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

(including General Data Protection Regulation)

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

Youth Dream
April 2018

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 European Data Protection Directive 1995 and General Data Protection Regulation 2018. The policy provides guidance on the maintenance of and access to records as set out in the Act and Regulation.

2.0 Data Controller

2.1 The Chairman of the Board is the Data Controller as defined in the Data Protection Act 1998 or his delegated Board Member.

2.2 Data management responsibilities have been delegated to the Manager of The Bridge, as the Data Protection Officer.

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

2.4 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
III. Data is processed using documented instructions
IV. Staff observe confidentiality in data processing
V. Appropriate security measures are taken
VI. Appropriate technical and organisational measures are in place
VII. Assist in ensuring compliance
VIII. Returns or deletes data at the end of the contract period
IX. Holding of information to demonstrate compliance

2.4 Data falls under the following headings:
Legal Obligation
Vital
Public Interest
Contractual Obligation
Consent

3.0 Duty of Data Protection and Confidentiality

3.1 Employees and volunteers working 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.

3.4 Consent to hold the data should be achieved and evidenced if required.

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. **Data Subject** is the identifiable living individual.

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 or philosophical beliefs, trade union membership, physical or mental health, sexuality and sexual orientation, criminal offences, genetic data and, biometric data.

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

5.0 Data Subjects

5.1 Data subjects have:

The right to be informed – of what data is being used, why and for what purpose
The right of Access – to see what data is being processed
The right of rectification – to have data corrected if it is incorrect
The right to erasure – to have all data on them deleted
The right to restrict processing – to prevent their data being used (unless legitimate legal reason to the continuation of processing to occur)
The right to data portability – to move all their data to another processor and to be provided with their data so that they can
The right to object – to use of their data and data must not be further used
Rights in relation to automated decision-making or profiling – demand they not be automated and instead reviewed by a human

Data Subjects must be advised of their rights and how to exercise those rights (making a Subject Access Request, having incorrect data erased or rectified, etc.) See Appendix B, C and D.

6.0 Data Protection Principles

6.1 Personal data shall be processed fairly and lawfully and shall not be used for any other purpose than that it is primarily intended for.

6.2 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.

6.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.

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

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

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

6.7 Computer based personal data will be stored in accordance with the provisions of the General Data Protection Regulations. Computers holding data should have appropriate, suitable and robust software systems to protect the data from breaches. This includes the use of passwords, firewalls, virus software, etc.

6.8 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.

6.9 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.

6.10 Data subjects will be informed of the data that is kept about them and advised of their rights and how to exercise those rights (making a Subject Access Request, having incorrect data erased or rectified, etc.)

6.11 Under Privacy by Design, all new processes, technologies and systems must include privacy and protection of data as part of the design and implementation. Data Protection Impact Assessments should assess any risks involved in the processing and put in place measures to minimise them. Appropriate resources will be put in place to achieve the measures.

7.0 Data Types

7.1 This policy covers data transferred by email, written forms, post, fax, text and social media entries or verbally. It further includes IP addresses, biometric data and genetic data.

7.2 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.
IV. Ensure that no data is left visible on computer screens or desks. In this regard a Clear Screen Policy and Clear Desk Policy should be followed.

7.3 Incorrect Data

As soon as the organisation is made aware that data is incorrect (i.e. telephone number, address) this should be immediately deleted regardless of whether the correct data is known and available at the time of deletion. Correct data can be added when known but incorrect data must be deleted immediately.

7.4 Withdrawal of data

As soon as a Data Subject wishes their data to be withdrawn, all data should immediately be deleted. Staff will be within their rights to explain that the service provided will be more difficult to provide and may need to cease or be managed in a different way, i.e. if Youth Dream does not hold a telephone contact number for a client it may be impossible to make appointments with them and appointment making would have to be made in person.

It will be the responsibility of Youth Dream to find another way to manage the appointment making process for that client.

8.0 Sharing Data

8.1 Personal data requests, called Subject Access 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.

8.2 A charge cannot be made for the data requested.

8.3 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

8.4 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.

8.5 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, relevant and accurate.

Adults requesting access to their child's data

8.6 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

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

8.8 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

8.9 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.

8.10 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 (see Appendix A).

8.11 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.

8.12 For school pupils children under the age of 13 must have parental consent but from the pupil themselves from the age of 13.

9.0 Disclosure of Information

9.1 **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 taken if the email software auto-completes email addresses
- When sending to more than one person, 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

9.2 **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.

9.3 **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.

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

10.0 Responsibilities

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

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

10.3 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.

11.0 Destruction of data

11.1 Records on individual clients should be kept for a period of 7 years after the day they leave school or reach the age of 21, whichever is sooner.

11.2 Records on volunteers should be kept for a period of no more than 2 years after a volunteer has retired and no data required in the process of acquiring a DBS check should be kept once the DBS certificate has been received.

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

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

12.0 Breach of Data Security

12.1 In the event that there is a breach in the security of data, the Information Commissioners Office must be informed within 72 hours of the discovery of the breach.

12.2 A report must include details of the breach, what data is at risk and what is being done to minimise the impact.

12.3 The data Subject must be advised on discovery of the breach so that they can take steps to protect themselves.

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 must record the details of your decision making.

Appendix B

Privacy Notice for Clients

Youth Dream Data Protection Policy

Youth Dream holds personal and sensitive data on its clients. Youth Dream operates and commits to a Data Protection Policy. To see a copy of the policy please contact the Data Manager.

Data is held in order to contact young people and their parents/carers and support the young people while they are working with us. Records are kept securely and confidentially.

At times we may share data with a young persons school or college, local authority, partner organisations and agencies or HM Court Services. Youth Dream contributes to the West Sussex County Council Holistics System which protects identified young people and informs all agencies working with that young person of any updates.

It will depend on how old the young person is as to whether data held on them is given to them and a young person will be assessed using Fraser Guidelines and the Gillick Competency Checklist. Parents and carers can request information on their child.

Client data will be kept for a period of 7 years after the day they leave school or reach the age of 21, whichever is sooner. The young persons data will be destroyed securely and safely.

The young person is called the Data Subject and has the following rights:

The right to be informed – of what data is being used, why and for what purpose
The right of Access – to see what data is being processed
The right of rectification – to have data corrected if it is incorrect
The right to erasure – to have all data on them deleted
The right to restrict processing – to prevent their data being used (unless legitimate legal reason to the continuation of processing to occur)
The right to data portability – to move all their data to another processor and to be provided with their data so that they can
The right to object – to use of their data and data must not be further used
Rights in relation to automated decision-making or profiling – demand they not be automated and instead reviewed by a human

The Data Controller for Youth Dream is: Bob Arnold, Board Trustee.
The Data Protection Officer for The Bridge is: Kim Long, Manager.
ICO Registration Number: ZA264899

Appendix C

Privacy Notice for Volunteers

Youth Dream Data Protection Policy

Youth Dream holds personal data on its volunteers. Youth Dream operates and commits to a Data Protection Policy. To see a copy of the policy please contact the Data Manager.

Data is held in order to contact volunteers and to obtain a copy of their DBS certification. Any documentation required for the DBS application process will be kept until the certification has been issued and on receipt of the certification will be destroyed. Records are kept securely and confidentially.

Volunteer data will be kept for a period of 2 years after the last day of volunteering. The volunteer's data will be destroyed securely and safely.

The volunteer is called the Data Subject and has the following rights:

The right to be informed – of what data is being used, why and for what purpose
The right of Access – to see what data is being processed
The right of rectification – to have data corrected if it is incorrect
The right to erasure – to have all data on them deleted
The right to restrict processing – to prevent their data being used (unless legitimate legal reason to the continuation of processing to occur)
The right to data portability – to move all their data to another processor and to be provided with their data so that they can
The right to object – to use of their data and data must not be further used
Rights in relation to automated decision-making or profiling – demand they not be automated and instead reviewed by a human

The Data Controller for Youth Dream is: Bob Arnold, Board Trustee.
The Data Protection Officer for The Bridge is: Kim Long, Manager.
ICO Registration Number: ZA264899

APPENDIX D

Privacy notice for staff

Privacy notice for staff

Under data protection law, individuals have a right to be informed about how Youth Dream uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our charity

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work for our charity. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other
- information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records
- and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence and car insurance certificate
- Photographs
- CCTV footage
- Data about your use of the charity's information and communications system
- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the charity, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards clients
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Ensure the safety and welfare of our staff

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you go about withdrawing consent if you wish to do so. Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify Youth Dream's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us. Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment. Once your employment with us has ended, this file and the information therein contained deleted.

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- The relevant local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Your family or representatives - to act in your vital interests should the need arise
- Suppliers and service providers – to enable them to provide the service we have contracted them for such as payroll

- Financial organisations - in order to meet our contractual obligations in facilitating banking and financial services
- Our auditors - to meet our legal obligations to share data in order to ensure compliance to relevant legislation
- Health authorities - to protect your vital interests should the need arise
- Security organisations - to meet our legal obligations to share information where appropriate, such as safeguarding concerns
- Health and social welfare organisations - to meet our legal obligations to protect the welfare of staff and clients
- Professional advisers and consultants - to meet our public task obligations in providing quality educational services
- Police forces, courts, tribunals - to meet our legal obligations as a responsible employer
- Professional bodies - to meet our public task obligations in providing continuous professional development
- Employment and recruitment agencies - to meet our legal obligations in providing responsible recruitment practices
-

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights:

How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that Youth Dream holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances. If you would like to make a request, please contact the Data Controller.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe.

You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)

- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the Data Controller.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance. To make a complaint, please contact the Data Controller.
Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact
The Data Controller for Youth Dream is: Bob Arnold, Board Trustee.
The Data Protection Officer for The Bridge is: Kim Long, Manager.
ICO Registration Number: ZA264899