**Revised: Jan 2025**

**Landworkers' Alliance Privacy and Data Protection Policy**

**Data controller:** The Landworkers' Alliance, 7 Dunvegan Road, Penryn,
Email: info@landworkersalliance.org.uk

**Data protection officers:**
**Nancy Langfeldt (employee data)**
**Lauren Simpson (membership data)**
**cee-cee manrique (data relevant to marketing and communications)**

The Landworkers' Alliance's (LWA) is committed to protecting the confidentiality and integrity of personal data and will process all data in accordance with our responsibilities under the UK General Data Protection Regulation (UK GDPR), Data Protection Act (DPA) 2018, Privacy and Electronic Communications Regulations (PECR) 2003 and all other applicable laws.

This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

The following definitions are used in this policy:

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

This policy also serves to inform all persons whose data we collect and process (Data Subjects), as well as guide all persons who process personal data for the LWA (Data Processors).

Anyone who processes data in the service of the LWA should read, understand and abide by this policy and any other LWA policies relevant to data processing and sign a Data Processor agreement to declare their commitment to upholding the terms set out below.

Anyone using LWA communications and data processing platforms must also respect this and any other LWA policy about data processing with regard to how they treat other people's personal data.

The LWA only keeps personal data if you have consented for us to do so. Personal data is only accessible by staff, coordinating group members and member organisers at the LWA who have signed a privacy policy agreement and a data processing agreement where relevant. Access to any personal data is only granted where the specific data is relevant to their work.

**Data protection principles**

The LWA processes personal data in accordance with the following data protection principles:

- The LWA processes personal data lawfully, fairly and in a transparent manner.
- The LWA collects personal data only for specified, explicit and legitimate purposes.
- The LWA processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The LWA keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

- The LWA keeps personal data only for the period necessary for processing.
- The LWA adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The LWA tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. If the organisation wants to start processing personal data for other reasons, individuals will be informed of this before any processing begins and have the opportunity to consent to any change.

Personal data will not be shared with third parties, except as set out in privacy notices. Where the organisation relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the organisation processes special categories of personal data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, this is done in accordance with a policy on processing special categories of data.

The organisation will update personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered is on maintained databases – either in personnel files in electronic format, on HR systems (BrightPay) or on a password protected CiviCRM database. The periods for which the organisation holds personal data are contained in its privacy notices to individuals.

**The LWA keeps a record of its processing activities in respect of members' and supporters' personal data in accordance with the requirements of the UK GDPR.**

**Individual rights**

As a data subject, individuals have a number of rights in relation to their personal data.

*Subject access requests*

Individuals have the right to make a subject access request. If an individual makes a subject access request, the LWA will tell them:

- whether their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the LWA has failed to comply with their data protection rights; and
- whether the LWA carries out automated decision-making and the logic involved in any such decision-making.

The LWA will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

To make a subject access request, the individual should send the request to lauren.simpson@landworkersalliance.org.uk or nancy.langfeldt@landworkersalliance.org.uk or use the organisation's form for making a subject access request [insert link]. In some cases, the LWA may need to ask for proof of identification before the request can be processed. The LWA will inform the individual if it needs to verify their identity and the documents it requires.

The LWA will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, it may respond within three months of the date the request is received. The LWA will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the LWA is not obliged to comply with it. Alternatively, the LWA can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing the LWA or causing disruption, or excessive where it repeats a request to which the LWA has already responded. If an individual submits a request that is unfounded or excessive, the LWA will notify them that this is the case and whether it will respond to it.

*Other rights*

Individuals have a number of other rights in relation to their personal data. They can require the LWA to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the LWA's legitimate grounds for processing data (where the LWA relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override the LWA's legitimate grounds for processing data.

To ask the LWA to take any of these steps, the individual should send the request to lauren.simpson@landworkersalliance.org.uk or nancy.langfeldt@landworkersalliance.org.uk

**Data security**

The LWA takes the security of personal data seriously. The LWA has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by staff, co-ordinating group members and member organisers in line with the terms set our in their data processor agreements. The LWA also restricts access to any personal data so that it is only available when access is required to perform a specific, stated and necessary function.

**Revised: Jan 2025**

**Third Parties**

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Particular details of third-party data processors are available in privacy notices.

**Impact assessments**

Some of the processing that the LWA carries out may result in risks to privacy. Where processing would result in a high risk to individual rights and freedoms, the LWA will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

**Data breaches**

If the LWA discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

**International data transfers**

The LWA will not transfer personal data to countries outside the UK.

**Individual responsibilities**

Individuals are responsible for helping the LWA keep their personal data up to date. Individuals should let the LWA know if data provided to the organisation changes, for example if an individual moves house or changes bank details.

Individuals may have access to the personal data of other individuals in the course of their interactions with the LWA. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to individuals.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's databases without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and

- to report data breaches of which they become aware to the data protection officers immediately.

Further details about the organisation's security procedures can be found in our data processor agreements and privacy notices.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure if it applies to you. Significant or deliberate breaches of this policy, such as accessing employee or member data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice or the termination of membership.

**Training**

The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.