Lord's Work Trust

Privacy Standard

1. Introduction

1.1 This Privacy Standard sets out how the Lord's Work Trust ('we', 'our', 'us', 'the Organisation', 'LWT') handle the Personal Data of our donors, beneficiaries, employees, workers and other third parties.

1.2 This Privacy Standard applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, donors, beneficiaries. website users or any other Data Subject.

1.3 This Privacy Standard applies to all Organisation Personnel ("you", "your"). You must read, understand and comply with this Privacy Standard when Processing Personal Data on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you for the organisation to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Privacy Standard. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Privacy Standard may result in disciplinary action.

1.4 Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a DPIA as referenced in this Privacy Standard or otherwise then you must comply with the Related Policies and Privacy Guidelines.

1.5 This Privacy Standard (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Secretary of the Trust.

2. Scope

2.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will enhance operational activity and legitimacy.. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Organisation is exposed to potential fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

2.2 All Organisation Personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure that compliance.

3. Personal data protection principles

3.1 We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

i. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

ii. collected only for specified, explicit and legitimate purposes (Purpose Limitation);

iii. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

iv. accurate and where necessary kept up to date (Accuracy);

v. not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

vi. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

vii. not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

viii. made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

3.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

4. Lawfulness, fairness, transparency

4.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

4.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

4.3 The GDPR allows Processing for specific purposes, some of which are set out below:

i. the Data Subject has given his or her Consent;

ii. the Processing is necessary for the performance of a contract with the Data Subject;

iii. to meet our legal compliance obligations;

iv. to protect the Data Subject's vital interests;

v. to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

4.4 You must identify and document the legal ground being relied on for each Processing activity.

5. Consent

5.1 We must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

5.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes

or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

5.3 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.4 When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

5.5 You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines so that the Organisation can demonstrate compliance with Consent requirements.

6. Transparency (notifying Data Subjects)

6.1 We need to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6.2 Whenever we collect Personal Data directly from Data Subjects, we must provide the Data Subject with all the information required by the GDPR including how and why we will use, process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

6.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

6.4 If you are collecting Personal Data from Data Subjects, directly or indirectly, then you must provide Data Subjects with a Privacy Notice in accordance with our Related Policies and Privacy Guidelines.

7. Purpose limitation

7.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

7.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

8. Data minimisation

8.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

8.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

8.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

8.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Organisation's data retention guidelines.

9. Accuracy

9.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

9.2 You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10. Storage limitation

10.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

10.2 The Organisation will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time. You must comply with the Organisation's guidelines on Data Retention.

10.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Organisation's applicable records retention policies. This includes requiring third parties to delete that data where applicable.

10.5 You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

11. Security integrity and confidentiality

11.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

11.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

11.3 You must follow all procedures we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

11.4 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

i. Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;

ii. Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed; and

iii. Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

11.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

12. Reporting a Personal Data Breach

12.1 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

12.2 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Secretary of the Trust. Contact details are as follows:-

Mr L Currie, Secretary, Lord's Work Trust, 42 Beansburn, Kilmarnock, Scotland, KA3 1RL

Email : *l.currie@lwtrust.co.uk*

Telephone : 01563 521098

13. Transfer limitation

13.1 The GDPR restricts data transfers to countries outside the European Economic Area (EEA) to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

13.2 You may only transfer Personal Data outside the EEA if one of the following conditions applies:

i. the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

ii. appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Secretary of the Trust;

iii. the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

iv. the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

14. Data Subject's rights and requests

14.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

i. withdraw Consent to Processing at any time;

ii. receive certain information about the Data Controller's Processing activities;

iii. request access to their Personal Data that we hold;

iv. prevent our use of their Personal Data for direct marketing purposes;

v. ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

vi. restrict Processing in specific circumstances;

vii. challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

viii. request a copy of an agreement under which Personal Data is transferred outside of the EEA;

ix. object to decisions based solely on Automated Processing, including profiling (ADM);

x. prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

xi. be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

xii. make a complaint to the supervisory authority;

xiii. in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format;

14.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

15. Accountability

15.1 The Organisation must have adequate resources and controls in place to ensure and to document GDPR compliance including:

i. nominating an individual responsible for data protection ;

ii. implementing Privacy by Design when Processing Personal Data;

iii. integrating data protection into internal documents including this Privacy Standard and related Policies, Privacy ;

iv. regularly training Organisation Personnel on the GDPR,; and

v. regularly testing the privacy measures and conducting periodic reviews.

16. Record keeping

16.1 The GDPR requires us to keep full and accurate records of all our data Processing activities.

16.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining consents.

16.3 These records should include, at a minimum, the name and contact details, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of

the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

17. Training and audit

17.1 We are required to ensure all Organisation Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

17.2 You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

18. Sharing Personal Data

18.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

18.2 You may only share the Personal Data we hold with another employee, agent or representative of our group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

18.3 You may only share the Personal Data we hold with third parties, such as our service providers, if:

i. they have a need to know the information for the purposes of providing the contracted services;

ii. sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

iii. the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

iv. the transfer complies with any applicable cross-border transfer restrictions; and

v. a fully executed written contract that contains GDPR-approved third party clauses has been obtained.

19. Changes to this Privacy Standard

19.1 We keep this Privacy Standard under regular review.

19.2 This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where the organisation operates.

20. Other Related LWT Policies

20.1 This policy should be read in line with the following LWT policies:

1. Safeguarding Policy
2. Code of Conduct
3. Complaints Policy
4. Photography and Filming Policy
5. Data Breach Policy
6. Data Retention policy
7. Whistleblowing Policy
8. Bribery Act Policy