify someone else). Peer Action will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes. In addition, Peer Action will ensure that:

It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection (this is the Director)

Everyone processing personal information understands that they are contractually responsible for following good data protection practice, that they are appropriately trained to do so, and supervised.

Anybody wanting to make enquiries about handling personal information knows what to do,

It deals promptly and courteously with any enquiries about handling personal information,

It describes clearly how it handles personal information,

It will regularly review and audit the ways it holds, manages and uses personal information and will evaluate its methods and performance in relation to handling personal information

All members, contractors, volunteers, and trustees are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

If a data subject wishes to request access to their personal information, they should make the request in writing to the Designated Data Controller as stated above. Peer

Action reserves the right to charge the maximum fee payable for each subject's access request, which is £10.00. Peer Action aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a data access request.

6.4 Financial Data

Financial data is anything to do with the management of the charity's finances and income. This is part of general accounting necessary to safe guard the financial stability of the organisation.

All data retained will be kept for the period specified in appendix 1.

All data will be handled and maintained following Peer Action's financial controls policy, procedure, and the auditing requirements as pre-set by the charity commission.

6.5 Complaints under Data Protection Act

Compensation

Under the 1984 Act, data subjects were only allowed to claim compensation through the courts where they had suffered damage because of inaccuracy or unauthorised disclosure. This right has been considerably extended to allow the data subject the right to claim compensation for damage caused by any breach of the Act and for distress in certain circumstances.

Making a Complaint

The regulation and enforcement of the Act in the UK is done by an independent public body known as the Information Commissioners Office (ICO). The ICO provides guidance to organisations and individuals and has various rights of enforcement against data controllers who do not comply with the Act. If a data subject feels that a data controller has not complied with the Act then the data subject has:

The right to complain to the ICO who will then investigate and if needed serve an information notice or an enforcement notice in case of non-compliance. Contact http://www.ico.gov.uk/complaints/data_protection.aspx

Appeal against the notices can be made to the Information Tribunal.

The right to sue the data controller

The Act also treats it as a criminal offence if:

A data controller having received a subject access request destroys the data rather than disclose it.

A data controller discloses personal data without the authority to do so.

A data subject does not comply with an enforcement notice.

A data subject knowingly or recklessly obtains, discloses, or procures the disclosure of personal information without the consent of the data controller.

<INSERT APPENDIX 1 & 2>

Revision History

Version	Date: -	Changes: -	Editor	OK
0.0	March 2015	As Issued	[name] – Chair	

Counter Signature/Approval

Signed:	
Position:	Date:
Review	Date

PEER ACTION
FOR EVERYONE AFFECTED BY HIV

Appendix 1 Archive Policy and Procedure: Introduction

Archiving Data within an organisation is an important facet to the data-protection act of 1998. In accordance to the same act and the Freedom of Information Act 2000, information needs to be held for a specific period. The scope of this appendix is to give a clear guide into the length that data needs to be retained. All data retained needs to be kept in accordance with the over-arching data protection policy that this is a part of.

Appendix 2. Data Schedule

Record	Statutory Minimum Retention Period	Statutory Instrument / Authority
Member casework records	None Exist PA Policy is for 2 year from member leaving	Not Applicable
Public Liability Insurance Records	40 years N/A	
Accident books, accident records/reports	3 years after the date of the last entry	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)
Accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985
Tax records and correspondence with the Inland Revenue	3 years after the end of the financial year	The Income Tax (Employments) Regulations 1993 (SI 1993/744)

Actuarial valuation reports	None Exist PA Policy is 3 years after the end of the financial year	Not Applicable
Inland Revenue approvals	none exist PA Policy is 3 years after the end of the financial year	not applicable
Money purchase & Expense Claims & receipts	None Exist PA Policy is 3 years after the end of the financial year	Not Applicable
Trust deeds and rules	None Exist PA Policy is 3 years after the end of the financial year	Not Applicable
Trustees' minute books	None Exist PA Policy is 3 years after the end of the financial year	Not Applicable
Steering Committee minutes	None Exist PA Policy is 3 years after the end of the financial year	Not Applicable
Records relating to children	until the child reaches the age of 21	Limitation Act 1980
Health and Safety Regulations Assessments	None Exist PA Policy is 3 years after the end of the financial year	Not Applicable

The following Entries are NOT applicable to Peer Action but are included in case of future Need: -

Medical records and details of biological tests under the Control of Lead at Work Regulations 1998	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998 (SI 1998/543)
Medical records as specified by the COSHH Regulations 1999	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 (SI 1999/437)
Records relating to Retirement Benefits	6 years from the end of the scheme year	The Retirement Benefits Schemes (Information Powers) Regulations 1995

Statutory Maternity Pay records	3 years after the end of the tax year	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960)
Statutory Sick pay records,	3 years after the end of the tax year	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894)
Wage/salary records	6 years	Taxes Management Act 1970

Counter Signature/Approval

Signed:	
Position:	Date:
Review	Date