Data Protection Policy

Definitions

Personal Data = any data that can be used to identify a person living or dead
Staff = All members of the DSWM workforce
Data Subject = actual person living or dead
Data Processor = Staff/Vols who add the data to the system
DSO = Data Security Officer
DC = Data Controller – is the organisation (DSWM)

Disability Solutions West Midlands (DSWM) retains personal/sensitive data about staff, volunteer's, clients, suppliers and other individuals for a variety of charity related reasons.

This policy sets out how DSWM will protect personal/sensitive data and ensure that staff understand the rules governing their use of personal/sensitive data to which they have access during their work. This policy requires staff to ensure that the DC or the DSO be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The purposes for which personal data may be used by DSWM:
Personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business/charity policies are adhered to (such as policies covering email and internet use etc.)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting and checking
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff/volunteer access to systems and facilities and staff/volunteer absences, administration and assessments
- Monitoring staff/volunteer conduct, disciplinary matters
- Improving services

Personal data
Personal data gathered by DSWM may include individuals' contact details, emergency details, and educational background. Information relating to identifiable individuals, such as job applicants, current and former employees, contract and other staff, clients, suppliers and marketing contacts, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Sensitive data
Personal data about an individual's racial or ethnic origin, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceeding. Any use of sensitive personal data should be strictly controlled in accordance with this policy.

Please be aware
This policy applies to all staff and volunteers within DSWM. You must be familiar with this policy and comply with its terms. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be, once approved, circulated to staff before being adopted.

Our Procedures

Fair and lawful processing

DSWM must process personal data fairly and lawfully in accordance with individuals' rights. No personal data should be processed or obtained without written consent from the data subject.

The DSO/DC responsibilities:

- Keeping the Board/Management Committee updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff/volunteers and those included in this policy
- Answering questions on data protection from staff, volunteers and Board members.
- Responding to individuals such as clients and staff who wish to know which data is being held about them by Disability Solutions West Midlands.
- Checking and approving (in conjunction with the CEO) with third parties that handle the company's data any contracts or agreement regarding data processing.

Responsibilities of the IT Lead:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly

- Researching third-party services, such as cloud services the company is considering using to store or process data

- Recommending to the CEO for approval Data Protection Statements attached to emails and other marketing copy

- Addressing data protection queries from clients, target audiences or media outlets

The processing of all data must be:

- Necessary to deliver DSWM services

- In our legitimate interests and not unduly prejudice the individual's privacy

- In most cases this provision will apply to routine business/charity data processing activities.

DSWM use a Data Protection Statement/Privacy Policy to inform clients/workforce/other interested parties regarding data protection

The notice:

- Sets out the purposes for which we hold personal data on customers and employees

- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers

- Provides that customers have a right of access to the personal data that we hold about them

Sensitive personal data
In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance
We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DC and/or DSO,

Your personal data
You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Security Officer so that they can update your records.

Data security
You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DSO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations, and this will be articulated to the DC/CEO.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DSO/IT Officer must appraise any cloud used to store data, and make recommendations to the DC/CEO
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the DSWM backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones or desktop pcs.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention
We must retain personal data for no longer than is necessary. This is determined by DSWM File Destruction Policy, which states, we abide by a 6+1yr retention policy.

Transferring data internationally
DSWM does not transfer data internationally naturally as part of its work.
Please Note: There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside of the UK without first consulting the DSWM Data Security Officer.

Subject access requests
Please note that individuals are entitled, subject to certain exceptions, to request access to information held about them. If you receive a subject access request, you should refer that request immediately to the DC/DSO. Then appropriate actions will be taken.
Please contact the DSO if you would like to correct or request information that we hold.

The agency will protect 3rd party information within their files where requests for data access are made, by ensuring that 3rd party consent to share is gained, or 3rd party data redaction will be made.

Processing data in accordance with the individual's rights
You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DSO about any such request. Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed. Please contact the DSO for advice on direct marketing before starting any new direct marketing activity.

Training
All staff and volunteers will receive training on this policy. New staff and volunteers will receive training as part of the induction process. Further training will be provided at least every 30months or whenever there is a substantial change in the law or our policy and procedures.

Training is provided through an in-house meeting
DSWM training will cover:

- The law relating to data protection / GDPR 2018
- Our data protection and related policies and procedures.

Completion of training is mandatory and must be undertaken for staff and volunteers to remain active within DSWM.

GDPR Provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	Name, address, current welfare benefit (if applicable), disability/LTHC, gender, DOB, NI number, marital status, medical records Tribunal papers, contact numbers,
Who is collecting it?	Staff and volunteers of DSWM
How is it collected?	Over the telephone, electronically, written format
Why is it being collected?	To assist/represent the data subjects in obtaining welfare benefit related claims (from form filling to tribunal level submission and representation through all phases of the process,), for charitable activity, contractual obligations,
How will it be used?	To help data subjects apply for appropriate welfare benefits and to represent the data subject for anonymised statistics when reporting statistics to contracted agencies (local authority, CCG), charitable activity,
Who will it be shared with?	Internally and only with organisations that the data subject has authorised us to share the

	information with, otherwise all information is not shared externally.
Identity and contact details of any data controllers	Mandy Rollins CEO and Data Controller (DC) for DSWM. David Lovat and Data Security Officer (DSO)
Retention period	6+1 years

Conditions for processing
We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff and volunteers who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a Privacy Statement/Policy.

Justification for personal data
DSWM will process personal data in compliance with all eight data protection principles as stated by the ICO – see Appendix 1.

DSWM will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

Consent
The data that DSWM collect is subject to active consent by the data subject. This consent can be revoked at any time. Consent must be gained (via an Authorisation Form) before any data can be processed.

Criminal record checks
Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability
Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right of erasure
A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default
Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DSO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan. Data Protection Impact Assessment (DPIA) / Privacy Impact Assessments (PIA) completed on all current services in April 2018.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Data audit and register
Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. Data Audit last completed in May 2018.

Reporting breaches
All staff and volunteers have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to our **Data Breaches Policy & Procedure**

Monitoring
Everyone must observe this policy. The CEO/DC and DSO have overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply
We take compliance with this policy very seriously. **Failure to comply puts both you and the organisation at risk.**

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which can result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DC/DSO.

Appendix 1

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.

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

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

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

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

ICO. 2018. *https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/*. [ONLINE] Available at: https://ico.org.uk/. [Accessed 7 February 2018].