Data Protection, Information Governance & Confidentiality Policy Statement

Date agreed by LDVS Senior Strategic Team: 26/11/2024

Signed electronically by:	**N. Peasgood**	**Partner Agency:**	LWA	**Position:**	CEO
	R. Davany		BCD		CEO
	R. Kelly		WHM		CEO

Date of next review: November 2027

Version 3

Statement of Purpose

Leeds Domestic Violence Service (LDVS) is a service delivered in partnership by Leeds Women's Aid (LWA), Behind Closed Doors (BCD) and Women's Health Matters (WHM). All three organisations are committed to following agreed LDVS policies and procedures. LDVS is committed to providing the best possible service to both individuals and professionals in the agencies we work with.

LDVS is committed to the provision of the highest quality service to its clients and to being open, honest and accountable in delivering its service. LDVS has set in place rules, regulations, quality standards and procedures to ensure that the highest standards of conduct and commitment to service are followed.

The purpose of this document is to provide guidance on data protection and information governance. Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a pro-active service. It provides a consistent way for individuals within LDVS to deal with the many different information handling requirements including assurance of:

- Effective Information Governance
- Safe Client Information
- Confidentiality and Data Protection
- Information and Internet Security

1.0 Principles

1.1 As three separate employing organisations, each partner agency has a Data Protection, Information Governance and Confidentiality Policy which relates to their employees. This statement is LDVS's commitment to sharing the ethos of data security and compliance with relevant legislation.

1.2 Each LDVS partner is registered as a Data Controller in their own right, but some aspects of UK GDPR compliance will be dealt with centrally, for example dealing with data subjects rights. This also applies to other organisations which host LDVS staff, specifically the Sanctuary Support Team and LDVS Voices work.

1.3 LDVS is committed to principles of good practice governing the collection, recording, storage and sharing of information. LDVS needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include service users, employees (present, past and prospective), donors, sponsors, suppliers and other business contacts. Information can include personal information such as name, address, email address, data of birth, and sensitive information such as ethnicity, religious beliefs, marital status, sexuality, physical & mental health, information about criminal court proceedings.

1.4 The EU General Data Protection Regulation (EU GDPR) has direct effect across all EU member states and became law on 25th May 2018. Following the UK's withdrawal from the EU, the UK General Data Protection Regulation (UK GDPR) came into effect on 1 January 2021. The Data Protection Act 2018 (DPA) sets out

the framework for data protection law in the UK and sits alongside and supplements the GDPR.

1.5 The lawful and proper treatment of personal information by LDVS is of paramount importance to the success of our organisation and in order to maintain the confidence of our service users and employees. Each partner organisation ensures that LDVS treats personal information lawfully and correctly.

1.6 All personal and sensitive information should be recorded and shared in a manner which prioritises service user safety, and which is concise, accurate and in compliance with relevant legislation.

1.7 LDVS will ensure that the personal data is:

- Held securely and confidentially
- Obtained fairly and lawfully
- Recorded accurately and reliably in accordance with LDVS Case Recording Principles
- Used effectively and ethically
- Shared and disclosed appropriately and lawfully

1.8 To protect the organisation's information from all threats, whether internal or external, deliberate or accidental. LDVS will ensure:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained and tested
- Information security and data protection training will be available to all staff
- All breaches of information security, actual or suspected, will be reported to, the Data Protection Lead (DPL) of their organisation. High risk data breaches should also be notified to the LWA Operations Director and DPL.

2.0 Collection and processing of data

2.1 LDVS partners fully support and comply with the six principles of the GDPR about how data should be processed. Data must be:

- Lawful, Fair, And Transparent; Data processing is not considered fair unless it meets at least one of the following conditions, and organisations must identify which legal basis before starting to process personal data.

- Consent - The individual has given their clear consent for their data to be processed for a specific purpose.
  - Contract - Processing is necessary to carry out a contract
  - Legal obligation - Processing is necessary to comply with the law
  - Vital Interest – Processing is necessary to protect someone's life

- Public Task – Processing is necessary to perform a task in the public interest or for official functions and the task/function has a clear basis in law

- Legitimate Interest: The processing is necessary for the legitimate interest of the organisation

- Limited for Its Purpose: Data must only be collected if there is a specific and valid reason and this data must not be used for any other, unrelated purpose.

- Adequate and Necessary: Data collected should be adequate, relevant and limited to what is necessary. Only data needed for a specific purpose should be asked for or recorded. This is known as the data minimisation principle. Information cannot and will not be collected simply because it may be useful in the future.

- Accurate: Personal data should always be accurate and kept up to date. Any changes to an individual's data must be updated on the relevant system(s) immediately.

- Kept only for as long as needed – retention settings on the case management system will be overseen by the LWA DPL

- Personal data should not be kept any longer than necessary

- Provides for integrity & confidentiality

2.2 Data must be processed in a way that ensures the security of the data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage. This is by both appropriate technical measures (such as IT security) and organisational measures (such as policies and procedures).

3.0 Personal Data and Special Category Data

3.1 The GDPR applies to 'personal data' meaning any information relating to an identifiable living person who can be directly or indirectly identified in particular by reference to an identifier.

3.2 This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

3.3 Some personal data is specially protected under GDPR and this is called 'sensitive' or 'special category data' and includes ethnicity, religious beliefs, marital status, sexuality, physical & mental health, genetic & biometric data. When collecting this data, LWA will ask for consent of the individual. Processing of special category data will comply with the requirements of data protection legislation.

3.4 Special category, or sensitive, data cannot normally be processed without the person's explicit consent; however, LDVS believes that along with consent we have a

legitimate interest to process sensitive data. This is in order to provide our services and ensure fair access for everyone with no sections of the community being discriminated against. Based on this, we may record ethnicity and sexual orientation for people who are referred to our services if this information is included on the referral for support. Alternatively, people who accept our support will be asked for their explicit consent to collect this data.

4.0 Data Controller and Data Processor

4.1 The organisation which collects the data, i.e. the LDVS partners, are referred to as the Data Controller. The data controller may use another organisation to process data on their behalf who would be a Data Processor. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller.

4.2 LDVS acts as both a data controller and data processor, and also works with other data controllers in delivering services in partnerships and consortia. LDVS will have appropriate data sharing agreements with other data controllers for such services

5.0 Case Management System

5.1 LDVS uses a case management system, Oasis On Track (OT), for recording support offered and delivered to service user. All relevant LDVS staff have access to OT and permissions are set specific to the individual's role to ensure that staff can only access the information relevant to their role.

5.2 The LWA DPL will deal with the permissions and settings on OT, including the compliance & retention settings section.

5.3 OT records for deceased persons – the LWA DPL should be notified if a person who we hold a record for on OT has died to the record can be locked down. This is regardless whether there are suspicious circumstances or not.

6.0 Consent and case recording

6.1 Consent from the service user must be clearly recorded on the case management system. It should include their consent for us to work with them and for us to share their information with specific named organisations that we think may be relevant either providing support or onward referral.

6.2 The client can withdraw their consent for information to be shared at any time and this must be clearly recorded on the case file. Client data may still be shared without their consent, after consultation with a manager, for example if there are safeguarding issues or if there is a court order.

6.3 When a service user is referred to LDVS for support, they will normally have given consent to the organisation making the referral for their basic information to be passed on to us. LDVS has a legitimate interest in processing this data in order to

make contact and offer support. If the person accepts support from LDVS, their consent must be requested and obtained in order for us to work with them.

7.0 Roles and Responsibilities

7.1 All LDVS partners will be registered with the Information Commissioner's Office (ICO) as a Data Controller

7.2 Training will be provided by LDVS partners to all staff and volunteers, whether 'in house' or by accessing workshops delivered by Women's Aid Federation England (WAFE) or IT Works (the software company who provides OT).

7.3 It is the responsibility of each employee to;

- Observe all forms of guidance, policy and procedures about the collection and use of personal information
- Understand fully the purposes for which LDVS uses personal information
- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by LDVS to meet its service needs or legal requirements
- Ensure the information is destroyed (in accordance with the provisions of the legislation and LDVS retention periods) when it is no longer required
- On receipt of a request by or on behalf of an individual for information held about them will immediately notify their line manager and the LWA DPL
- All employees, volunteers and trustees must make sure that they use the organisation's IT systems appropriately, and adhere to all relevant IT policies

8.0 Rights of Individuals

8.1 All LDVS partners will be aware of the rights of individuals under data protection legislation. If a LDVS service user makes a request to exercise these rights, the request will be directed to the LWA DPL immediately. This applies to LDVS partners and other organisations with staff delivering LDVS services under the Sanctuary Service Team and LDVS Voices work.

8.2 The rights of individuals are as follows:

- Right to be Informed - Individuals must be told what the information collected will be used for; who it will be shared with; the legal basis for collecting the data; and how long it will be kept. This information can be given to individuals in a range of ways:
    - In writing – e.g. Privacy Notice available in the Service User Handbook
    - Orally – either over the phone or face to face
    - Electronically – privacy information is available on the website and can be emailed to service users

- Right of Access – Subject Access Request (SAR)
  GDPR gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why

LDVS is using their data, and check we are doing it lawfully. A SAR must be completed within one month of the request being made

The LDVS staff member who receives the request must complete the LDVS Subject Access Request Form and send it immediately to the LWA DPL to ensure the strict timescales are complied with. Individuals are not required to put their request in writing, although the DPL may contact them to verify their ID.

- Right to Rectification - GDPR includes a right for individuals to have inaccurate or incomplete personal data to be rectified. Requests for rectification can be made either verbally or in writing and must be dealt with within a month. These requests could vary from correcting the spelling of a name/address to rectifying inaccurate facts or statements about that person. Requests such as this must always be referred to a manager.

- Right to Erasure (or the right to be forgotten) - The GDPR introduces a right for individuals to have their personal data erased; however, this is not an absolute and only applies in certain circumstances. Any request to be 'forgotten' should be referred to the DPL

- Right to Restrict Processing - Individuals have the right to request that the processing of their data is restricted in certain circumstances. Any request received for processing of data to be restricted should be directed to the DPL or LWA CEO.

- Right to Data Portability - The right to data portability allows individual consumers to obtain and reuse their personal data and transfer it from one IT environment to another in a safe and secure way.

9.0 Data Sharing

9.1 Data sharing always needs to be done securely and for legal reasons. LDVS shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing personal data must be encrypted using CJSM
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail Tracked & Signed For
- No personal data may be shared informally unless all staff, volunteers or trustees involved have the authority to do so, if not, they must request authority from the relevant line manager or DPL.
- No personal data may be transferred to third parties, whether they are working on behalf of LDVS or not, without relevant authorisation. See the Responding to Requests for Information Procedure

- Staff must not access any personal data without a valid business reason for doing so, this includes accessing client data on the case management system

10.0 Breaches of Personal Data

10.1 Breaching someone's personal data is a huge problem for organisations, and individuals working or volunteering for LDVS must be aware of what a breach is and take every effort to ensure that when dealing with sensitive personal data that it is kept safe at all times and only shared when appropriate. A personal data breach can broadly be defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

10.2 The GDPR defines a personal data breach as:
"…a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". This includes breaches that are the result of accidental or deliberate causes. It also means that a breach is more than just about losing personal data.

10.3 It can include:

- Sending personal data to an incorrect recipient – this includes accidentally emailing the wrong person or sending a fax or letter to the wrong person
- Loss or theft of computing devices, such as laptops, smart phones or USB drives containing personal data (all phones, devices or laptops must have passwords)
- Alteration of personal data without permission
- Wilful destruction of personal data
- Access by an unauthorised person or third party, including accessing client or other personal data without valid business reason
- Deliberate or accidental action (or inaction) by a data controller or data processor

10.4 There are specific procedures that the organisation must follow in order to comply with GDPR. We must be registered with the Information Commissioners Office and must report any notifiable breaches to them within 72 hours.

10.5 Any breaches of this policy must be immediately reported to line managers, who must in turn report through to the DPL immediately. It could be a criminal offence for someone to breach data protection legislation so breaches must be dealt with swiftly and appropriately.

10.6 As all LDVS, Sanctuary Support Team and LDVS Voices partners are data controllers in their own right, each partner will maintain their own log of data breaches in accordance with UK GDPR requirements. Should a data breach occur which is potentially notifiable to the ICO, these should also be reported to LWA as the contract lead to ensure all measures to contain and mitigate the breach and deal with any potential financial, physical or reputational damage to the organisation(s), staff, service users or any other linked people.

11.0 Complaints

11.1 An individual has the right to use our Compliments and Complaints Policy or to lodge a complaint directly with the ICO.