BLEND YOUTH PROJECT

DATA PROTECTION & CONFIDENTIALITY POLICY

SEPTEMBER 2025

blend youth project
raising aspirations, releasing potential

Data Protection & Confidentiality Policy: - *Procedures & Guidelines*

Statement of Intent

Blend Youth Project has a responsibility to ensure that personal information about employees and service users is kept confidential. In the course of your work you may come into contact with or use confidential information about employees and service users, (for example their names and home addresses, medical conditions, payment methods for example. This policy seeks to provide you with guidance in relation to your rights and responsibilities pertaining to your own information and that of service users.

This policy is aligned with UK GDPR, Data Protection Act 2018, Data Protection and Digital Information Bill (2024), KCSIE 2025, Working Together 2025, and DDSCP Information Sharing Guidance.

Policy Scope

Blend Youth Project collects, stores and processes personal information about staff, young people, parents or carers and other individuals who come into contact with the provision, in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) .

This policy applies to all personal data, regardless of whether it is in paper or electronic format.
This information is gathered in order to enable Blend Youth Project to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the provision complies with its statutory obligations. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with relevant legislation.

Why this policy exists

This data protection policy ensures Blend Youth Project:

- Complies with data protection law and follows good practice
- Protects the rights of staff, service users, parents and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

This policy is based on the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It also reflects the Data Protection and Digital Information Bill (2024) and the principles of the Information Commissioner's Office (ICO). It aligns with the duties set out in KCSIE 2025 and Working Together 2025, which permit lawful information sharing where necessary to safeguard children and young people.

The Data Protection Act 2018 is underpinned by eight important principles.
In summary, these state that personal data must be:

1. **Obtained and processed fairly and lawfully;**
   The conditions are either that the person in question has given consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the person in question and consists of information relating to: race or ethnic origin, political opinions and trade union membership, religious or other beliefs, physical or mental health or condition, sexual life, criminal offences both committed and alleged.

2. **Obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose;**
   This means that at least one specified reason for processing must be justified. There may be many reasons but there must be at least one.

3. **Adequate, relevant and not excessive for that purpose;**
   The Organisation will review personnel/service user files on an annual basis to ensure they do not contain a backlog of out-of-date information and to check there is sound business reason requiring information to continue to be held.

4. **Accurate and kept up to date;**
   If your personal information changes, for example you change address, you must inform your line manager as soon as practicable so that the Organisation's records can be updated. The Organisation cannot be held responsible for any errors unless you have notified the Organisation of the relevant change. In the same way, if data is processed, the updating of the details should take place where appropriate.

5. **Not be kept for longer than is necessary;**
   The Organisation will keep personnel files for no longer than six years after termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which the Organisation decides it does not need to hold for a period of time will be destroyed after six months. Data relating to unsuccessful job applicants will only be retained for a period of six months unless permission has been obtained to retain information.

6. **Processed in accordance with the data subject's rights;**
   Processing means any use of the data including (but not limited to) storage, viewing (use) and disposal.

7. **Kept safe from unauthorised access, accidental loss or destruction;**
   Secure, technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data. Data stored on removable media will be kept in locked filing cabinets. Data held on computer will be stored confidentially by means of password protection, encryption or coding and again only authorised employees shall have access to that data. The Organisation has network backup procedures to ensure that data on computers cannot be accidentally (or intentionally) lost or destroyed. Paper-based Personnel files are confidential and are stored in locked filing cabinets. Only authorised staff have access to these files. Files will not be removed from their normal place of storage without good reason.

8. **Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.**

This means not sharing (or even taking to or storing) data (including anonymous statistical data) with any other country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the processing of personal data.

Data Protection Risks

This policy helps to protect Blend Youth Project from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Blend Youth Project has some responsibility for ensuring data is collected, stored and handled appropriately. Each individual or team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **Valley CiDS Board of Directors** are ultimately responsible for ensuring that Blend Youth Project meets its legal obligations.

The **Valley CiDS IT Manager** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

The **BYP Senior Management** are responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Blend Youth Project holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

All **BYP Staff** are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the provision of any changes to their personal data, such as a change of address.
- Contacting the managers in the following circumstances:
    - With any questions about the operation of this policy, data protection law; retaining personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
    - If there has been a data breach;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they need help with any contracts or sharing personal data with third parties.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their Line Managers.
- **Blend Youth Project will provide training** to all employees to help them understand their responsibilities when handling data.
- **Employees should keep all data secure**, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager if they are unsure about any aspect of data protection.
- **It is the responsibility of the EMPLOYER** to produce policies, training and advice regarding Data Protection as well as the tools necessary to maintain compliance with the Act (lockable filing cabinets, I.T. Infrastructure, shredders, etc.).
- **It is the responsibility of the EMPLOYEE** to undertake working methods that comply with the Act, otherwise it will be the EMPLOYEE whom will be criminally liable following the breach of the Act.
- **A breach of data protection is also a disciplinary offence** and will be dealt with under the Organisation's disciplinary procedures.
- **If you access another employee's personnel records without authority, this constitutes a gross misconduct offence** and could lead to your summary dismissal.
- **Matters relating to the business and functioning of Blend Youth Project** (e.g. the investigation of complaints or internal consultation about future plans for the organisation) which must also be kept confidential.

Third Party Data Processors

Where external companies are used to process personal data on behalf of Blend Youth Project, responsibility for the security and appropriate use of that data remains with Blend Youth Project. Where a third-party data processor is used:

- A data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- Reasonable steps must be taken that such security measures are in place;
- A written contract establishing what personal data will be processed and for what purpose must be set out;
- A data processing agreement must be signed by both parties.

Collecting Information

Whenever information is collected about people, they should be informed why the information is being collected, who will be able to access it and to what purposes it will be put. The individual concerned must agree that he or she understands and gives permission for the declared processing to take place, and it must be necessary for the legitimate business of Blend Youth Project.

Examples of data collection include:

- Job Applications & associated personal information
- Volunteer records
- Parental Consent Forms for services users
- Referral Forms for service users
- Attendance Registers
- Sessional Evaluation Forms
- Incident Report Forms
- Photographs

Information Held

Personal Information is defined as any details relating to a living, identifiable individual. Within Blend Youth Project this applies to employees, trustees, volunteers, young people and other members of the public such as job applicants and visitors. We need to ensure that information relating to all these people is treated correctly and with the appropriate degree of confidentiality.

Blend Youth Project holds Personal Information in respect of its employees, trustees, volunteers, young people and other members of the public. The information held may include an individual's name, postal, e-mail and other addresses/contact information.

Personal Information is kept in order to enable Blend Youth Project to understand the history and activities of individuals or organisations and to effectively deliver and promote its services to its users and partner agencies.

Some Personal Information is defined as Sensitive Data and needs to be handled with special care *(see below).*

Sensitive Information

Sensitive information is defined by the Data Protection Act (2018) as that relating to ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sexual orientation, criminal proceedings or convictions. The person about whom this data is being kept must give express consent to the processing of such data, except where the data processing is required by law for employment purposes or to protect the vital interests of the person or a third party.

Data Processing & Storage of Personal Information

BYP retains personal data only for as long as necessary to fulfil its purposes and legal requirements. Records are reviewed annually and disposed of securely through shredding or secure electronic deletion. Where third-party disposal services are used, data processing agreements are required.

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

These rules describe how and where data should be safely stored:

- When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.
- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.
- When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing service**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones, without encryption.

- All servers and computers containing data should be protected by **approved security software and a firewall**.
- Personal and private information should only be **divulged on a need to know basis**, whether this is internally between staff and volunteers or to external agencies
- Where statistics are maintained for monitoring and/or marketing, e.g. funding monitoring, etc., this must be done in such a way as to maintain the confidentiality of the individual(s) wherever possible.

Data Use

Personal data is of no value to Blend Youth Project unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted/password protected before being transferred electronically**.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers**

Data Accuracy

The law requires Blend Youth Project to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort Blend Youth Project should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a detail when they call.
- Blend Youth Project will make it **easy for data subjects to update the information** Blend Youth Project holds about them.
- Data should be **updated as inaccuracies are discovered**. For instance, if a family can no longer be reached on their stored telephone number, it should be removed from the database.

Data Disposal

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the provision's behalf. If we do

so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Particular care should be taken to delete information from computer hard drives, pens drives etc. if a machine is to be disposed of or passed on to another member of staff.

Sharing Personal Data

We will not normally share personal data with anyone who is not linked to a young person but may do so where:

- There is an issue with a young person or parent/carer that puts the safety of our staff at risk.
- Our suppliers or contractors need data to enable us to provide services to our staff and young people – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share;
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud;
- The apprehension or prosecution of offenders;
- The assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- Where the disclosure is required to satisfy our safeguarding obligations;
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our young people or staff.

Duty to disclose information

There is a legal duty to disclose some information including:

- Child abuse and other safeguarding concerns, which will be disclosed to Social Care or other agencies within the parameters of the Information Sharing Protocol in the interests of promoting the safety/welfare of the young person.
- Drug trafficking, money laundering or acts of terrorism will be disclosed to the police.
- In addition, colleagues believing an illegal act has taken place, or that a user is at risk of harming themselves or others, must report this to the Chief Officer who will report it to the appropriate authorities. Users should be informed of this disclosure.

Technology

CCTV

If we use CCTV in various locations around the provision sites to ensure it remains safe, we will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we should make it clear where individuals are being recorded. Security cameras must be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Photographs & Videos

As part of our delivery of activities & services, we may take photographs and record images of individuals within our provision.

We will obtain written consent from parents/carers, or young people aged 18 and over, for photographs and videos to be taken of young people for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and young person. Where we don't need parental consent, we will clearly explain to the young person how the photograph and/or video will be used.

Uses may include:

- Within provision on notice boards and in flyers, brochures, newsletters, etc.
- Online on our website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the young person, to ensure they cannot be identified.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

Staff Responsibilities

All staff are responsible for checking that any information that they provide to Valley CIDS in connection with their employment is accurate and up to date. Staff have the right to access any personal data that is being kept about them either on computer or in manual filing systems.

Staff should be aware of and follow this policy, and seek further guidance where necessary.

Your Consent to Personal Information Being Held

The Organisation holds personal data about you and by signing your contract of employment, starter form, return to work form, etc., you have consented to that data being processed by the organisation.

It is therefore vital that we store information about you (Bank details for payroll, etc.,) and therefore, agreement to the organisation processing your personal data is a condition of your employment.

The organisation also holds limited sensitive personal data about its employees and by signing your contract of employment, you give your explicit consent to the organisation's holding and processing of that data, for example sickness absence records, health needs and equal opportunities monitoring data.

Subject Access Requests

All individuals who are the subject of personal data held by Blend Youth Project are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts, the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the HR Manager at HR@valleycids.co.uk. The HR Manager can supply a standard request form, although individuals do not have to use this. The HR Manager will always verify the identity of anyone making a subject access request before handing over any information.

Your Right to Access Personal Information

You have the right, on request, to receive a copy of the personal information that the organisation holds about you, including your personnel file and to demand that any inaccurate data be corrected or removed. This pertains to any organisation that stores information about you.

You have the right on request:

- to be told by the Organisation for what purpose(s) personal data about you is being processed;
- to be given a description of the data held about you and the recipients to whom it may be disclosed;
- to have communicated to you the personal data concerned and any information available as to the source of the data;
- to be informed of the logic involved in the decision-making concerning computerised processing.

What will Blend Youth Project do if Data Protection is breached?

Breaches

All staff members have an obligation to report data protection breaches or contact the management if they have concerns of such a breach. This will allow the appropriate personnel to investigate further and take the appropriate steps to fix the issue in a timely manner.

What to do if staff fail to comply?

If data protection is not followed, this will be discussed in supervision meeting with staff and may involve staff warnings.

Staff training

All staff and volunteers receive induction and refresher training on data protection, confidentiality and information sharing. Compliance will be monitored through supervision, audits and data breach reviews.

Review

This policy will be reviewed annually or sooner if there are significant changes to legislation or statutory guidance. Review will be overseen by the DPO and DSL and approved by the Valley CiDS Board.

Appendix 1: - Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject- young people and families	The identified or identifiable individual whose personal data is held or processed.
Data controller- management	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor / 3rd party -	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Appendix 2: - Confirmation of understanding & compliance

I hereby confirm that I have read, understood and agree to comply with Blend Youth Project's 'Data Protection & Confidentiality Policy'

Name ……..

Position/Post Held…….

Signed …….. Date ……

Once completed, signed and dated, please return this form to the Head of Youth Services.