Serving and Protecting Selsey's Young People

Youth Dream (Selsey) Limited
Registered in England and Wales
Company Registration No. 8752886 Registered Charity No. 1155982

The Bridge Youth Support Centre

DATA PROTECTION POLICY

ICO Registration No: ZA264899

Registered Office:
Unit E Penny Lane, 118 High Street, Selsey, West Sussex PO20 0QG
Telephone: 01243 201616 E-mail: info@youthdream.co.uk

April 2017

1.0 Policy Statement

The purpose of this policy is to ensure compliance of the Charity with all of its obligations under the Data Protection Act 1998. The policy provides guidance on the maintenance of and access to records as set out in the Act.

2.0 Data Controller

The Chairman of the Board is the Data Controller as defined in the Data Protection Act 1998.

Data management responsibilities have been delegated to the Manager of The Bridge.

Data handling responsibilities have been delegated to the Key Worker – Administration Officer.

Data handling responsibilities include but are not limited to:

I. Implementing any policies regarding data protection
II. Ensuring that safe and confidential systems are in place throughout Youth Dream

3.0 Duty of Data Protection and Confidentiality

3.1 Employees working at for Youth Dream will work with and over hear confidential personal information relating to students, staff, volunteers, stakeholders and the wider community.

3.2 In order that personal information is handled according to the requirements of both common law and the Data Protection Act 1998, you are required to maintain the confidentiality of personal information and must follow the Charity's Data Protection Policy and procedures therein.

3.3 All Youth Dream employees and volunteers agree:

- To treat all information about students, staff, volunteers, stakeholders and the wider community as confidential.
- To adhere to Youth Dream Data Protection Policy and related policies.
- To only disclose personal Information in accordance with this policy.
- That any non-compliance with this Policy will be treated as misconduct and subject to Disciplinary Procedures.
- That all confidential information about Youth Dream, that is information not in the public domain, must not be disclosed.
- To maintain this confidentiality even when employment and volunteering has ceased for the protection of the individual.

4.0 Definitions

4.1 Personal data is information that relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining or disposing of information.

4.2 The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to information in education records. Examples would be names of staff and clients or pupils, dates of birth, addresses, national insurance numbers, assessment results, medical information, SEN assessments, reviews and some minutes of meetings.

4.3 Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sexuality and criminal offences.

4.4 There are greater legal restrictions on processing sensitive personal data than there are on personal data.

5.0 Data Protection Principles

5.1 Personal data shall be processed fairly and lawfully.

5.2 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 that purpose or those purposes.

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

5.4 Personal data shall be accurate and where necessary, kept up to date.

5.5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

5.6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

5.7 Computer based personal data will be stored in accordance with the provisions of the Data Protection Act.

5.8 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.

5.9 Personal data shall not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

6.0 Data Types

6.1 This policy covers data transferred by email, written forms, post, fax, text and social media entries or verbally.

6.2 Employees must:

I. Be able, if asked, to justify their sharing of personal information;
II. Maintain security to the level expected by the classification of the personal information, whether the sharing is in person, by email, written forms, post, fax, text and social media entries or verbally;
III. Not use removable media devices – such as memory sticks to share information, except in instances where this is the most sensible means of sharing where the memory stick must be encrypted with a code or password and where the code or password is shared separately to the memory stick. Codes or passwords should not be written down but memorised.

7.0 Sharing Data

7.1 Personal data requests must be made in writing to the charity and responded to within 28 days of receipt. If the data requested will take longer than 28 days to compile, a holding letter must be sent within 28 days of receipt of the request.

7.2 A charge can be made for the data requested, in line with the costs of the printing, postage and staff time to collate the data. A charge must be reasonable and not be used to discourage a request.

7.3 Before sharing or sending the personal information you must be satisfied:

I. Of the **identity of the recipient**; this includes internal colleagues, external third parties and individuals;
II. Of the **contact details of the recipient** – e.g. email address, fax number, phone number, address;
III. Of the recipient's **need to know and/or their entitlement to** the personal information, seeking written proof where necessary;
IV. That they are **authorised** to be in receipt of the sharing of the personal information

7.4 If in doubt, the personal information should be not shared. Instead, further details and assurance must be sought. For example,

I. Return the intended recipient's call using a known telephone number.
II. Verify the intended recipient's email address by checking against a known source.
III. Verify the intended recipient's postal address by checking against a known source (e.g. seeking copies of formal, official headed documentation).

Always consider the amount of information you are sharing.

7.5 The personal information to be shared must

I. Only be that required to fulfil the purpose or purposes behind the proposed sharing, or
II. Only be that defined on any court order or other document compelling disclosure and
III. Otherwise be accurate.

Adults requesting access to their child's data

7.6 A person who has parental responsibility for a child has a right to make decisions about their care and upbringing. The following people automatically have parental responsibility:

- All birth mothers
- Fathers married to the mother at the time the child was born
- Fathers who are not married to the mother but are registered on the child's birth certificate. The registration or re-registration must have taken place after December 2003.
- Civil partners and partners of mothers registered as the child's legal parent on the birth certificate.
- Others may acquire parental responsibility through a court residency or parental responsibility order
- Parental responsibility may be shared with the local authority if the child is subject of a care order

7.7 Automatic right to access is given to those with parental responsibility where the child is up to and including age 11.

7.8 Automatic right to access is not given to those with parental responsibility where the child is age 12 and over. After the age of 11 Fraser Guidelines and Gillick Competency should be applied (see Appendix A).

Under 16's requesting access to their own data

7.9 Children under the age of 12 will not have automatic rights to their records. Where a child under the age of 12 requests access to their own records, this must be done in conjunction with a person or persons with parental responsibility.

7.10 Children age 12 and over will not have automatic rights to their records and Youth Dream must be assured that the child meets the requirements of Gillick Competency and that Fraser Guidelines apply before any records are shared with the child .

7.11 When assessing Gillick Competency an interview and a written account of the interview must be made. A record should be made of the details of the decision making process.

8.0 Disclosure of Information

8.1 **EMAIL** - care should be taken when addressing all emails to prevent accidental sharing to unintended recipients

- Each email address should be double checked before pressing send
- Care should be given if the email software auto-completes email addresses
- When sending to more than one person or persons, use BCC so as not to disclose one recipients personal email address to another recipient
- Use the "Delivery Receipt" and "Read Receipt" facilities within the software to ensure delivery and readership by the correct recipient
- Confidential emails should have the word CONFIDENTIAL in capital letters in the heading
- The first paragraph of the email should be the following disclaimer or similar: *The information contained in this email is strictly confidential and is intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this email in error, please notify the sender.*
- Where deemed necessary the "call and confirm" approach should be used, in so much as a follow up telephone call can be made to ensure that the recipient received the email

8.2 **POST** – sensitive personal information, especially regarding health or criminal record (actual or suspected) must be posted by special delivery or recorded delivery OR delivered in person, with the recipient signing to state that they have received the data.

8.3 **VERBALLY** – employees must protect the interests of the individuals subject to their personal information, for example their confidentiality and right to privacy, and the Charity's interests when

- Discussing personal information in conversations (be sure you are not overheard)
- Using telephones; or
- Recording information on voicemail, answering machines, video or audio devices.

Employees must

- Use any private offices, rooms or spaces or
- Otherwise take due care to ensure they are not overheard by anyone who has no need to access the information being discussed. For example, calls must not be made or taken in confined public spaces or on public transport.

8.4 **FAX -** No fax facilities are currently available within the Charity office or The Bridge. Should this change then this policy will require updating.

9.0 Responsibilities

9.1 All staff are personally liable in their duties for complying with the Data Protection principles.

9.2 Trustees of the charity are responsible for ensuring that they fulfil their duties with regard to the Act.

9.3 All systems which contain information about individuals are identified and made secure. Managers need to be aware of databases holding personal data held by staff and be prepared to justify such databases as required.

10.0 Destruction of data

10.1 Records on individuals should be kept for a period of 7 years.

10.2 Records should be kept in a safe and secure place and should be marked with a destruction date.

10.3 Records should be destroyed in a permanent manner either by confidential shredding or burning.

APPENDIX A

What is Gillick competency? What are the Fraser guidelines?

When deciding whether a child is mature enough to make decisions, people often talk about whether a child is 'Gillick competent' or whether they meet the 'Fraser guidelines'.

Gillick competency and Fraser guidelines refer to a legal case which looked specifically at whether doctors should be able to give contraceptive advice or treatment to under 16-year olds without parental consent. But since then, they have been more widely used to help assess whether a child has the maturity to make their own decisions and to understand the implications of those decisions.

In 1982 Mrs Victoria Gillick took her local health authority (West Norfolk and Wisbech Area Health Authority) and the Department of Health and Social Security to court in an attempt to stop doctors from giving contraceptive advice or treatment to under 16-year-olds without parental consent.

The case went to the High Court where Mr Justice Woolf dismissed Mrs Gillick's claims. The Court of Appeal reversed this decision, but in 1985 it went to the House of Lords and the Law Lords (Lord Scarman, Lord Fraser and Lord Bridge) ruled in favour of the original judgment delivered by Mr Justice Woolf:

"...whether or not a child is capable of giving the necessary consent will depend on the child's maturity and understanding and the nature of the consent required. The child must be capable of making a reasonable assessment of the advantages and disadvantages of the treatment proposed, so the consent, if given, can be properly and fairly described as true consent."

Common Assessment Framework
Fraser Guidelines / Gillick Competency Checklist

The following should be used as guidance for practitioners in determining and recording their decision as to whether a young person is able to participate in the CAF process without the involvement and support from their parent(s) / carer(s).

Consider:-
1. Has the young person explicitly requested that you do not tell their parents/carers about the common assessment and any services that they are receiving?

2. Have you done everything you can to persuade the young person to involve their parent(s)/carer(s)?

3. Have you documented clearly why the young person does not want you to inform their parent(s)/carer(s)?

4. Can the young person understand the advice/information they have been given and

have sufficient maturity to understand what is involved and what the implications are? Can they comprehend and retain information relating to the common assessment and the services, especially the consequences of having or not having the assessment and services in question?
Can they communicate their decision and reasons for it?
Is this a rational decision based on their own religious belief or value system?
Is the young person making the decision based on a perception of reality? E.g. this would not be the case for a chaotic substance misuser.

5. Are you confident that the young person is making the decision for themselves and not being coerced or influenced by another person?

6. Are you confident that you are safeguarding and promoting the welfare of the young person?

7. Without the service(s), would the young person's physical or emotional health be likely to suffer? (if applicable)

8. Would the young persons' best interests require that the common assessment is done and the identified services and support provided without parental consent?

You should be able to answer YES to these questions to enable you to determine that you believe the young person is competent to make their own decisions about consenting to and taking part in the Common Assessment, sharing information and receiving services without their parent's consent. You should record the details of your decision making.