Data Protection Policy

The Policies outlined below are intended to comply with and refer to the principles outlined in the Data Protection Act 1998 (see appendix I)

Details of staff, volunteers, clients and candidates will only be stored with the consent of the individual – confirmed at the point of gathering the data – usually through application or by the initiation of the individual (they contact Creating Space for You CIC and volunteer the information).

Records will be kept electronically on password protected devices with access and distribution restricted to those individuals who will be using the data in order to undertake work for which the data is intended and supplied. This will include such things and communication, financial, payments, and data sharing as required to complete the work for which the individual has contracted with Creating Space for You (CIC). This may include:

Paid work, work experience, voluntary work, learning development,
Accreditation of learning through qualifications.

This may include sharing data with third parties namely:
Sub contracted facilitators/ assessors/ verifiers and with accredited organisations. Again such data sharing will only take place in line with and in adherence to the DPA 1998

Any wider use of data (such as for research, evaluation, case study publication) will be with permission of the individual or will be anonymised to ensure individual's cannot be identified or their personal details accessed.

Any persons gaining access to such data will be reminded of their responsibilities under the act when contracting with them.

On completion of a contract period personal data will be deleted unless the individual confirms that data be held on record for the purposes of ongoing communication. Again any historical records will only be retained if required through awarding bodies or legislation (for quality or financial audit purposes for example).

Last updated: 20/04/2016 Due to be updated by 20/04/2017

Appendix I

Data Protection Act 1998 – The Principles explained

Introduction

There are eight guiding principles to the Data Protection Act 1998 (DPA) which the council must adhere to when processing personal data. The DPA defines processing as obtaining, organising, adapting, accessing, using and deleting.

1. First Principle

"Personal data shall be processed fairly and lawfully"

In order to comply with the first principle; one of the following conditions from Schedule 2 must be met if personal data is being processed:

1. The 'data subject' has given their consent
2. The processing is necessary -
    a. For the performance of a contract to which the data subject is party, or
    b. For the taking of steps at the request of the data subject with a view to entering a contract
3. The processing is necessary to comply with legal obligation
4. The processing is necessary in order to protect the vital interests of the data subject
5. The processing is necessary for the Administration of justice
6. The processing is necessary for the legitimate interests of the data controller

(except where unwarranted because of prejudice or legitimate interests of data subject)

2. Second Principle

'Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes'

To comply with the second principle, the council must inform the Information Commissioner of all the purposes for which it processes personal data. If the reasons for processing this information are changed, both the Information Commissioner and the Data subject must be informed.

3. Third Principle

‘Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.’

It is the council’s responsibility to ensure that personal data is adequate enough to distinguish between data subjects with similar details. The council must also ensure that the information processed about a data subject is relevant and not excessive.

4. Fourth Principle

‘Personal data shall be accurate and, where necessary, kept up to date’

Where the council obtains information either directly from the data subject or via a third party, it must ensure the accuracy of the data. If the data subject informs the council of a (factual) inaccuracy, the data must be amended to reflect this. In order to maintain accuracy, it is the responsibility of the data subject to to inform the council of any changes.

5. Fifth Principle

‘Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes’

The council should not retain information for longer than it is required to fulfil the purposes for which it is collected. Legislation and business requirement based retention schedules are used to enforce this across directorates.

6. Sixth Principle

‘Personal data shall be processed in accordance with the rights of data subjects under the act’

The data subject has the right to request any information processed by the council relating to them, they also have the right to request their personal data to be rectified, blocked or erased. It is the responsibility of all staff in the council to be aware of the data subjects rights and to respond to such requests.

7. Seventh Principle

‘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.’

The council must have contingency plans to cope with or manage any unforeseen events, which may affect the processing of personal data. All staff must be aware of how the contingency plans affect them as well as knowing what security issues accompany data processing.

8. Eighth Principle

‘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’

If data is to be shared with an organisation outside the European Economic area, the council must assess adequacy by looking at the following issues:

1. The nature of the data.
2. The country of origin.
3. The country where the data is being sent.
4. The purpose for which the data is processed.
5. The security measures in place

A transfer can take place if any of the following conditions are met:

1. If the data subject grants permission
2. If it is required in the performance of a contract
3. If the data subject makes a request in order to enter into a contract
4. In the conclusion or performance of a contract in the data subjects interest
5. Under the order of the Secretary of State
6. Under the approval of the Information Commissioner
7. As part of legal proceedings/advice

Exemptions

The processing of some personal data may be exempt from certain sections of the act.

• Subject Information Provisions

Where a Subject Access Request is made, personal data may not be disclosed to the individual

• Non- Disclosure

Exemption allows for processing of information, which are exempt from the act

• The exemptions:

1. National Security
2. Crime and Taxation
3. Health, Education and Social Work
4. Regulatory Activity
5. Journalism
6. Research
7. Information available to the public
8. Disclosure required by law