DRAFT LJWB General Data Protection Policy (GDPR) December 2017

1.Introduction

LJWB (Leeds Jewish Welfare Board) holds personal data regarding employees, volunteers, donors, people who access our services, suppliers and other individuals for a variety of business purposes. Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. This policy highlights how we collect personal sensitive data and what we will do with it:

The GDPR, Article 4, defines Personal Data as,

"Personal data means any information relating to an identified or identifiable natural person data subject); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an outline identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

LJWB will at all times adhere to the 7 key principles that guide GDPR:

- Legality, Transparency and Fairness
- Purpose Limitation
- Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

This policy sets out how LJWB seeks to protect personal data, and ensure that staff understand the legal requirements regarding use of personal data to which they have access in the course of their work. In particular, this policy highlights the need for staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant

2. Definitions

Business Purposes: The purposes for which personal data may be used by the LJWB are:

Personnel, administrative, financial, regulatory, payroll and business development purposes.

2.1Business 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 policies are adhered to, policies covering email and internet use.

- Operational reasons, such as recording Community Support Service transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing
- Improving services

2.2 Personal Data

- Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contracts.
- Personal data we gather may include; individual's contact details, medical information provided by the Data Subject, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title and CV.
- Sensitive personal data, such as race or ethnic origin, political opinions, religious or similar beliefs, trade union membership)or non-membership), physical or mental health or condition, criminal offences or related proceedings- any use of sensitive personal data should be strictly controlled in accordance with this policy.

3. Scope

This policy applies to all staff. All staff should be familiar with this policy and comply with its terms. This policy supplements all other policies relating to internet and email use. This policy may be supplemented or amended by additional policies and guidelines as required. Any new or modified policy will be circulated to staff before being adopted.

4. Who is responsible for this policy?

The LJWB Data Protection Officer, Janine Field, has overall responsibility for the day-to-day implantation of this policy.

5. Our Procedures

5.1 Fair and lawful processing

LJWB must process personal data regarding all staff, volunteers, people who use our services, donors, other service providers fairly and lawfully in accordance with individuals' rights This generally means that we should not process personal data unless the individual whose details we are processing has explicitly consented to this.

5.2 Consent

Consent will be freely given, specific, informed and unambiguous. Information regarding consent will be provided in an understandable and easily accessible format, using clear and plain language appropriate to the audience. It must be specific for the purpose and be explicit. I.e. a physical action such as having an "Opt In " box so that recording demonstrates how the individual gave consent. How long the data will be kept for will be explicitly stated.
Consent will be rejected if it is not unambiguous, clear and simple.
Records of consent will be retained and include dates when consent was obtained.

GDPR provides individuals with the right to withdraw consent at anytime. Individuals will be informed of this prior to consent. Once consent is withdrawn, individuals have the right to have their personal data erased and no longer used for processing.(The Right to Erasure) LJWB will ensure that withdrawing consent will be as easy as giving it.

5.3 Children's Consent

If a child is under 16 LJWB will acquire parental or guardian's consent in order to process the child's personal data. When the individual stops being a child, the parent or guardian's permission become invalid and new consent must be obtained from the individual.

5.4. Individuals Unable to Provide Consent

Where the individual lacks capacity, a Lasting Power of Attorney should be identified to act on their behalf, advocating on issues relating to finance or health and welfare pertaining to the individual.

It should however be noted that relatives, carers and even those documented as next of kin, do not necessarily have the right to access the personal or sensitive records of a person

6. Roles and Responsibilities Of:

6.**1 The Data Protection Officer (DPO)**

- To be the link between the ICO (Information Commissioner's Office) and LJWB to report any data breaches.
- Keeping the Board of Trustees, CEO and Senior Managers updated with information and issues pertaining to data protection, including responsibilities and risks.
- Reviewing all data protection procedures and policies on a regular basis
- Promoting and providing data protection training and advice for staff members and those included in this policy
- Clarifying queries regarding data protection from staff, board members and other stakeholders
- Responding to individuals and employees who wish to know the extent and purpose of personal data being held by LJWB
- Ensuring the compliance and adherence of GDPR requirement with third party operations that provide infrastructure support, e.g. IT and Case Management Systems, LJWB contracts or agreements regarding data processing

6.2 Staff and Trustees

- Understanding the need for compliance with GDPR.
- Ensuring safe storage of data, both on site and remotely
- Ensure all records of "Opt In" consent are recorded and retained
- All staff and Trustees have an obligation to report Data Protection breaches via the DPO if they have concerns a breach may have occurred.
- Adherence to the 8 rights of the individual in consenting to provide their information.
  These are:
  1. The right to be informed
  2. The right of access
  3. The right to rectification
  4. The right to erasure
  5. The right to restrict processing
  6. The right to data portability
  7. The right to object
  8. Rights in relation to automated decision making and profiling

6.3 Senior Management

- LJWB must implement appropriate technical and organisational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure, or access.
- Ensure all systems, services, software and equipment meet acceptable security standards
- Ensure appropriate technical and organisational measures are implemented to protect personal data, such as encryption to prevent unauthorised data access.
- Ensure that their staff are appropriate trained and understand their roles and responsibilities with regards to GDPR

6.4 Information Technology Leads

- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Ensuring that contracts with third party suppliers are appropriately secure to hold LJWB information
- Review the security arrangements of our IT software and hardware supplier on a regular basis and conduct cyber security checks.

6.5 Income Generation/ Marketing Manager

- Approving with the DPO data protection statements attached to emails and other marketing copy
- Addressing data protection queries from people who use the service, donors, staff and volunteers. and working with the DPO to ensure a timely and appropriate response
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the LJWB's Data Protection Policy.

7. Processing of all data:

In line with the new GDPR regulations which come into effect on May 25th 2018 all data collected by LJWB must be:

- Necessary to deliver LJWB services
- In the legitimate interests of LJWB and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

8. Privacy Notice

Our Terms of Business contains a Privacy Notice on Data Protection. This is available on the LJW website.

8.1 The Privacy Notice:

- Sets out the purposes for which we hold personal data on people who use LJWB services, donors, volunteers and employees
- Highlights that on occasions, LJWB may be required to share information with third parties, statutory and legal organisations.
- Informs all individuals that they have a right of access to their personal data, LJWB hold on them

9. Sensitive Personal Data

In all cases where LJWB processes 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.

10. Accuracy and Relevance

LJWB will ensure that any personal data processed is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. LJWB will not process personal data obtained for one purpose for any other unconnected purpose, unless the individual concerned has fully consented to this.

Individuals may ask that LJWB rectify inaccurate personal data relating to them. If information is found to be inaccurate, this should be recorded with a full account as to why the accuracy of the information is disputed and inform the DPO, Janine Field

Individuals must take reasonable steps to ensure that personal data provided to LJWB is accurate and updated as required. For example, if personal circumstances change, individuals should inform the relevant staff member, to enable records to be relevant and up dated.

11. Data Security

Data must be kept safe and secure at all times against loss or misuse. Where other organisations process personal data as a service on LJWB's behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

11.1 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, containing personal information, securely disposed of. LJWB hold a contract with a confidential waste handler and certified evidence provided on destruction.
- Data stored on a computer should be protected by strong passwords that are changed monthly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO and Senior leadership Team must approve any cloud used to store data
- 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 LJWB's backup procedures which will be reviewed with best practice guidelines.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.
- Data should never be saved without encryption to mobile devices such as laptops, tablets or smartphones.
- Personal devices must not be used to hold LJWB data in any circumstances.

.

11.2 Data Retention

Personal Data must not be retained for longer than is necessary. What is deemed necessary will depend on the circumstances of each case, taking into account the reasons the personal data was obtained, but should be determined in a manner consistent with LJWB data retention guidelines and legal requirements for each service.

11.3 Transferring Data Internationally

There are restrictions on international transfers of personal data. Personal Data must not be transferred anywhere outside the UK without first consulting the Data Protection Officer. This will ensure that personal data is not transferred to a territory outside the European Union unless that territory provides an adequate level of protection for the rights and freedoms of data subjects with the regard to personal processing of data.

12. Subject Access Requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

- If a subject access request is received, the request should be referred immediately to the DPO.
- LJWB have one month to provide the information, although this period of compliance may be extended by a further two months in cases where the requests are complex or multiple. In

such cases the individual must be informed in one month of the receipt of the request and an explanation why the extension is necessary.

- In line with the Right of Access this principle will be followed. However the regulations include exceptions, which may result in refusal of a request. If a request is rejected, adequate reason explaining why the request was rejected, must be communicated and LJWB will inform the requester about their rights to contact the ICO (Supervising Authority). An example of this will be, where disclosing information would "Adversely affect the rights and freedoms of others."

13. Processing Data in Accordance with the Individual's Rights

LJWB will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

LJWB will not send direct marketing material to anyone electronically (e.g. via email) unless the individual has an existing relationship with them in relation to the services being marketed.

14. Reporting Breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows LJWB to investigate the failure and take remedial steps if necessary. LJWB will maintain a full and accurate record of all breaches.These will be reported on a six monthly basis to the Finance committee and in turn the Board of LJWB.

The DPO is obliged to notify the Data Subjects and the ICO within 72 hours of disclosure. Where there is high risk data subjects need to be informed immediately if possible, by direct contact. If this is not possible the DPO should consult with the ICO to determine a way forward.

15. Privacy by Design and Default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all new projects and services developed by LJWB will commence with a Privacy Plan.

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.

16. Training

All existing staff will receive training on this policy. New employees will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure. Training will be recorded on an individual staff member's training record.

Training is provided through an in-house seminar on a regular basis.
It will cover:

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

Completion of training is required level of understanding.

17. 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.

18. Monitoring

All Trustees, staff and volunteers must observe this policy. The DPO has overall responsibility for this policy and will monitor it regularly to make sure it is being adhered to.

19. Consequences of Failing to Comply

LJWB's approach to compliance with this policy is taken with the utmost gravity. Failure to comply could place both the individual and the organisation at risk. This could result in the imposition of significant financial penalties for LJWB.

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

Policy Owner: Janine Field
Date: December 2017
Date of Review: December 2018