21 POLICY & PROCEDURE – DATA PROTECTION

1. AIMS AND PRINCIPLES

This policy sets out ESDAS' commitments to compliance with the requirements of the General Data Protection Regulation ("GDPR"), Data Protection Act 1998 and any successive legislation (together, the "Data Protection Legislation").

The enclosed procedures aim to ensure that all employees, volunteers and others who have access to any Personal Data held by or on behalf of ESDAS are fully aware of and responsible for handling Personal Data in line with Data Protection Legislation.

For the purpose of providing its services and acting as an employer, ESDAS collects and uses Personal Data about people with whom it works including, but not limited to past, current and prospective employees, clients, volunteers, funders and suppliers.

2. PRINICPLES FOR THE USE OF PERSONAL DATA

The Trustees are the people with specific responsibility for data protection within ESDAS.

To comply with Data Protection Legislation, the following principles are applied to the use of personal data:

a) it is processed lawfully, fairly and in a transparent manner

b) it is only collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

c) collection is limited to what is adequate and relevant in relation to the purpose for which the data is processed

d) all reasonable steps are taken to ensure that if any data is identified as being inaccurate it is erased or rectified without delay

e) it is kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the personal data is processed and may only be stored for longer periods if is being processed solely for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisation measure require the Data Protection Legislation to safeguard the rights and freedoms of individuals

f) personal data is processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing, accidental loss and destruction or damage, using appropriate technical and organisational measures.

3. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

ESDAS only processes Personal Data under one of the six lawful bases set out in applicable Data Protection Legislation:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

In summary, these six lawful bases are:

a) Consent- the individual has given clear consent
b) Contract – to carry out a contract with an individual
c) Legal Obligation – to comply with the law
d) Vital Interests – to protect someone's life
e) Public Task – to perform a task in the public interest
f) Legitimate Interests (unless there is a good reason to protect an individual's Personal Data which overrides those legitimate interests)

ESDAS primarily uses consent as the lawful basis for processing personal data. Data may also be processed on the basis of legitimate interest (eg. that it is necessary to process that data for purposes that meet the legitimate aims of the charity) as long as this is justified on balance against the potential impact on the individual.

4. LAWFUL BASIS FOR PROCESSING SPECIAL CATEGORY DATA

Special Category Data ("SC Data") is personal data that needs more protection because it is sensitive and includes racial or ethnical origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, a person's sex life and sexual orientation.

In addition to the six bases set out in section 3 above, Special Category Data will only be processed if **in addition** that processing meets one of the specific conditions set out in applicable Data Protection Legislation:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

In summary, those ten specific conditions are:

a) Explicit consent
b) Employment, social security and social protection
c) Vital interests
d) Not-for-profit bodies
e) Made public by the Data Subject
f) Legal claims or judicial acts
g) Reasons of substantial public interest
h) Health or social care
i) Public health
j) Archiving, research and statistics

ESDAS primarily uses explicit consent or employment as the lawful basis for processing SC Data. If an individual does not give explicit consent to store or process their SC Data then it must not be recorded.

5. LAWFUL BASIS FOR PROCESSING CRIMINAL OFFENCE DATA

Criminal Offence Data ("CO Data") is personal data relating to criminal convictions and offences or related security measures including information about criminal proceedings and data relating to unproven allegations.

There are 37 conditions under which CO Data can be processed as set out in applicable Data Protection Legislation:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/

Of the 37 conditions, ESDAS primarily uses the "safeguarding of children and individuals at risk" as the lawful basis for processing CO Data.

ESDAS may also process CO Data under the lawful condition of employment.

6. SECURITY OF PERSONAL DATA

ESDAS will maintain appropriate technical and organisational security measures to ensure security of Personal Data.

ESDAS has a detailed "Acceptable Use of IT" policy for employees which sets out that they must:

a) never share usernames or passwords
b) always keep PCs and mobile devices secured
c) log out or turn off devices when not in use
d) ensure that they only pass Personal Data on to others where this in compliance with Data Protection Legislation
e) not disclose Personal Data or discuss Personal Data within hearing of others outside the offices
f) keep all paperwork secure
g) clear their desks of paperwork at the end of each day
h) shred paperwork that is no longer required

ESDAS use a case management system (currently OASIS) to process information and Personal Data provided by clients seeking advice and support.

All information and Personal Data is regarded as being confidential between the individual and ESDAS unless expressly indicated otherwise.

Where it is considered necessary to share Personal Data with a third party, to provide a service to an individual or to refer them for further assistance, their explicit consent must be obtained.

Personal Data will only be shared without prior explicit consent if it is for lawful disclosure for :

1) Vital Interests and all the following apply:

a) there is a danger to someone's life (whether or not they are a client)
b) the danger is imminent
c) urgent intervention is needed (probably from the police or medial professionals)

2) Vital Interests due to a safeguarding issue for a child (under 18)

3) Vital Interests due to a safeguarding issue for an adult at risk where all of the following apply:

    a) the adult has care and support needs
    b) they are experiencing, or are at risk of, abuse or neglect
    c) they are unable to protect themselves because of their care and support needs

If an employee considers that disclosure without consent is required, they must refer to their Service Manager before taking action

The Service Manager and the CEO of ESDAS will decide if a breach of confidentiality is lawful and will document this decision and the lawful basis for it. Adult and Child Safeguarding policies must be applied.

Any Personal Data shared with a third party will always be the minimum necessary required to carry out the lawful purpose.

Where possible, any Personal Data which enables the identification of an individual should be removed from emails between ESDAS staff and outside the charity (eg. replacing names with case numbers).

In all cases the relevant consent must be obtained, or alternative lawful basis determined, for any processing or sharing of client Personal Data or SC Data or CO Data.

7. INDIVIDUAL'S RIGHTS

ESDAS will ensure that individual's can exercise their rights regarding any of their personal data that is stored or processed by the charity. This includes the:

a) Right to be informed – individuals will be informed that their personal data is being collected when it is provided by them to the charity
b) Right of access – individuals will be provided with a copy of their personal data, if requested, in less than one month of the request and without a fee
c) Right of rectification – personal data will be rectified promptly where an error is notified to ESDAS
d) Right to erasure – if an individual requests the erasure of their personal data this will be erased where holding that data is no longer necessary for the original purpose for which it was collected or processed or where consent to hold that information is withdrawn and is the basis for holding the data
e) Right to restrict processing – if an individual requests the restriction of the use of their data this will be considered and acted upon in the light of Data Protection Legislation at that date
f) Right to data portability – where personal data is held in a machine readable format, an individual can request that this is transferred electronically to another organisation where it is feasible to do so
g) Right to object – if an individual objects to the use of their personal data, this will be acted upon in light of the Data Protection Legislation applicable at that date
h) Rights related to automated decision making – ESDAS does not use personal data for automated decision making (eg. profiling)

All queries about processing Personal Data are promptly and courteously dealt with within the requirements of Data Protection Legislation.

8. NOTIFICATION OF PERSONAL DATA BREACHES

If an employee recognises that there has been a personal data breach, then they must report it to their line manager immediately. This will be reported to the CEO or Management Committee who will assess the breach against current Data Protection Legislation and determine how the breach should be reported.

In line current Data Protection Legislation, ESDAS will notify personal data breaches:

a) to the Information Commissioner's Office within 72 hours where feasible (unless the breach is unlikely to result in a risk to the rights and freedoms of individuals)

b) to the individuals affected without undue delay (unless the breach is unlikely to result in a high risk to their rights and freedoms)

Regardless of whether the break is required to be reported, ESDAS will maintain a record of any personal data breaches and take steps to rectify the situation that permitted a breach.

9. DATA PROTECTION RESPONSIBILITIES

The trustees (and ultimately the Chair of Trustees) have specific responsibility for Data Protection in the organisation.

ESDAS ensures that all employees and volunteers managing and handling Personal Data, SC Data or CO Data understand that they are responsible for following good information governance and assurance practice and for complying with Data Protection Legislation.

In addition, everyone managing and handling Personal Data is appropriately trained and supervised to do so. All staff receive online Data Protection Legislation training annually from an approved training provider.

Data sharing will only be carried out under an appropriate written agreement, setting out the scope and limits of the sharing and any disclosure of Personal Data will be following approved procedures.

All employees and volunteers are to be made fully aware of this policy and their duties and responsibilities under it and will take steps to ensure that Personal Data is kept secure against unauthorised or unlawful loss or disclosure.