DATA PROTECTION/ GDPR POLICY

2023 VERSION

Terms, Acronyms

Service Users

To include all children, young people (0-17) and vulnerable adults (18+) who access Dost's services

Staff

To include all employees, coaches, tutors, student placements, volunteers at Dost

Trustees

To include all Dost Trustees

Management

To include Director and Board of Trustees

Visitors

To include all visitors, funders, staff, volunteers and coaches from other organisations

Carers

To include all parents/ extended family/ foster carers, keyworkers, corporate parents, such as Children's Services

The Public

To include members of the public who may come into contact with Dost services or Service Users

Named Leads

Director - Marian Spiers
Designated Safeguarding Lead and Deputy Designated Lead – DSL/ DDSL

DSL - Marian Spiers (updated December 2023)
DDSL - Kelly Williams – ESOL Tutor (completed December 2023)

Supervising to Safeguard
Marian Spiers (completed October 2023)

Safer Recruitment
Marian Spiers (Updated November 2023)

First Aider at Work

Marian Spiers (updated July 2021)
Kelly Williams – ESOL Tutor (completed July 2021)

Mental Health First Aider

Marian Spiers (February 2021)

Data Protection Officer

Marian Spiers

Safety and Safeguarding Trustee

Thomas Edwards (DSL Trained 2021)

DATA PROTECTION/ GDPR

Introduction

This document sets out the appropriate management and protection of any personal data held in relation to any Service User or Staff Member involved with Dost; any supplier, contractor or agent; and any members of other organisations or the public approached as part of promotional or research activities (henceforth all termed as 'Data Subjects'). It responds directly to the legal requirements imposed by the UK Data Protection Act (DPA) of 2018 and the 2018 EU General Data Protection Regulation (GDPR) with regard to the collection, handling, storage and transmission of any personal data received from any such Data Subjects.

What is data protection?
The Data Protection Act (DPA) is designed to:

- Safeguard the handling and use of personal information (termed 'personal data');
- Respect an individual's rights over their personal information or data; and
- Enable organisations to use personal data legitimately in order to operate their business/ organisation.

What is personal data?
Personal data refers to any information which relates to, and which can specifically identify, an individual living person. This includes, but is not limited to: names and addresses, telephone numbers, email addresses, credit or debit card details or HR details. (See Appendix A - Information Sheet on Personal Data)
[Note: Even anonymised data may constitute personal data if the individual is identifiable when the information is combined with other data held by the same organisation.]

When does the DPA apply?
The DPA applies whenever there is **ANY** processing of personal data. This includes collecting, handling, storing, transmitting, or using the data in any way (including simply accessing the data, regardless of whether such access takes place from inside or outside the UK).
The DPA applies to **ALL** personal data which is stored, either (a) electronically (i.e., on a computer or server) or b) manually, if this is within any kind of filing system sophisticated enough to make the data readily accessible.

How does the DPA relate to Dost?
We collect personal data in order to develop a better understanding of our members and supporters so that we can make better decisions about our future programmes and services and to fundraise more efficiently. This allows us to progress our aim of working with young refugees and migrants and for them to connect, grow and feel supported to continue their journey in the UK.
Dost is bound by the terms of the DPA as we need to collect, store, access and disclose certain personal data associated with the people and organisations that we work with when carrying out the activities that enable us to:

- Monitor and evaluate our reach and impact;
- Inform Service Users of what services and activities we are providing;
- Inform others of the work we are doing that may benefit them; and
- Ensure we safeguard Service Users effectively.

We may gather some information indirectly, when information is shared with us by a third party. For example, Service Users may be recommended to one of our sessions or our Project by a friend or by being referred to us for support by a local authority or other charity.

However, because we recognise that any failure in the correct and lawful treatment of this personal data could not only cause real harm and distress to the individual to whom the information relates, but also undermine our reputation within the community, we strive to go beyond the simple letter of the law and, instead, try to align with its' deeper goal, by keeping data collection to a minimum.

Data Protection Policy Commitments

Dost fully endorses the seven data protection principles listed under the 2018 DPA and complies with both the DPA and wider EU requirements on GDPR by ensuring that any personal data we hold about Data Subjects is:

1. Processed lawfully, fairly and transparently.

Dost staff must always consult with the Director whenever planning any activity that involves the collection or use of any personal data. The Director should then assess the planned data use to ensure that there is a legitimate reason for requesting and retaining the Data Subject's information and that the use of such information will be in line with what that person would expect, before establishing and documenting a clear plan for how that information will be stored and accessed that is in line with the requirements of the DPA.

Dost must **EXPLICITLY** inform all Data Subjects about the nature of the required data, the purposes and processes for which it is being/ has been collected and any parties to whom it may be disclosed. (for example, funders) In addition, Dost staff must ensure that all forms and activities **ALWAYS** provide potential Data Subjects with the option not to share their personal information - unless this is a matter of vital interest, public interest or legal obligation.

The Director must ensure that reasonable requests by individuals to access or delete their personal data are enabled by means of an easily accessible Data Subject Access Request process, clearly signposted on the charity's online presence.

2. Obtained and processed only for specified and limited purposes

Dost Staff must only ever process personal data in a way which is compatible with the original purposes for which the data was obtained.

3. Adequate, relevant and not excessive.

The Director must ensure that the volume and extent of any personal data that the charity holds on a Data Subject is the minimum amount of data required to achieve the stated purpose.

4. Accurate and kept up to date.

Dost Staff, under the supervision of the Director, must take all reasonable steps to ensure the accuracy of all data and ensure that this is monitored, with regular correction or removal of any data that is no longer accurate or relevant. Dost uses Salesforce CRM database to record all information on young people, Staff, Trustees and has limited access to its named users depending on what information they need to do to perform their role.

5. Not kept for longer than is necessary.

The Director must ensure that an annual audit of all data collections is scheduled, undertaken and documented in order to review the nature of any personal information being held by the organisation and ensure that there is still a valid business reason for the information being retained. They must then ensure that any data no longer needed for the purposes for which it was obtained, and any information deemed unnecessary is securely and systematically destroyed.

6. Used with integrity and maintained in complete confidentiality.

Dost takes the integrity and confidentiality of any information shared with us, by or about Data Subjects, very seriously. In order to ensure data integrity, the Director should include in their annual review, an assessment of whether the continued existence and use of any data held by the charity, conforms with the original consent and whether this consent can reasonably be expected not to have expired as a result of the time elapsed since it was given.

In order to prevent unauthorised or unlawful processing of personal data and to protect against the accidental loss, destruction or damage of any data, Dost must ensure that all data is stored securely by means of limited-access, lockable or password protected files, databases, drives and facilities.

In addition, Dost must ensure that access to such data is limited to those employees, volunteers, temps, trustees and funders who reasonably require access to the data for the performance of their obligations and duties by ensuring that:

- Any doubt about a person's authorisation to be in any of Dost's workplaces is reported immediately to the Director (and/ or building supervisor/ centre management team if appropriate);
- Any desks, cupboards or rooms that hold confidential information of any kind are securely locked whenever they are not being actively supervised/occupied;
- Paper documents which are no longer required are shredded with a cross-cut shredder and CD-ROMs and USBs are physically destroyed when they are no longer required;
- Personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party;
- Access to databases is password protected and restricted to staff members with a legitimate requirement to access the system;
- Anti-viral software is installed and regularly updated on all organisational devices and staff are trained in effective anti-virus behaviour;
- Third party access to any database is password protected and is only made available to specific partner organisations who are working with us on specific programmes, who are only ever able to access the data of those young people whose data they have entered into the database; and
- Data is never transferred to any other country without it being established in advance that there is adequate protection, (at a level equivalent with the DPA).

7. Managed in a clear and accountable manner.

To ensure that Dost's commitment to all seven principles of the DPA can be easily scrutinised by the Information Commissioner's Office (ICO), our funders, our partners, and our service users, the Director, working in combination with the Trustees, must ensure that all actions contained within this policy document are supported by appropriate checklists and calendar reminders, and that the results of all reviews are clearly documented in readiness for any audit of our Data Protection process.

Practical Implementation

Data Subject consent

Whenever personal data is given to Dost; Staff must ask the Data Subject (or their parent/ carer/ guardian if the Data Subject is under 12) to give explicit consent to that information being stored and used.

In addition:

- The Data Subject (or their parent/ guardian/carer) must be fully informed of the nature of the data storage and all intended uses of the data; (stated on the Referral Forms)
- Data should only be stored if consent has been given - or if there is a legal obligation, in which case this must be clearly and adequately explained to the Data Subject or their carer;
- All consent forms must be retained and stored in a secure manner;
- The relevant personal data obtained should not be accessible to anyone other than parties declared at the point of consent being given; and
- Any individual who has their personal data held by Dost has the right to access such data and the prescribed process to obtain this (as described below).

Access to Personal Data by Data Subjects

Under the DPA, all Data Subjects have the right to:

- Be told whether any of their personal data is being processed;
- Be given a description of the personal data, the reasons why it is being processed and whether it may be given to any third-party organisation or other person;
- Be given a copy of the personal data (subject to such redaction as Dost considers necessary to comply with its' safeguarding obligations and/or to protect its' operational interests); and
- Be given details of the source of the data.
- Withdraw consent to processing at any time
- Ask us to erase personal data if it is no longer necessary in relation to the purpose for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
- Challenge processing which has been justified on the basis of our legitimate interest or in the public interest
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms
- Make a complaint to the supervisory authority.

Dost Staff must therefore make sure that all Data Subjects are aware of this policy and their rights under the DPA whenever asking for any personal information. They should further identify the Director as the appropriate contact person for any data requests and direct Data Subjects to the relevant contact details on the charity's printed and digital communications.
All Dost Staff must ensure that up-to-date contact details are included on all printed literature and consent forms, and the Director must ensure that appropriate information and contact details are clearly displayed on the Dost website. The Director must ensure that any access request from Data Subjects is answered as quickly as possible and the relevant information provided within 40 days of a written request.
The Director must verify the identity of an individual requesting data under any of the rights listed above and not allow third parties to persuade them into disclosing personal data without proper authorisation.
(*Note: In the event of a request for subject access or the amendment of personal information, Dost reserves the right to charge a limited fee to cover administrative costs.)

Publication of Charity Information Relating to Dost

As information published as part of press releases and promotional media is exempt from the DPA, Dost Staff must make it clear in all communications and at all events that any individual who wishes for their personal information to be excluded from any such promotional publications should inform the Director.

Data Relating to Service Users

To ensure full compliance with the principles of transparency, integrity and confidentiality contained within the DPA, Dost Staff must ensure that:

- Data protection statements are used on all registration forms along with information for individuals (including photo consent forms where appropriate);
- All consent forms are retained by an appropriate Staff member and filed appropriately; and
- A statement on what information we hold, why, and the Data Subject's right to view information is included on the Dost website.

Disclosure of Personal Data

As indicated in our Data Protection Statement, Dost reserves the right to, on occasions, share information with our funders, (for reporting purposes) and with other agencies that we consider might benefit our Service Users. However, Dost staff may share information in circumstances of public interest, legal obligation, or where Service Users are considered to be at immediate risk or might put others at immediate risk.
When information is shared with us or available publicly, we may use this information to gain a better understanding of our supporters. We do this in order to improve our fundraising methods and services.
We encourage our supporters and service users to regularly check and update their privacy settings with Dost and third-party organisations, including other charities

Third-party data processors

Third-party data processors are third party organisations or individuals that may provide Dost with data processing services under our instructions and who process personal data on our behalf.
For example, they may process data on behalf of Dost for specific purposes and services such as payroll and benefits providers; website hosting services; data archiving/destruction; any outsourcing activity etc.
If we are dealing with third party data processor(s) we must ensure any processor we choose adopts appropriate technical and organisational security measures to safeguard the personal data and that such measures are managed appropriately.

Staff Training

The Director (Data Protection Officer) is trained in Data Protection, and this is updated on an annual basis. Upon induction of any staff member or volunteer, they are made aware of what personal data is, what sensitive data is, how to keep data and how to report a data breach.

Special Considerations: Child Protection in Relation to this Data Protection Policy

Confidential Information and Retaining Records

As outlined in our Safeguarding Policy, Dost believes that all children, young people and their families, are entitled to have their privacy respected. However, where there are concerns about the safety or welfare of a Service User, Dost must share those concerns and the necessary personal information with those who can make decisions about actions required to safeguard them.
There is nothing in the DPA or any other legislation that prohibits the sharing of confidential and personal information where there are concerns about the safety or welfare of a child/young person, or where a criminal act may be being, or may have been committed - in fact, this is covered in the DPA by the legal bases of 'vital interest' and 'public interest'. However, to ensure complete transparency around this, all Dost Staff should:

- Explain to Service Users, openly and honestly, what, why and how information will, or could be shared and seek their agreement. (NOTE: The only exception to this are those situations where to do so would put that Service User or others at increased risk of significant harm, an adult at risk of serious harm, or if it would undermine the prevention, detection or prosecution of a serious crime, including where seeking consent might interfere with any potential investigation)
- Always consider the safety and welfare of a Service User when making decisions about whether to share any information about them. (Again, where there is concern that the child may be suffering or is at risk of suffering significant harm, then their safety and welfare must be the overriding consideration);
- Wherever possible, respect the wishes of Service Users who do not consent to share confidential information. In this case, information may still be shared if, in our judgement on the facts of the case, there is sufficient need to override that lack of consent (see the first bullet point above);
- Seek advice where there is doubt, especially where that doubt relates to a concern about possible significant harm to a Service User or serious harm to others;
- Ensure that any information shared is accurate and up-to-date, necessary for the purpose for which it is being shared, shared only with those people who need to see it, and shared securely; and
- Always record the reasons for a decision - whether this was to share information or not.

Information Sharing: Working Together to Safeguard Children

All Staff must ensure that any recordings or documentation related to concerns about a Service User's safety or welfare are held securely and that all records held on a computer comply fully with the DPA.
They should further ensure that these detailed records are kept until Dost is confident that the information is held accurately with the agency responsible for taking further action to safeguard the Service User, i.e., partner agencies, Social Care, Children's Services or the Police. The Director must compile a clear chronology of all decisions made and actions taken, and keep this on file even after the detailed records are deleted or destroyed.

Responsibilities

Overall responsibility for the effective implementation of the DPA lies with the nominated Data Protection Officer (currently the Director).

However, while the Data Protection Officer is responsible for ensuring that this policy and subsequent organisational administrative systems enforce the principles and specific obligations of the DPA, **ALL** Staff and Trustees of Dost are required to comply fully with this policy and the procedures referred to within it in order to ensure full compliance with the DPA's provisions, and to report any concerns in good time to the Data Protection Officer.

Disciplinary action may be taken against any individual who breaches any of the instructions or procedures set out in this policy. Even individuals who do not handle data as part of their normal work have a responsibility to ensure that any personal data they may see or hear during the course of their work remains strictly confidential and is not disclosed to any third party. This includes all personal data and any information extracted from such data. For example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer.

Trustees should be regarded as data controllers, if they process personal data either manually or by computer, whether on their own equipment or on equipment provided to them by Dost. Just as any other individual holding and processing personal information about others, Trustees must comply with this policy and the DPA, and must notify the Data Protection Officer of all purposes for which they access, hold or process any personal data.

Reporting

Staff should contact the Data Protection Officer directly if there is a breach in data protection or they are uncomfortable about any aspect of data protection at Dost (or the Chair of the Board of Trustees if their concern relates to the behaviour of the Data Protection Officer).
We will notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.
If staff know or suspect that a Personal Data Breach has occurred, they must not attempt to investigate the matter yourself. They must immediately contact the Director as the key point of contact for Personal Data Breaches and preserve all evidence relating to the potential Personal Data Breach.

Monitoring

As with all other policies at Dost, this policy will be subject to regular annual review, unless superseded by new relevant legislation.

Appendix A - Information Sheet on Personal Data

The UK GDPR applies to the processing of personal data that is:

- wholly or partly by automated means; or
- the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.

Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information?

Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.
Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
If personal data can be truly anonymised then the anonymised data is not subject to the UK GDPR.
It is important to understand what personal data is in order to understand if the data has been anonymised.
Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.
Information about companies or public authorities is not personal data.
However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

What are identifiers and related factors?

- An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.
- A name is perhaps the most common means of identifying someone. However, whether any potential identifier actually identifies an individual depends on the context.

A combination of identifiers may be needed to identify an individual.

The UK GDPR provides a non-exhaustive list of identifiers, including:

- name;
- identification number;
- location data; and
- an online identifier.
- 'Online identifiers' includes IP addresses and cookie identifiers which may be personal data.
- Other factors can identify an individual.

Can we identify an individual directly from the information we have?

- If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable).
- You don't have to know someone's name for them to be directly identifiable, a combination of other identifiers may be sufficient to identify the individual.
- If an individual is directly identifiable from the information, this may constitute personal data.

Can we identify an individual indirectly from the information we have (together with other available information)?

- It is important to be aware that information you hold may indirectly identify an individual and therefore could constitute personal data.
- Even if you may need additional information to be able to identify someone, they may still be identifiable.
- That additional information may be information you already hold, or it may be information that you need to obtain from another source.
- In some circumstances there may be a slight hypothetical possibility that someone might be able to reconstruct the data in such a way that identifies the individual. However, this is not necessarily sufficient to make the individual identifiable in terms of UK GDPR. You must consider all the factors at stake.
- When considering whether individuals can be identified, you may have to assess the means that could be used by an interested and sufficiently determined person.
- You have a continuing obligation to consider whether the likelihood of identification has changed over time (for example as a result of technological developments).

Appendix B – Dost Professional Referral Form

DOST PROFESSIONAL REFERRAL FORM

ABOUT YOUNG PERSON				
First Name				
Family Name				
Age				
Date of Birth	**Date**	**Month**	**Year**	
Age assessed DOB?				
Their Country				
Their First Language				
Name of School or College				
Sex/ identity	**Male**	**Female**	**Transgender**	**Other identity**
Level of English	**Basic**	**Intermed**	**Advanced**	**Unknown**
WHERE DO THEY LIVE?				
Address				
Postcode				
Their Mobile Number				
WHO DO THEY LIVE WITH? (Tick one)				
Family			**Foster carers**	
With friends			**Hostel/ Hotel**	
Supported housing			**Alone**	
EMERGENCY CONTACT				
Name parent/ carer/ keyworker				
Address				
Mobile Number				
HEALTH				
Health issues?	**YES**		**NO**	
Details				
Medication?				
CONSENT				
Does the young person know that you are making this referral?	**YES**		**NO**	
If not, why not				
OTHER PROFESSIONALS				
Do they have a Social Worker?	**YES**		**NO**	
Borough?				
Do they have a solicitor?	**YES**		**NO**	
Date of referral?				
REASON FOR REFERRAL				
Please say why you think the young person will benefit from attending Dost				
RISK FACTORS				
Please say if you are aware of any risk factors surrounding the young person attending - either for themself or for others (trauma/ self-harm/ PTSD/ mental health issues/ violent tendencies)				
PROFESSIONALS INVOLVED				
Please say which other professionals are involved with the young person and contact details if you have them				

Please send us your referral form and we will contact you and the young person soon.
Email to marian@dostcentre.co.uk

Appendix C - Dost Young Person Referral Form

First Name			
Family Name			
Country you come from?			
Age			
Date of Birth	**Date**	**Month**	**Year**
Age assessed DOB?			
Sex/ identity?	**Male**	**Female**	**Other identity**
First language?			
English level?	**Basic**	**Intermed**	**Advanced**
Name of School or College			
WHERE DO YOU LIVE?			
Address			
Postcode			
Your Mobile Number			
WHO DO YOU LIVE WITH? (tick 1)			
Family			
Foster carers			
With friends			
Hostel			
Supported housing			
Alone			
EMERGENCY CONTACT			
Name parent/ carer/ keyworker			
Address			
Mobile Number			
HEALTH			
Health issues?	**YES**		**NO**
Details			
OTHER PROFESSIONALS			
Do you have a Social Worker?	**YES**		**NO**
Do you know the Borough?			
Do you have a solicitor?	**YES**		**NO**
Date arrived in the UK?			
Date of joining?			

We are all equal here…RESPECT RESPECT RESPECT!
SPEAK NICELY, PLAY NICELY, BE NICE AND HAVE A NICE TIME!

I will respect and listen to staff and volunteers
I will be friendly and respectful to everyone
I will respect the Club and equipment
I will not fight and I will not get involved if others fight
I will not bring or use drugs, alcohol or weapons
I will come here to have fun and help others have fun
I will help out – I will look after my Club and keep it clean and safe

I agree to (please tick):	✓
Dost keeping my information safely and securely and contacting me about activities or services. I understand that Dost needs some information to keep me and others safe and I understand that Dost will only share my information with others who need to know this, for example funders or other organisations who may offer support to young people or if I or someone else is at risk if Dost doesn't share this information.	
Ask to see what information Dost has about me if I want to see this. I am aware I don't need to decide to share any personal information - although this may mean that I am unable to join in activities due to safety. Dost will delete all my information after a certain period of time.	
Talk to Marian or other Dost Staff, if I am not comfortable at any time during activities - so they can help me feel safe and secure	
Receive emergency medical treatment if my Carer is not available to answer and to share my Carer's details	
Being filmed or photographed during the activities. I understand that the photographs or film might be used to tell other people about what Dost does. If I don't agree, Dost will not use any images of me.	
I understand that I can make a complaint about something that happens at Dost and will speak to Staff about this	
I understand that enjoying the activity and being safe means, I need to follow the safety rules above.	

NAME:			
SIGN:		**DATE:**	

DATA PROTECTION	**2020**	**2021**	**2022**	**2023**	**2024**
Reviewed and revised (Marian Spiers)	December 2020		July 2022	September 2023	
Agreed by Trustees	December 2020 **(Michael Havard)**		September 2022 **(Michael Havard)**	October 2023 **(Michael Havard/ Bejal Shah)**	