Data Protection Policy

Document code	Effective date	Approved by	Description of Amendment	Review date
PO-DP	13/12/17	Leanne Edwards	N/A	12/18

References:

1. https://www.gov.uk/data-protection/the-data-protection-act

Introduction

1. The purpose of the Data Protection Act (1998), which came into force on 1st March 2000, is to protect personal data and it therefore provides the legal framework within which individuals' personal data must be handled.

2. People care about how personal information about them is used and they must be able to trust Youthforce to use it responsibly. All organisations owe a duty of care, but it is especially important for charities and those who work with children and young people. We cannot afford to lose our good reputation due to carelessness with personal data which – ultimately – we do not own, but hold in care for the person concerned.

Policy

Youthforce will therefore:

3. Register with the Data Protection Commission and notify them of the purposes for which we intend holding personal data, the subjects and data classes.

4. Meet all the requirements of the Data Protection Act (1998) as required under the terms of this registration.

5. Only keep data that is adequate, relevant, not excessive, accurate and up to date.

6. Incorporate into the Job Description of a named individual the responsibility to:
-Oversee the organisation's compliance with the Act.
-Regularly monitor procedures and recommend changes as necessary.
-Ensure that any short-comings are adequately dealt with.
-Ensure that Youth Force has full and up-to-date information on any changes in the Act.

Policy into Practice

7. Definitions
(Under the Data Protection Act 1998)

Data Anything that can identify a living individual counts as data, however it is kept and whatever it consists of. This includes computer or manual records, photos, videos, etc.
Data Controller In this instance Youthforce

Data Subject The individual whose data is being held.
Data Processing Anything we do with personal data (collecting it, holding it, using it, changing it, copying it, disclosing it, destroying it) all counts as processing.
De-personalised Data Data from which no identifiable person can be identified, even if linked with other data sources. This is outside the Act and may be passed to relevant organisations for bona fide purposes.
Personal Data Personal data relates to an individual who is identifiable from that data, or in conjunction with other data the Data Controller holds or is likely to obtain.
Sensitive Data Data on racial or ethnic origin, political opinions or beliefs, Trades Union Membership, physical or mental health, sexual life, any offences or alleged offence or court proceedings. Even the source data may indicate that the subject has a characteristic that is included within the definition of sensitive personal information.
Data Protection Practice
8. Our registration number is

9. Information of any kind can only be held on an individual if they know we have it and why we have it. It can only be processes for the purposes notified to the Data Protection Commission and no without informing the Commission, e.g. if we keep information about those in training courses, the funding Co-ordinator cannot then approach them for donations.

10. All documents seeking personal data must have an appropriate statement explaining:
-Why the information is needed
-What will be done with it
-How long it will be held and
-That it will not be sold or passed on without their consent.

11. Sensitive data can only be processed if
-The data subject has given explicit consent
-It is a legal requirement of the subject's employment
-It is necessary to protect the vital interests of the employment
-It is necessary for legal proceedings, medical purposes or monitoring of equal opportunities

Procedures

It is the legal responsibility of individual Trainers/Staff:

12. When holding personal data
To ensure the subject knows it is being held and why
Only use it for the purpose/s for which it was originally obtained
To take good care of it – security must be appropriate
Use it 'fairly'
To ensure that the data is: adequate, relevant, not excessive, accurate, up to date, and not held longer than necessary

13. When obtaining personal data
Not to deceive or mislead anyone as to what will be done with it
To ensure the individual knows what information will be used for

14. When data is obtained from someone other than the subject
To tell the subject as soon as practicable that you have their data and why and how you will use it

15. When disclosing personal data, to check that
The disclosure fits the purpose/s for which the data is being held
The person to whom information is being disclosed is authorised to have it
The data subject is aware that this type of disclosure is possible, or that there is an overriding reason – such as legal obligation
The information is not transferred outside the European Union without following the specific rules

Fundraising

16. Youthforce does not at present sell names of individual donors and will not without reviewing the policy and notifying all potential individuals beforehand, providing the opportunity for them to give consent.

Access to Data

17. Provided the Subject can prove their identity and unless the subject agrees to withdraw their request or fulfilling it would involve disproportionate effort, or it contains information about a third party, Youthforce will, within 40 days of written request and payment of £20 from a data subject, supply
A description of data held on the subject
The purpose for which it is being held
The source of the data
The person/s to whom the data will be disclosed (if any)

Quality Management Requirements

18. As a minimum requirement, centres must maintain the following records for seven years after the completion of the course/certification is granted:

A register of learners containing details of each learner and their ULN (where appropriate)
A register of achievement per registered learner (by unit and/or qualification where appropriate)
Names, dates of employment by the centre and CV's of tutors, assessors and internal verifiers
Records of standardisation/assessor/internal verification activity/meetings
Moderation reports
External verification activity/meetings
Records of appeals, complaints, access arrangements, allegations of malpractice and allegations of child/vulnerable adult abuse.
Samples of completed assessments as required and agreed with the EV

19. It is deemed appropriate that records are stored electronically if they are effectively backed up. Youthforce will:

Clearly identify themselves and/or organisations on behalf of which the data is being collected prior to the collection of any personal data.
Refrain from holding any personal data for any purpose other than that which has been stated, which must be relevant and not excessive.
Ensure personal data is only used for the expressed purpose for which permission has been provided in advance by the supplier of the data.

Upon completion of the course/programme must retain their portfolios as evidence. Centres are required to retain a sample of copies of portfolios and samples of learner's work, as agreed with the EV, until the next external verification course/cohort-based visit.