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 Youth Work Project Manager (YWPM) whenever planning any activity that involves the collection or use of any personal data. The YWPM 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 YWPM 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 YWPM 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 YWPM, 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.

5. Not kept for longer than is necessary.

The YWPM 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 YWPM 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 YWPM (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 YWPM, 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;
- 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;
- 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
- Given details of the source of the data.

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 YWPM 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 YWPM must ensure that appropriate information and contact details are clearly displayed on the Dost website.

The YWPM 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.
(*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 YWPM.

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

<u>Special Considerations: Child Protection in Relation to this Data Protection Policy</u>

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 YWPM 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 Youth Work Programme Manager).

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).

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

Data Subject Access Request (SAR)

Why is this important?

Everybody has the right under the **Data Protection Act 2018** to make a request to any organisation, for a copy of the information that organisation holds about you.
There are many reasons why you may want to apply for an SAR. It could be to find out the reason why a certain decision has been made about you or you might want to establish whether an organisation has the correct information about you. It's important to know how to go about getting this information and also, what you can do if an organisation refuses to give it to you.

What is a subject access request (SAR)?

A subject access request is simply a verbal or written request under the Data Protection Act 2018 to an organisation asking for copies of personal data and any other supplementary information that organisation holds about you. A SAR enables you to understand how and why an organisation is using your data and to check that they are doing it lawfully.

What Information are you entitled to ask for?

A SAR gives you the right to request:

- whether the organisation is processing your personal data;
- a copy of the personal data they hold about you;
- any other supplementary information.

In addition, you may also want to ask to be provided with details of:

- the purpose for which your data is being processed
- the types of personal data being processed
- any third parties that your data is being shared with
- how long your data will be kept for
- how you go about making a request to have your data amended or deleted
- how the organisation became aware of data, if it was not provided directly by you
- whether the organisation uses any automated decision-making processes.

Applying for your SAR

You can make a SAR request to Dost verbally or in writing. If you make your request verbally, it's recommended that you follow it up in writing to provide a clear trail of correspondence. We have details on our website as to how you can apply for your SAR.

When making a subject access request you should provide us with the following information:

- Your name and contact details
- Any information used by the organisation which would distinguish you from others with the same name
- Specific details of the information you require together with any relevant dates – to help us deal with your request more quickly.

The ICO have a **template letter** which can be used when applying for your SAR.
Always keep a copy of your request together with proof of postage or delivery.
A SAR should be free of charge, although we may need to charge a reasonable administrative fee if you require additional copies or if we believe that the SAR is 'manifestly unfounded or excessive".
Dost will aim to respond within a month, to your request, but in certain circumstances we may need to extend the time for an extra two months.
In this case, we will inform you of the extension and the reason why it is needed.

Can an organisation refuse to provide you with an SAR?

We may refuse your request if your data includes information about another individual, except where:

- The other individual has agreed to the disclosure, or
- It is reasonable to provide you with the information without the other individuals' consent.

We may also refuse if we believe that the request is 'manifestly unfounded or excessive'.
In either case, we will provide you with the reason for this refusal/ decision.

How can you raise a concern regarding your SAR?

If you're unhappy with the way Dost has handled your SAR you should first **make a complaint to the ICO**.
If their reply does not resolve your concern than you can make a complaint to the **Information Commissioners Office (ICO)**