The Social and Health Education Project

Data Protection Policy

Introduction
The Social and Health Education Project needs to collect and use data (information) for a variety of purposes about its staff, course participants, service users and other individuals who come in contact with the Project. The purposes of processing data include the organisation and administration of courses, the delivery of services, research activities, the recruitment and payment of staff, compliance with statutory obligations, etc. Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. The Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 confer rights on individuals as well as responsibilities on those persons processing personal data. Personal data, both automated and manual, are data relating to a living individual who is or can be identified, either from the data or from the data in conjunction with other information.

Purpose of this policy
This policy is a statement of the Project's commitment to protect the rights and privacy of individuals in accordance with the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003.

Principles of the Acts
The Project undertakes to execute its responsibilities in accordance with the eight Data Protection Principles/Rules as outlined below:

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to that individual, on request

1. Obtain and process information fairly
The Project will obtain and process personal data fairly and in accordance with the fulfilment of its functions.

SHEP will ensure that data subjects are aware, at the time the personal data is being collected, of: the identity who is collecting it; the purpose for collecting it; how the data will be used; the categories of persons to whom the data may be disclosed; and any other information which is necessary so that processing is fair.

In most cases individuals will have consented to the collection of their data by SHEP either because they have applied to enroll as a learner/course participant or applied to participate in some other SHEP service (eg Counselling or Advocacy Support), applied to work with SHEP, or because of the performance of a contract.

2. Keep it only for one or more specified, explicit and lawful purposes

The Project will keep data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes.

SHEP will state at the point of data capture (application forms, customer service forms, website) the purpose for collecting the information, that the information will be processed and kept only in a manner which is compatible with this purpose and that the obtaining, processing and retention of such information will be done in line with the Data Protection Acts.

A PPS number will only be requested from those participating in QQI accredited training courses – and from those who participate on SHEP courses with financial support from groups such as ETB, DSP..

3. Use and disclose it only in ways compatible with these purposes

The Project will only disclose personal data that is necessary for the purpose/s, or compatible with the purpose/s, for which it collects and keeps the data.

SHEP will ensure, by way of implementing a specific disclosure policy, that staff involved in processing personal data are aware of the purpose of collecting such data and use/process it only for that specific purpose or compatible purpose(s).

For the purposes outlined at 1 & 2 above, it may from time to time be necessary to disclose data subject's personal data to third parties.

The transfer of personal data will be compatible with the original purpose for obtaining such data and if it is not, consent for transfer will be sought.

The data subject will be informed of these disclosures at the time of obtaining the data via data protection notices on application forms, enrolment forms etc.

Where a data subject has been informed of the potential disclosure or where consent has been collected, it may then be acceptable to disclose relevant personal information to entities such as funding agencies.

Where consent is not in place, SHEP understands that it must have a legal basis for disclosing an individual's information.

4. Keep it safe and secure

The Project will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. The Project is aware that high standards of security are essential for all personal information.

SHEP stores all personal information in controlled access, centralised databases (including computerised and manual files) at its offices.

SHEP will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction.

5. Keep it accurate, complete and up-to-date

The Project will have procedures that are adequate to ensure high levels of data accuracy. The Project will examine the general requirement to keep personal data up-to-date. The Project will put in place appropriate procedures to assist staff in keeping data up-to-date.

SHEP relies on the individuals who supply personal information (staff, course participants, service users and others) to ensure that the information provided is correct and to update us in relation to any changes to the information provided. Notwithstanding this, under Section 6 of the Data Protection Acts, individuals have the right to have factual personal information corrected if necessary. If an individual feels that the information held is incorrect they should write to the Project Director. SHEP will reply to such a request within 40 days detailing either the confirmation of the rectification or erasure, or a full explanation as to why the request is being refused.

6. Ensure that it is adequate, relevant and not excessive

Personal data held by the Project will be adequate, relevant and not excessive in relation to the purpose/s for which it is kept.

SHEP will ensure that information sought and retained is the minimum amount needed for the specified purpose and is adequate, relevant and not excessive in relation to the purpose(s) for which it is kept. The methods of collecting personal information will be subject to periodic review to assess the continued need for information sought.

7. Retain it for no longer than is necessary for the purpose or purposes

The Project has a policy on retention periods for personal data. Retention times cannot be rigidly prescribed to cover every possible situation and SHEP will exercise judgement, taking account of statutory obligation and best practice in this regard in relation to each category of records held. However, the following particular requirements should be met:

Details of courses completed/certification are required to be kept indefinitely within the Project.

Pay, taxation and related employment records should be retained in accordance with the time periods set out in various Acts and Statutory Instruments governing taxation and employment law.

Personal data which is no longer required to be retained will be disposed of securely i.e. paper files confidentially shredded, disks wiped clean before disposal.

Where litigation may potentially arise in the future (e.g. in relation to accidents/personal injuries involving employees/participants or accidents occurring on SHEP property), the relevant records will be retained until the possibility of litigation ceases.

8. Give a copy of his/her personal data to that individual, on request

The Project will have procedures in place to ensure that data subjects can exercise their rights under the Data Protection legislation.

The right of access does not include a right to see personal data about another individual, without that other person's consent.

Should an employee, Committee member, member of a Board of Management, student, service user or creditor wish to access their personal information they should contact SHEP's Data Protection Officer (Ms Geraldine Flanagan) in the first instance and check if the data can be released routinely. The

individual may use the Data Protection application form or write a letter clearly stating that s/he is applying under Data Protection Acts. The individual will be asked to provide proof of identity.

The individual is legally entitled to a decision regarding the request within 40 days of the Project receiving the request. However every effort will be made by the Data Protection Officer to deal with the request as soon as possible.

If the individual is unhappy with the decision of the Data Protection Officer s/he has the right to complain to the Data Protection Commissioner who can investigate the matter.

Responsibility

The Project has overall responsibility for ensuring compliance with the Data Protection legislation. However, all employees of the Project who collect and/or control the contents and use of personal data are also responsible for compliance with the Data Protection legislation. All employees are charged with the responsibility of ensuring that all data that they access, manage and control as part of their daily duties is carried out in accordance with the Data Protection Acts and this Code of Practice.

The Project will provide support, assistance, advice and training to all departments, offices and staff to ensure it is in a position to comply with the legislation.

The Project has appointed a Data Protection Officer who will assist the Project and its staff in complying with the Data Protection legislation.

Employees found in breach of the Data Protection rules may be found to be acting in breach of or, in certain circumstances, committing an offence under the Data Protection Acts 1988 and 2003. All current and former employees of SHEP may be held accountable in relation to all data processed, managed and controlled by them during the performance of their duties in the organisation.

Procedures and Guidelines

This policy supports the provision of a structure to assist in the Project's compliance with the Data Protection legislation, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection.

Review

This Policy will be reviewed regularly in light of any legislative or other relevant indicators.

Definitions

of words/phrases used in relation to the protection of personal data and referred to in the text of the code of practice;

The Data Protection Acts – The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All SHEP staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation.

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Relevant Filing Systems - Any set of information organised by name, PPS Number (if applicable in an organisation), payroll number, employee number, student number or date of birth or any other unique identifier would all be considered relevant.

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Sensitive personal data - relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership. Individuals have additional rights in relation to the processing of any such data.

Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under section 4 of the Acts.

Data Processing - performing any operation or set of operations on data, including:

- · Obtaining, recording or keeping the data,
- · Collecting, organising, storing, altering or adapting the data,
- · Retrieving, consulting or using the data,
- · Disclosing the data by transmitting, disseminating or otherwise making it available,
- · Aligning, combining, blocking, erasing or destroying the data.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Act places responsibilities on such entities in relation to their processing of the data.

The Social and Health Education Project Ltd

Requests for access to personal data under the Data Protection Act 1988 and (Amendment) Act 2003

Under the Data Protection Acts, you have the right to be given a copy, clearly explained, of any of your personal data kept on computer or manual relevant filing systems simply by making a written request.

If you wish to access your personal data held by the Project you should contact the relevant staff member or SHEP's Data Protection Officer (Ms Geraldine Flanagan) in the first instance and check if the data can be released routinely.

If this is not possible you can make an application under the Data Protection Act 1988 and (Amendment) Act 2003.

You may use the Data Protection application form or write a letter clearly stating that you are applying under Data Protection Acts.

All applications should be addressed to Geraldine Flanagan, Data Protection Officer, Village Centre, Station Road, Ballincollig, Co. Cork.

To help us answer your request please be as specific as possible about the information you wish to see, and give as much information as you can to help us find it.

You are legally entitled to a decision regarding your request within 40 days of the Project receiving your request. However every effort will be made by the Data Protection Officer to deal with your request as soon as possible. You will be asked to provide proof of your identity.

If you are unhappy with the decision of the Data Protection Officer you have the right to complain to the Data Protection Commissioner who will investigate the matter for you. The Commissioner has legal powers to ensure that your rights are upheld.

Ms Geraldine Flanagan,
Data Protection Officer,
The Social and Health Education Project,
Station Road, Ballincollig,
Co. Cork.
Tel: (021) 4666 180
geraldine.flanagan@socialandhealth.com

Further details on your rights under the Data Protection Acts are available at the Data Protection Commissioners website www.dataprivacy.ie.

Office of the Data Protection Commissioner
3rd Floor, Block 6
Irish Life Centre
Lower Abbey Street
Dublin 1
Telephone: + 353 1 874 8544
Fax: from abroad: + 353 1 874 5405
E-mail: info@dataprivacy.ie

SHEP Data Protection Procedures Checklist
(from www.dataprotection.ie)

MAIN RESPONSIBILITIES

Rule 1: Fair obtaining:

- At the time when we collect information about individuals, are they made aware of the uses for that information?
- Are people made aware of any disclosures of their data to third parties?
- Have we obtained people's consent for any secondary uses of their personal data, which might not be obvious to them
- Can we describe our data-collection practices as open, transparent and up-front?

Rule 2: Purpose specification

- Are we clear about the purpose (or purposes) for which we keep personal information?
- Are the individuals on our database also clear about this purpose?
- Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each?

Rule 3: Use and disclosure of information

- Are there defined rules about the use and disclosure of information?
- Are all staff aware of these rules?
- Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.

Rule 4: Security

- Is there a list of security provisions in place for each data set?
- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data we keep?
- Are our computers and our databases password-protected, and encrypted if appropriate?
- Are our computers, servers, and files securely locked away from unauthorised people?

Rule 5: Adequate, relevant and not excessive

- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?
- Does a policy exist in this regard?

Rule 6: Accurate and up-to-date

- Do we check our data for accuracy?
- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure our databases are kept up-to-date?

Rule 7: Retention time

- Is there a clear statement on how long items of information are to be retained?

- Are we clear about any legal requirements on us to retain data for a certain period?
- Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?
- Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

Rule 8: The Right of Access

- Is a named individual responsible for handling access requests?
- Are there clear procedures in place for dealing with such requests?
- Do these procedures guarantee compliance with the Act's requirements?

Training & Education

- Do we know about the levels of awareness of data protection in our organisation?
- Are our staff aware of their data protection responsibilities - including the need for confidentiality?
- Is data protection included as part of the training programme for our staff?

Co-ordination and Compliance

- Has a data protection co-ordinator and compliance person been appointed?
- Are all staff aware of his or her role?
- Are there mechanisms in place for formal review by the co-ordinator of data protection activities within our organisation?