Confidentiality and Data Protection Policy

Updated on: July 2025	**Next review**: July 2027
Owner: Latin American Women's Rights Service (LAWRS)	
Authorised by: LAWRS' Management Committee	

Principle: The Latin American Women's Rights Service (LAWRS) firmly believes that our users have the right to a confidential service.

Purpose: The aim of this policy is to set out the principles that the organisation adheres to in order to guarantee that the information given to us is used properly and fairly and remains protected, building a relationship based on trust. LAWRS shall use this information only for the purpose for which it was collected.

Coverage: The policy applies to every aspect of the organisation and every person that LAWRS collects, processes, and stores personal information from, such as but not limited to, trustees, staff, volunteers, service users , members and donors, freelancers, event attendees, building visitors (Individual and collectively Individuals).

Contents:

Appendix 7: Data Protection Impact Assessment

1. Introduction

The principles outlined in the policy are to be applied to every aspect of LAWRS work. LAWRS believes it is necessary to protect all personal information regarding Individuals. All personal information shall be collected, processed, and stored in a lawful, fair and transparent manner.

The personal information collected by LAWRS shall be accurate, relevant and limited to what is necessary in relation to the purposes for which it is processed and shall be held for no longer than necessary pursuant to the Recording of Processing Activities (ROPA). LAWRS will do its best effort to keep the information secure and accurate according to the standard procedures.

All members of staff and volunteers will be given a copy of this policy during the induction process and required to attend basic training in GDPR and internet safety. During induction, Volunteers will be required to sign the Volunteer's agreement that contains a section on confidentiality (refer to LAWRS' Volunteering policy and procedure). In addition, staff and volunteers will be notified whenever the policy is updated.

2. Definitions

Personal information is the data that identifies an individual which may include sensitive data such as, but not limited to, name, address, telephone number, marital status, sexual orientation, and nationality, number of children, immigration status, ethnic origin, job applications, evaluations, among others.

The protection of personal information applies to information discussed in person, virtually or over the phone, which will be registered in LAWRS systems in a way that allows to identify how the data was collected. It may be stored in hard copy, on computers, in the cloud storage, videotaped, as audio or in any other available and lawful form.

LAWRS Administrators are the designated Data protection officers (DPO) and as such are responsible for controlling and supervising the personal information and providing advice for data management of new projects.

3. General Principles

3.1 Informed consent and Lawful Basis for Processing

LAWRS processes personal data in accordance with the UK GDPR and the Data Protection Act 2018. This includes basic personal information (e.g. name, contact details) and special category data (e.g. health, ethnicity, immigration status) where relevant to our services.

LAWRS will obtain consent (verbal or written) from Individuals before collecting any personal data (see Appendix 1). LAWRS will obtain explicit consent from individuals before processing special category data, except where we are required or permitted by law to act without consent (e.g. in safeguarding situations, serious risk to life, or legal disclosures). Consent must be freely given, specific, informed and unambiguous . Consent may be written or verbal and must be recorded in the Lamplight case management system. Therefore, individuals must be informed and understand why their data is being collected, how the data will be used, who it may be shared with (if anyone), how long it will be kept for and their rights, including how to withdraw consent.

At the point of collecting personal data, LAWRS will either provide the individual with a copy of its Privacy Notice or clearly direct them to where it can be accessed (e.g. on the LAWRS website or as a printed copy at reception). If the personal data is obtained from another source, LAWRS will provide the data subject with a copy of its Privacy Notice within a reasonable period of time (within a month).

Staff and volunteers must only collect the minimum amount of personal data needed and ensure all entries:

- Reflect the user's requirements
- Are factual information about what has been discussed and the relevant implications to the case
- Are free of any prejudice
- Are relevant
- Are legible and recorded accurately
- Are accompanied by the name of the person who collected it and the date

All members of staff are responsible to control that LAWRS has the required consent from the Individuals pursuant to the applicable legislation, which shall be also documented accordingly in LAWRS' case management system.

LAWRS maintains a Record of Processing Activities (ROPA) that outlines the lawful basis and retention period for each processing activity (see Section 13).

3.2 Sharing of personal data with third parties

LAWRS will not share personal information about individuals to any third party without their express consent, with exceptions of safety matters that require disclosure to Social Services or the Police in accordance with applicable legislation and LAWRS' Safeguarding and Child protection policy and procedure and Safeguarding adults policy and procedure.

Staff may share information with other members of staff at LAWRS as long as it is relevant to the case (e.g. internal referral). This also applies to volunteers when they are assisting staff. In these cases staff and volunteers must make sure that the personal information will not be discussed outside LAWRS' premises, unless it is during external supervision meetings. Likewise, files containing personal data shall not be removed from the premises unless proper authorisation to do so has been granted by the service user (e.g. to attend court hearings).

LAWRS may contact a third party for the benefit of the individual, such as, but not limited to, clinical supervisor, lawyers or any other organisation in order to provide a high quality service. However, this will only happen with expressed consent from the Individual who shall be properly informed.

In line with UK GDPR requirements, LAWRS uses a secure digital case management system called Lamplight, provided by Lamplight Database Systems Ltd, to store and manage personal data. Lamplight acts as a data processor on behalf of LAWRS and does not access or share personal data except as required to maintain and support the system. All processing is governed by a formal Data Processing Agreement, including safeguards around access, hosting, encryption, and international data transfers.

3.3 Right to withdraw consent

Individuals are free to withdraw their consent at any time, but this might prevent LAWRS from providing the services required in full or in part. Requests to withdraw consent (full or partial) can be made to any member of staff, who shall:

- Explain the next steps and possible implications of withdrawing consent to the requestant;
- Complete and send the Personal data request form (Appendix 2) to their line manager and DPO via email on the same day of request.

Once a Request form is received, the DPO and relevant line manager have 7 working days to consult and assess possible effects of consent withdrawal to provision of services.

Within eight working days from the date of request, the DPO will inform (via email, if possible) the Service user (SU) of the implications of their request and ask for their confirmation to proceed with it.

Taking into account the SU’s decision and assessment of implications, the DPO will process, carry out any relevant action and record the request in LAWRS’ case management system.

LAWRS will seek to resolve requests within 8 working days. If this is not possible, for any reason, a progress update should be sent to the requestant with an indication of when a full reply can be expected.

The following statement will be displayed in English, Spanish and Portuguese prominently in our offices at the waiting area at all times:

"LAWRS offers a confidential service. None of the information shared with us will be disclosed to any other organisation or person without your expressed consent unless required by law or by LAWRS' safeguarding policies".
You have the right to withdraw your consent at any time, however this may impact LAWRS capacity to provide services.
A copy of LAWRS Confidentiality and data protection policy is available on request."

3.4 Right to be forgotten, also known as Right to Erasure Request

Individuals also have the right to be forgotten and LAWRS is committed to comply with this right unless there are legal obligations or any other reasonable grounds to keep personal records within the established periods (see point 13). Requests to be forgotten can be made to any member of staff, who shall:

- Explain the next steps and possible implications of being forgotten the requestant;
- Complete and send the Personal data request form (Appendix 2) to their line manager and DPO via email on the same day of request.

Once a request form is received, the DPO will contact the relevant Senior Manager within 2 working days to confirm if the requestant's personal data can be deleted according to funders' agreements.

Within 15 working days from the date of request, the relevant Senior Manager should inform the DPO of the findings of the relevant funder agreements' details.

The DPO will inform (via email, if possible) the requestant of which data will be erased, which data will be kept and why.

The DPO will then process, carry out any relevant action and record the request in LAWRS' case management system.

LAWRS will seek to resolve requests within 20 working days. If this is not possible, for any reason, a progress update should be sent to the requestant with an indication of when a full reply can be expected.

3.5 Subject Access Request (SAR)

Under the UK GDPR, all individuals have the right to access personal data that LAWRS holds about them. Subject Access Requests (SARs) may be made verbally or in writing, and LAWRS must respond within one calendar month of receiving the request.
If a request is particularly complex or involves a large volume of data, LAWRS may extend the response period by up to two additional months. In such cases, the individual will be informed of the extension and the reasons for it within the original one-month timeframe.

Requests may be submitted to any member of staff. Upon receiving a request, the staff member shall:

- Explain the next steps and expected timeframes to the requester
- Complete and send the Personal Data Request Form (Appendix 2) to their line manager and DPO on the same day
- The following internal procedure shall be followed:
    - Day 0–2: DPO to notify the relevant Senior Manager
    - Day 3–15: Senior Manager to gather the requested data and assess whether disclosure may pose risks to the individual (e.g. emotional distress, legal complications)
    - Day 16–20: DPO informs the requester of any potential risks and confirms whether they wish to proceed
    - Day 21–30: DPO provides the requested data to the individual (in writing, preferably by secure email) and records the request in the Lamplight case management system.

If the request cannot be completed within one calendar month, the DPO will notify the individual by Day 30 with an explanation and a revised deadline, not exceeding an additional two months.
No fee will be charged for SARs unless the request is manifestly unfounded, excessive, or repetitive. In such cases, LAWRS may charge a reasonable fee or refuse the request in line with Article 12(5) UK GDPR.

4. Data storage, access and management

Data shall be stored in the following way:

- All hard copy files containing personal information will be kept in locked filing cabinets.
- All electronic data will be stored under password protected systems, and passwords changed when deemed necessary (eg: change of staff, suspected leak).
- Each member of staff will have a personal username and password to access LAWRS' network and the Lamplight case-management system. Credentials must never be shared.
- Two Factor Authentication authentication is set up for accessing emails, cloud storage and Lamplight system.
- The DPOs are responsible for monitoring the change of passwords.

4.1 Casework and work records

LAWRS records all casework and service user data mainly in the Lamplight case management system, which acts as the secure digital repository for all service user interactions, support notes, documents, and referrals. No paper-based records are kept unless strictly necessary for legal or procedural reasons (e.g. court bundles). Any

physical documents must be securely uploaded to Lamplight and destroyed immediately afterward. If a paper based document needs to be kept for legal requirements, The Senior Management Team is responsible for ensuring that all documents are kept locked in filing cabinets.
The Lamplight system is hosted in the European Economic Area (EEA) by Amazon Web Services (AWS) and is protected by encryption, role-based access controls, multi-factor authentication, and audit logging. Access is restricted to authorised staff and supervised volunteers, who are assigned individual accounts with defined permission levels based on their role.
All case records must:

- be entered on the same working day as the session or contact (where possible)
- contain only factual, relevant and respectful information
- be attributed to the staff member or volunteer who entered the record

Volunteers may only access service users' records in Lamplight under supervision and for cases to which they have been formally assigned. They must not retain copies or notes outside the system.

Remote & offline working
If an adviser must work offline (e.g. outreach with no internet), notes should be taken in a dedicated password-protected file and uploaded to Lamplight within 24 hours, after which the local copy must be deleted.

Retention & deletion
The DPOs monitor cases for deletion annually to confirm the action or extend retention where a legal hold exists.

4.2 Use of Mobile Phones and Messaging Apps for Casework Communication

LAWRS staff may communicate with service users by telephone or messaging apps (such as WhatsApp) using LAWRS-issued mobile phones. This communication is governed by the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and LAWRS' confidentiality obligations.

1. Consent and timing
• Before initiating contact by phone or WhatsApp, staff must obtain the express consent of the service user, including their preferred method, date, and time for communication.
• This preference must be documented in Lamplight and reviewed regularly.

2. Use of interpreters
• Where an interpreter is required for communication, they must be fully briefed on and agree to abide by the principles of UK GDPR, including confidentiality, purpose limitation, and data minimisation.
• Interpreters may not retain or record any personal data shared during calls or sessions and must confirm their agreement to LAWRS' data protection terms in writing before assisting.

3. Permitted devices
• Preferably only LAWRS-issued mobile phones should be used for t communication with service users. Personal phones must never be used to store or share service user data.

4. Permitted apps and tools
• Calls, SMS, and WhatsApp may be used for limited, appropriate communication (e.g. scheduling, brief updates).
• WhatsApp is allowed due to its end-to-end encryption.

5. Record keeping
• Any relevant conversation (e.g. session planning, crisis updates) must be summarised in Lamplight the same day.
• Key points from WhatsApp messages must be logged (e.g. “Confirmed appointment by WhatsApp on 04/06 at 14:00”). Screenshots are not a substitute for logging.

6. Security and confidentiality
• LAWRS phones must be protected by a strong password or biometric lock and auto-lock after inactivity.
• Phones must not be left unattended in shared spaces.
• Any loss or theft must be reported to the DPOs immediately so the device can be remotely wiped.

7. Service user safety
• Staff must verify that it is safe to call or message the service user. If the person shares their phone or lives in a controlled environment, safer alternatives (e.g. coded email or in-person follow-up) must be used.

8. Retention and deletion
• Staff must regularly delete WhatsApp messages from phones once the information is recorded in Lamplight. Messages or screenshots must not be stored on phones, backups or external drives.

9. Training and oversight
• All staff and volunteers using LAWRS phones must be trained on mobile data handling and agree to abide by this policy.
• The DPOs may conduct periodic checks and provide guidance on compliant use of mobile communication tools.

4.3 Staff and Volunteers

Staff and volunteer HR records (e.g. contracts, references, performance reviews, DBS checks) are stored separately in secure, access-controlled folders within LAWRS’ organisational Google Drive. These records are only accessible to the Senior Management Team, Administrators, and relevant line managers. Board access to employee files is restricted and must be justified and documented. The Volunteers’ Coordinator manages volunteer records, with access restricted as above.

4.4 Members

Members' personal information will be kept in LAWRS' Case management system - Lamplight. The Administrators are responsible for managing their data. Although all staff members and some volunteers can have access to the information, only the Administrators, Policy and Communications Team and the Senior Management Team should process the data.

4.5 Board

Trustees' personal information will be kept in the Google Drive. The Administrators are responsible for managing the information, whilst the Administrators and Senior Management Team have access to their information.

As a general rule and in accordance with our organisation's commitment to transparency and accountability, the minutes, reports and proposals of the Board are shared and open documents except when a confidential item is being discussed.

When documents marked 'Private and Confidential' are discussed at Board meetings, they cannot be shared with third parties without the express consent of the relevant individual. Minutes from confidential items will be kept out separately from the main minutes of the meeting.

Trustees must not discuss confidential matters addressed at meetings outside of these.

4.6 Lamplight Case-Management System – Data-Processor Notice

LAWRS is the data controller for all personal data entered into the Lamplight case-management system. Lamplight Database Systems Ltd acts as data processor, and Amazon Web Services (AWS) acts as sub-processor providing the cloud-hosting infrastructure.

Hosting location – Primary and backup data reside in AWS EU-West regions (Republic of Ireland and, for resilience, other EU data centres). No routine transfers are made outside the UK/EEA.

Contractual safeguards – Processing is governed by Lamplight's Data-Processing Agreement (DPA, v 2024-12), which incorporates:

UK International Data Transfer Addendum (IDTA) & EU Standard Contractual Clauses for any onward transfers;

AWS Service Terms and Data-Protection Addendum (last updated 1 Feb 2025).

Security measures – AWS is certified to ISO 27001, SOC 2 Type II and employs encryption at rest (AES-256) and in transit (TLS 1.2+). Lamplight enforces role-based access control, MFA, daily encrypted backups and quarterly restore tests.

Audit & deletion – LAWRS retains the right to request summary audit reports or to commission a third-party inspection. On contract termination Lamplight will, at LAWRS' choice, return or securely erase all personal data within 30 days.

4.7 Artificial Intelligence Meeting Recordings & Transcription Tools

Due to the sensitive nature of the work carried out by LAWRS, including the regular processing of special category and confidential personal data, the use of artificial intelligence (AI) transcription tools or any form of artificial intelligence (AI) meeting recording (audio or video) is not allowed. This applies to all internal and external meetings involving service users, staff, volunteers, or third parties.
LAWRS has taken this position to protect the privacy, dignity, and safety of individuals, and to ensure full compliance with the UK GDPR, particularly Articles 5 and 9, regarding data minimisation, integrity, confidentiality, and the processing of special category data.

5. Media

Any member of the media who contacts LAWRS should be referred initially to the Director. The Director may provide information about LAWRS work and position, and authorise a member of staff to do the same. It will be to the Director's discretion to decide whether or not to share such information and weigh the benefits and possible risks.

When the Director is not present, the Deputy Director or a designated member of staff appointed by the Director, will evaluate if it is appropriate to share information with the press, broadcast or electronic media and the potential benefits and risks. However, personal information shall not be shared, unless LAWRS holds express consent of the Individual involved.

LAWRS may share anonymised information with the media or press, any other organisation or to the public in general, if the Director considers lawful and appropriate without the express consent of the individual. Anonymisation involves removing all identifying information so the individual can no longer be recognised. Before any kind of disclosure, LAWRS shall assess each situation in particular balancing the risks and the benefits. The Director or the person designated by the Director shall decide which process to use in each circumstance, such as, but not limited to use of a pseudonym, change the nationality, age, number of family members and so on. The organisation should also consider how LAWRS and its users would benefit from the sharing of such information.

6. Research

Users, volunteers, and staff shall be provided the following information before participating in research carried out by or through LAWRS:

- Individual in charge of the research and contact details

- Information about partner institution/s
- Research topic
- Anonymity policy of the research
- Right to withdraw consent at any time
- Dissemination plans
- Participants right to withdraw consent at any stage of the research

At the point of gathering consent, all SUs will be informed that "LAWRS will use anonymised data, through which the SU is not identifiable, to improve services, to report to funders, for research purposes and to increase awareness of donors, partners, the general public & others about the problems affecting its service users".

7. Statistical information

LAWRS may keep statistical records of Individuals in order to monitor the services provided and the needs of the community. The statistical information will be provided anonymously, thus the Individual will not be identified.

Line managers of each project are responsible for assessing any personal information provided for statistical analysis to third parties, such as, but not exclusively: in support of grant applications, for reporting purposes, etc.

8. E-mails, telephone and post

LAWRS shall enquire Individuals whether they wish to be contacted by LAWRS. Staff must enquire about the SU's preferred method of contact and the type of information that individuals wish to receive. If a VAWG user is contacted over the telephone, staff and volunteers must make sure LAWRS is not mentioned when leaving messages or communicating with people other than the SU.

The member of staff or volunteer who distributes the mail shall keep the information confidential in accordance with data protection legislation and LAWRS' policies. Post which is addressed to LAWRS will be opened by a member of staff or a volunteer under supervision of a member of staff and decide to whom it will be given.

In order to avoid breaching this policy the following paragraph should be included in each email sent from the organisation:

"The information included in this email is confidential and is intended for the exclusive use of the named addressee. If you have received this email in error, please contact us immediately.

9. Exceptions

LAWRS may share personal information from individuals in certain circumstances. Thus, if any member of staff or a volunteer identifies any kind of personal harm, risk of

personal harm, abuse, neglect, or signs of physical or psychosocial violence including emotional abuse to yourself or others, LAWRS shall report the issue to the police, social workers, or the appropriate institution. In addition, when there is knowledge of a child being abused or at risk of being abused or when there is information of a vulnerable adult at risk, a member of staff or volunteer will follow the procedure set out in LAWRS' Safeguarding and child protection policy and procedure or Safeguarding Adults policy and procedure.

There may be other circumstances when LAWRS is obliged by law to share personal information, for example to comply with a court order after being notified.

10. Sanctions in case of breach of Confidentiality

LAWRS recognises that many of the breaches of confidentiality are not intentional and may happen when a conversation is overheard by a third person, a file is left unattended, or when the ICT systems do not have the appropriate security measures. However, such incidents will be considered as seriously as those done deliberately.

When a staff member shares confidential information to a third party, breaches this policy or there is a suspicion of breach, they must:

- Complete and send the Data breach form (Appendix 3) to their line manager and DPO via email as soon as breach has been identified.

Once a Data breach form is received, the DPO will investigate the incident, assess risks it might pose and draw a plan with next steps within 72 hours from when the breach was identified.

The DPO will then process, carry out any relevant action - depending on gravity and risk it poses to affected individual(s). The Office of the Information Commissioner (ICO) and individual(s) are to be contacted via appropriate form and email within the same timeframe and a record of the request should be made in LAWRS' case management system.

The result of this investigation may require a disciplinary procedure in accordance with the rules established in the Grievance, disciplinary and whistleblowing policy and procedure.

LAWRS will seek to resolve requests within 72 hours. If this is not possible, for any reason, a progress update should be sent to both ICO and Individual(s) affected with an indication of when a full reply can be expected.

In case of a breach of confidentiality by the Director, it will be the responsibility of the Chair, or if unavailable, a member of the Board, to follow the Data breach procedure, complete the Data breach form and carry out the investigation and potentially a disciplinary procedure in accordance with the rules established in the Grievance, disciplinary and whistleblowing policy and procedure.

When a volunteer shares confidential information to a third party or breaches this policy, it should be reported immediately to the Volunteers' coordinator and to the DPO, following the Data breach procedure and completing the Data breach form. Depending on the seriousness of the breach of confidentiality, it can be decided that this person should not volunteer any longer and should leave the organisation altogether.

In the case of members of the Board, it would be the Board's responsibility to decide what actions to take regarding the trustee who breached confidentiality taking into consideration the seriousness of the breach and the potential damage to LAWRS' reputation. The Data breach procedure is to be applied.

LAWRS has the duty to report data breaches to ICO in 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals, such as discrimination, damage to reputation, or financial loss. Eventually, if the breach is likely to result in a high risk to the rights and freedoms of the individual, it must be also notified to the individual concerned directly without undue delay. The Director or the designated person will be responsible for managing the process.

11. Complaint procedure

LAWRS complaint procedure, as established in the LAWRS' Complaints policy and procedure, offers a mechanism through which any Individuals may express their disagreement or concern regarding any data management issue.

If an individual is not happy with our response to the complaint, she can contact ICO which oversees the protection for personal data in the UK or the Fundraising Regulator which is responsible for overseeing fundraising activities carried out by charities in the UK.

12. Data Protection Act

LAWRS complies with all legal obligations established in the UK GDPR, The Data Protection Act 2018 and the Privacy and Electronic Communications Regulations (PECR) Therefore, the collection, processing and storage of personal information is done in accordance with such legislation
LAWRS will ensure compliance with the law by:

- Informing all Individuals about the responsibilities derived from the law as part of the induction process.
- Keeping Individuals up to date with any change to their legal obligations under the law.

13. Record of Processing Activity (ROPA) and Destruction of Information

The destruction of personal information collected and stored by LAWRS will be done in the following way, unless required by legal obligations:

	PROCESSING ACTIVITY	Art 6 lawful basis	Art 9 special-category condition	Typical data held	Retention trigger period
1	Advice, advocacy and casework support	6(1)(b) Contract (service requested by user)	9(2)(d) Not-for-profit with safeguards	Contact details, immigration status, health, children's details, referrals, case notes	6 years after last case entry (Creche contract details stored in Google Drive will be deleted 1 year after last access to the Creche service)
2	Safeguarding referrals or disclosures (not registered in Lamplight as specified in LAWRS Safeguarding policies)	6(1)(d) Vital interests	9(2)(c) Vital interests	As above + risk notes	Until statutory investigation concludes + 1 yea r
3	Recruitment	6(1)(f) Legitimate interests	Art 10 basis DPA 2018, Schedule 1, Part 1, para 1 – Employment & safeguarding	CV, contact details, interview notes, application forms	6 months after recruitment ends
4	Equal-opportunity and impact monitoring (staff and volunteers job applicants)	6(1)(f) Legitimate interests	9(2)(g) Substantial public interest – equality	Ethnicity, sexual orientation, disability	Anonymise after annual report, then delete raw data
5	Email, SMS & postal updates on LAWRS services	6(1)(a) Consent	n/a (no special-categor y data)	Name, email, language preference	Until consent withdrawn or 2 years of inactivity

6	HR & Volunteer management	6(1)(b) Contract	9(2)(b) Employment & social-security law	References, DBS checks, health info, Volunteers application forms (Google form)	6 years for staff and 2 years for volunteers - after employment/volunteering ends
7	Board & governance records	6(1)(c) Legal obligation (Companies Act, Charities Act)	n/a	Trustee contact details, minutes	Board minutes – permanent; personal data – 6 years after tenure
8	Health and safety incident records	6(1)(c) Legal obligation	9(2)(f) Legal claims	Injury reports, witness statements	40 years from incident (Employers' Liability regs)
9	Google form responses for events	6(1)(a) Consent	n/a (no special-category data)	Name, email address, phone number, Date of Birth, Language	Include anonymised data in Lamplight and delete data after event
10	Google form (referrals)	6(1)(a) Consent	n/a (no special-category data)	Name, email address, phone number, Date of Birth, Language,	Upload response in Lamplight and delete response
11	Complaint Records	6(1)(f) Legitimate interests	N/A (unless complaint includes special category data – then 9(2)(f) Legal claims)	Complainant name, contact details, incident details, case notes, outcomes	3 years after complaint resolution

12	Research and evidence collection	6(1)(f) Legitimate interests	9(2)(j) Research purposes with safeguards (if personal data is used)	Survey responses, anonymised service user data, demographic info	5 years after publication
13	Suppliers, providers and contractors information	6(1)(b) Contract	n/a	Name, business contact details, contract terms, payment records	6 years after contract end (per Limitation Act 1980)
14	Accounting and financial information	6(1)(c) Legal obligation (Finance Act 1998, Companies Act 2006)	n/a	Invoices, payroll, receipts, budget reports	6 years from end of financial year (per HMRC guidance)
15	Insurance policy contracts	6(1)(c) Legal obligation	n/a	Policy documents, coverage terms	6 years from policy expiry
16	Employers' liability insurance policies	6(1)(c) Legal obligation	n/a	Policyholder name, cover details, certificate numbers	40 years from policy expiry
17	Supporting documentation for EU-funded projects	6(1)(c) Legal obligation (EU/UK grant conditions)	n/a	Project plans, staff records, budgets, participant registers	five years after the last EU payment/recovery for the project.

The destruction of hard-copy information will be done with a paper shredder, or contracting a certified shredding company, and under the supervision of the Director.

The destruction of digitally kept information will be done by deleting it from the cloud (case management system and organisational drive).

14. Data Protection Impact Assessment (DPIA)

In line with the UK General Data Protection Regulation (UK GDPR), LAWRS will carry out a Data Protection Impact Assessment (DPIA) before introducing any new service, project, or change in working practices that involves the processing of personal data, particularly sensitive or special category data. The purpose of the DPIA is to identify potential data protection risks, ensure that appropriate safeguards are in place, demonstrate compliance with data protection law, protect the rights of service users, staff, volunteers, and members of the public. The DPIA will be led by the Data Protection Officers (DPO's) in partnership with the relevant activity or service lead, initiated no later than two weeks before the planned start of the new activity or service, reviewed and files before any processing begins
All DPIAs will be documented and retained on record as part of LAWRS' accountability obligations under Article 35 of the UK GDPR.

Approved by LAWRS' Management Committee:

Chair Signature	**Secretary Signature**

Appendix 1: Service user consent form

Service User consent form

In accordance with current legislation (Data Protection Act 2018 and UK GDPR), LAWRS requires your explicit consent to process, record, and store your personal data, including special category data such as information related to your health, ethnicity, immigration status, family information or other sensitive matters relevant to the support we provide

Your personal information will be securely stored in paper and electronically, and treated as confidential only accessible by relevant staff and volunteers, with the following exceptions:

● When you **expressly request us to contact** other services or organisations on your behalf. The purpose and nature of any information likely to be shared will be discussed with you prior to any contact.

● When the member of staff identifies **risk** of harm to yourself or others, particularly children or vulnerable adults, including potential exposure to any form of negligence or abuse, in compliance with UK legislation.

● In line with professional and ethical requirements, members of staff may discuss their work with external **supervisors** to ensure the quality of the service.

● When required by **audits and quality checks**.

A unique code will be assigned to you to preserve your identity. LAWRS also uses anonymised data, through which individuals are not identifiable, to improve services, to report to funders, for research purposes, and to increase awareness of donors, partners, the general public and others about the problems affecting its service users.

You are entitled to withdraw your consent and to request access to your files with prior notice, which in some cases may affect LAWRS ability to provide some services. Service users' personal information will be destroyed after six years, unless required by law or for an exceptional reason, as stated in LAWRS' Confidentiality and Data Protection Policy.

Voice, video or any other kind of recording without explicit consent and agreement from all parties is strictly forbidden and can result in immediate cancellation of provision of services.

For further information, please request a copy of LAWRS Confidentiality and Data Protection Policy to any member of staff, via email at lawrs@lawrs.org.uk.

I give my consent to LATIN AMERICAN WOMEN'S RIGHTS SERVICE "LAWRS" to:

	Record, process and store personal and sensitive information about myself for the purposes mentioned in this form.
	I understand that edited information, that would not identify me, may be included in LAWRS public communication and funder's reports.
	I know that I am entitled to see the information if I ask to and to withdraw consent.
	I understand that I need to provide truthful information to the best of my knowledge, and that otherwise I may not be able to continue being supported by LAWRS
	I agree to be contacted by LAWRS in person, by phone, by emails or text message to receive information about LAWRS activities, campaigns, news, job vacancies, etc.

	I give my express permission to use photos or footage of me recorded while participating in activities organised by LAWRS in publications, campaigns, material, adverts, display material, electronic material, media work, etc.

Appendix 2: Personal data request form

Personal data request form

(for internal use)

Person taking request**:**	
Role in the organisation:	
Date and time of request:	
Type:	

	Consent Withdraw Request
	Right to Erasure quest
	Subject Access Request

Requestant's details:

Name:		
Telephone:		
Address:		
Email:		
Preferred communication means:	**Post**	**Email**
☐ **ID verified (only required if request is from someone not previously known to LAWRS)**		

Use the space below to write down the circumstances of request and any other relevant information

Please explain in as much detail as possible what the request is about (eg: specify which consent requestant wishes to withdraw; what personal data the requestant wishes to have it deleted; which information does the requestant wants to have access to).

Brief explanation of procedure and deadlines after request is made:

Consent Withdraw Request: Form only needs to be completed if consent withdrawal relates to topics 1, 2, 3 and 4, as it may affect LAWRS ability to provide some services. For topic 5 and 6 of Consent form, withdrawal requests can be proceeded immediately and recorded directly in the LAWRS' case management system.

Consent form topics	
1.	Record, process and store personal and sensitive information about myself for the purposes mentioned in this form.
2.	I understand that edited information, that would not identify me, may be included in LAWRS public communication and funder's reports.
3.	I know that I am entitled to see the information if I ask to and to withdraw consent.
4.	I understand that I need to provide truthful information to the best of my knowledge, and that otherwise I may not be able to continue being supported by LAWRS
5.	I agree to be contacted by LAWRS in person, by phone, by emails or text message to receive information about LAWRS activities, campaigns, news, job vacancies, etc.
6.	I give my express permission to use photos or footage of me recorded while participating in activities organised by LAWRS in publications, campaigns, material, adverts, display material, electronic material, media work, etc.

Action	Deadline
Line manager and DPO to be informed	same day of request
Both to assess possible effects it may have on requestant's provision of service	7 working days of date of request
DPO to inform requestant of findings. Confirm if she wishes to proceed	8 working days of date of request
DPO to update LAWRS' case management system	as soon requestant is contacted

Right to Erasure Request: LAWRS has the right to deny or partially accept the request. Some data might have to be kept in order to comply with a legal obligation.

Action	Deadline
Line manager and DPO to be informed	same day of request
DPO to request Senior Manager to confirm if there are any personal data that cannot be deleted (Senior manager will rely on the contract/agreement signed with funder)	within 2 working days of day of request
Senior manager to inform DPO of the findings.	15 working days of date of request
DPO to inform requestant which data will be erased and kept & why	20 working days of date of request
DPO officer to update LAWRS' case management system	20 working days of date of request

Subject Access Request: LAWRS has to respond to the request within **one month**. If the request is complex, LAWRS may need extra time to consider the request and can take up to an extra **two months** to respond.
All service user personal information is destroyed after 6 years the case is closed.

Action	Deadline
Line manager and DPO to be informed	same day of request

DPO to inform Senior Manager of the request	within 2 working days of day of request
Senior manager to gather data requested, assess what potential risks it may present to service user (eg: produce evidence against oneself) and inform DPO	15 working days of date of request
DPO to inform requestant of potential risks, confirm if she wishes to proceed with request	20 working days of date of request
DPO to send request information to requestant and update LAWRS' case management system	30 working days of date of request
If no resolution within 30 days, DPO to inform the requestant of extension and reasoning behind it	If the request cannot be completed within one calendar month, the DPO will notify the individual by Day 30 with an explanation and a revised deadline, not exceeding an additional two months.

Requestant's Declaration

I declare that:

- I was informed of LAWRS' Confidentiality and data protection policy and a copy was made available to me.
- I received a brief explanation about LAWRS' Confidentiality and data protection policy, including what will happen next and estimated time for resolution.
- I understand that although LAWRS' aim is to resolve requests as promptly as possible, in some cases, there may be extraordinary circumstances that may delay the resolution, in which case LAWRS will keep the requestant updated throughout the process.
- To the best of my knowledge, everything I have told you is correct.
- The content registered on this form was read back to me and I agree with it.
- I understand that, to help resolve my request, LAWRS will need to use and keep personal information about me – for example, how to contact me and details about my request and sometimes sensitive personal information.
- I understand that except in exceptional circumstances, every attempt will be made to ensure that both myself and LAWRS maintain confidentiality. However, the circumstances giving rise to the request may be such that it may not be possible to maintain confidentiality (with each request judged on its own merit). Should this be the case, the situation will be explained to me.

Signature:

Print name:

Date:

Form last updated: July 2025

Appendix 3: Data breach form

Data breach form

(for internal use)

Please complete this form if any personal data has been breached or suspected of been breach

Person reporting**:**
Role in the organisation:
Date and time it occurred:
Date and time of it was identified:
Type of data breached:

Details of affected individual (please add more individuals if required):

Individual #1

Name:
Lamplight ID:

Individual #2

Name:
Lamplight ID:

Use the space below to write down the circumstances of data breach or potential data breach, which data was breached and any other relevant information

Please explain in as much detail as possible how you found out of breach, what happened, how it happened, what information was leaked

Brief explanation of what will happen after data breach is identified and deadlines:

Timeline	Deadline
1. Complete form	when breach has been identified

2. Line manager and DPO to be informed	same day
3. Investigation to be carried by DPO to assess risks and next steps	within 72 hours
4. Depending on gravity and risk it poses to affected individual(s), ICO and individual(s) will be contacted.	72 hours
5. DPO to update Lamplight in case individual has been notified	as soon notification has been made
6. Possible implementation of changes to avoid future breaches	as soon as possible
7. Disciplinary procedure, in accordance with the Grievance, disciplinary and whistleblowing policy and procedure, might be followed	after investigation is concluded

Appendix 4: Guidance on sending bulk emails from Lamplight

Guidance on sending bulk emails from Lamplight

To prevent data breaches and ensure compliance with service users' contact permissions, bulk emails must only be sent through Lamplight.

*** Please note**: This does not apply to the Comms Team, who may continue using their own bulk mailing list via a different mail merge platform.

Before sending bulk emails, please make sure your email account is properly linked to Lamplight, as per the Admin team's instructions.

Once your email account is set up, follow these steps to send bulk emails through Lamplight:

1. Log in to your Lamplight account.

2. Click on the “Record” tab at the top of the screen.

3. Select “Communication,” then click “Create.”

4. Choose “Email” (the first option in the list).

5. In the “Summary for saving” field, include a brief description of the email topic, then click “Next.”

6. In the “2. Recipients” tab, enter the profile numbers or full names of the service users you want to contact. Select as many as needed. As you select them, their names and email addresses will appear in a box below.

   Note: Service users who have opted out of email or bulk communications will not have their email addresses listed, meaning the system will not send the email to them, even if selected.

7. Once you’ve chosen all recipients, click “Next.”

8. In the “Email details” tab:

    - Enter the email subject without using accents (accents in the subject line may display incorrectly to recipients). Accents can still be used in the email body.
    - The "From email address" field will be automatically completed with the email you’ve registered in Lamplight.
    - The "From display name" field will be automatically completed with the organisation’s name, but due to character limits, we recommend changing it to "LAWRS" instead of “Latin American Women's Rights Service".
    - For bulk emails, in the “How do you want to send the emails?” field, always choose the second option: “A single email blind-copied (bcc) to all recipients.” Then click “Next.”

9. In the “Files” tab, attach any necessary files by clicking “Choose file.” You can attach up to 7 files per email. Click “Next.”

10. In the “Message content” tab, write the body of your email. It’s recommended to review the content at least twice to check for typos or errors. When you’re finished, click “Create/Send” at the bottom right.

Tip: It’s strongly recommended to test the process by sending a trial email to yourself. This helps ensure the email is correctly formatted and that all attachments arrive as expected.

Form last updated: July 2025

Appendix 5: LAWRS PRIVACY NOTICE (FOR SERVICE USERS AND GENERAL PUBLIC)

Latin American Women\'s Rights Service customer privacy notice

This privacy notice tells you what to expect us to do with your personal information.

- Contact details
- What information we collect, use, and why
- Lawful bases and data protection rights
- Where we get personal information from
- How long we keep information
- Who we share information with
- How to complain

Contact details

Post: Latin American Women's Rights Service, 52-54 Featherstone Street, LONDON, EC1Y 8RT, GB

Telephone: 0808 145 4909

Email: lawrs@lawrs.org.uk

What information we collect, use, and why

We collect or use the following information to provide services, including delivery and third-party referrals:

- Names and contact details
- Gender
- Pronoun preferences
- Addresses
- Date of birth
- Emergency contact details
- Next of kin details
- Call recordings
- Service use history
- Health information (including medical conditions, test results, allergies, medical requirements and medical history)
- Information about care needs (including disabilities, home conditions, dietary requirements and general care provisions)
- Information about work, home and living conditions
- Information about support requirements
- Criminal offence data
- Records of meetings and decisions
- Information about income and financial needs for funding or personal budget support
- Website user information (including user journeys and cookie tracking)

We also collect or use the following special category information to provide services, including delivery and third-party referrals. This information is subject to additional protection due to its sensitive nature:

- Racial or ethnic origin
- Health information

We collect or use the following information to receive donations or funding and organise fundraising activities:

- Names and contact details
- Addresses

We collect or use the following personal information for service updates or marketing purposes:

- Names and contact details
- Addresses
- Marketing preferences

We also collect or use the following special category information for research or archiving purposes. This information is subject to additional protection due to its sensitive nature:

- Racial or ethnic origin

We collect or use the following personal information for dealing with queries, complaints or claims:

- Names and contact details
- Address

Lawful bases and data protection rights

Under UK data protection law, we must have a "lawful basis" for collecting and using your personal information. There is a list of possible lawful bases in the UK GDPR. You can find out more about lawful bases on the ICO's website.

Which lawful basis we rely on may affect your data protection rights which are set out in brief below. You can find out more about your data protection rights and the exemptions which may apply on the ICO's website:

- Your right of access - You have the right to ask us for copies of your personal information. You can request other information such as details about where we get personal information from and who we share personal information with. There are some exemptions which means you may not receive all the information you ask for. You can read more about this right here.
- Your right to rectification - You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete. You can read more about this right here.
- Your right to erasure - You have the right to ask us to delete your personal information. You can read more about this right here.
- Your right to restriction of processing - You have the right to ask us to limit how we can use your personal information. You can read more about this right here.
- Your right to object to processing - You have the right to object to the processing of your personal data. You can read more about this right here.

- Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you. You can read more about this right here.
- Your right to withdraw consent – When we use consent as our lawful basis you have the right to withdraw your consent at any time. You can read more about this right here.

If you make a request, we must respond to you without undue delay and in any event within one month.

To make a data protection rights request, please contact us using the contact details at the top of this privacy notice.

Our lawful bases for the collection and use of your data

Our lawful bases for collecting or using personal information to provide services and goods, including delivery and third party referrals are:

- Consent, including explicit consent to process special category data - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
- Vital interests – collecting or using the information is needed when someone's physical or mental health or wellbeing is at urgent or serious risk. This includes an urgent need for life sustaining food, water, clothing or shelter. All of your data protection rights may apply, except the right to object and the right to portability.
- Public task – we have to collect or use your information to carry out a task laid down in law, which the law intends to be performed by an organisation such as ours. All of your data protection rights may apply, except the right to erasure and the right to portability.

Our lawful bases for collecting or using personal information to receive donations or funding and organise fundraising activities are:

- Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

Our lawful bases for collecting or using personal information for service updates or marketing purposes are:

- Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

Our lawful bases for collecting or using personal information for research or archiving purposes are:

- Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

Our lawful bases for collecting or using personal information for dealing with queries, complaints or claims are:

- Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
- Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

Where we get personal information from

- Directly from you
- Regulatory authorities
- Family members or carers
- Other health and care providers
- Social services
- Charities or voluntary sector organisations
- Councils and other public sector organisations

How long we keep information

	PROCESSING ACTIVITY	Art 6 lawful basis	Art 9 special-category condition	Typical data held	Retention trigger period
1	Advice, advocacy and casework support	6(1)(b) Contract (service requested by user)	9(2)(d) Not-for-profit with safeguards	Contact details, immigration status, health, children's details, referrals, case notes	6 years after last case entry (Creche contract details stored in Google Drive will be deleted 1 year after last access to the Creche service)
2	Safeguarding referrals or disclosures (not registered in Lamplight as specified in LAWRS Safeguarding policies)	6(1)(d) Vital interests	9(2)(c) Vital interests	As above + risk notes	Until statutory investigation concludes + 1 yea r

3	Recruitment	6(1)(f) Legitimate interests	Art 10 basis DPA 2018, Schedule 1, Part 1, para 1 – Employment & safeguarding	CV, contact details, interview notes, application forms	6 months after recruitment ends
4	Equal-opportunity and impact monitoring (staff and volunteers job applicants)	6(1)(f) Legitimate interests	9(2)(g) Substantial public interest – equality	Ethnicity, sexual orientation, disability	Anonymise after annual report, then delete raw data
5	Email, SMS & postal updates on LAWRS services	6(1)(a) Consent	n/a (no special-categor y data)	Name, email, language preference	Until consent withdrawn or 2 years of inactivity
6	HR & Volunteer management	6(1)(b) Contract	9(2)(b) Employment & social-security law	References, DBS checks, health info, Volunteers application forms (Google form)	6 years for staff and 2 years for volunteers - after employment/volu nteering ends
7	Board & governance records	6(1)(c) Legal obligation (Companies Act, Charities Act)	n/a	Trustee contact details, minutes	Board minutes – permanent; personal data – 6 years after tenure
8	Health and safety incident records	6(1)(c) Legal obligation	9(2)(f) Legal claims	Injury reports, witness statements	40 years from incident (Employers' Liability regs)
9	Google form responses for events	6(1)(a) Consent	n/a (no special-categor y data)	Name, email address, phone number, Date of Birth, Language	Include anonymised data in Lamplight and delete data after event

10	Google form (referrals)	6(1)(a) Consent	n/a (no special-category data)	Name, email address, phone number, Date of Birth, Language,	Upload response in Lamplight and delete response
11	Complaint Records	6(1)(f) Legitimate interests	N/A (unless complaint includes special category data – then 9(2)(f) Legal claims)	Complainant name, contact details, incident details, case notes, outcomes	3 years after complaint resolution
12	Research and evidence collection	6(1)(f) Legitimate interests	9(2)(j) Research purposes with safeguards (if personal data is used)	Survey responses, anonymised service user data, demographic info	5 years after publication
13	Suppliers, providers and contractors information	6(1)(b) Contract	n/a	Name, business contact details, contract terms, payment records	6 years after contract end (per Limitation Act 1980)
14	Accounting and financial information	6(1)(c) Legal obligation (Finance Act 1998, Companies Act 2006)	n/a	Invoices, payroll, receipts, budget reports	6 years from end of financial year (per HMRC guidance)
15	Insurance policy contracts	6(1)(c) Legal obligation	n/a	Policy documents, coverage terms	6 years from policy expiry
16	Employers' liability insurance policies	6(1)(c) Legal obligation	n/a	Policyholder name, cover details, certificate numbers	40 years from policy expiry

17	Supporting documentation for EU-funded projects	6(1)(c) Legal obligation (EU/UK grant conditions)	n/a	Project plans, staff records, budgets, participant registers	five years after the last EU payment/recovery for the project.

For more information on how long we store your personal information or the criteria we use to determine this please contact us using the details provided above.

Who we share information with

Data processors

Lamplight - CRM system: This data processor does the following activities for us: service users data management.

Others we share personal information with

- Charities and voluntary organisations
- Care providers
- Organisations we need to share information with for safeguarding reasons
- Emergency services in case of imminent danger or risk to someone's life
- Legal bodies or authorities
- Local authorities or councils
- Relevant regulatory authorities
- Organisations we're legally obliged to share personal information with
- Professional consultants

How to complain

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy notice.

If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the ICO.

The ICO's address:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Helpline number: 0303 123 1113

Website: https://www.ico.org.uk/make-a-complaint

Last updated July 2025

Appendix 6: LAWRS PRIVACY NOTICE FOR STAFF AND VOLUNTEERS

Latin American Women\'s Rights Service staff / volunteers privacy notice

This privacy notice tells you what to expect us to do with your personal information when you work for us.

- Contact details
- What information we collect, use, and why
- Lawful bases and data protection rights
- Where we get personal information from
- How long we keep information
- Who we share information with
- How to complain

Contact details

Post: Latin American Women's Rights Service, 52-54 Featherstone Street, LONDON, EC1Y 8RT, GB

Telephone: 0808 145 4909

Email: lawrs@lawrs.org.uk

What information we collect and use, and why

Staff recruitment, administration and management

We collect or use the following personal information as part of staff recruitment, administration and management:

- Contact details (eg name, address, telephone number or personal email address)
- Date of birth
- National Insurance number
- Gender
- Copies of passports or other photo ID
- Next of kin or emergency contact details
- Employment history (eg job application, employment references or secondary employment)
- Right to work information
- Details of any criminal convictions (eg DBS checks)

We also collect or use the following special category information for staff recruitment, administration and management. This information is subject to additional protection due to its sensitive nature:

- Racial or ethnic origin

Salaries and pensions

We collect or use the following personal information as part of managing salaries and pensions:

- Job role and employment contract (eg start and leave dates, salary, changes to employment contract or working patterns)
- Time spent working (eg timesheets or clocking in and out)
- Expense, overtime or other payments claimed
- Leave (eg sick leave, holidays or special leave)
- Maternity, paternity, shared parental and adoption leave and pay
- Pension details
- Bank account details

Lawful bases and data protection rights

Under UK data protection law, we must have a "lawful basis" for collecting and using your personal information. There is a list of possible lawful bases in the UK GDPR. You can find out more about lawful bases on the ICO's website.

Which lawful basis we rely on may affect your data protection rights which are set out in brief below. You can find out more about your data protection rights and the exemptions which may apply on the ICO's website:

- Your right of access - You have the right to ask us for copies of your personal information. You can request other information such as details about where we get personal information from and who we share personal information with. There are some exemptions which means you may not receive all the information you ask for. You can read more about this right here.
- Your right to rectification - You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete. You can read more about this right here.
- Your right to erasure - You have the right to ask us to delete your personal information. You can read more about this right here.
- Your right to restriction of processing - You have the right to ask us to limit how we can use your personal information. You can read more about this right here.
- Your right to object to processing - You have the right to object to the processing of your personal data. You can read more about this right here.
- Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you. You can read more about this right here.
- Your right to withdraw consent – When we use consent as our lawful basis you have the right to withdraw your consent at any time. You can read more about this right here.

If you make a request, we must respond to you without undue delay and in any event within one month.

To make a data protection rights request, please contact us using the contact details at the top of this privacy notice.

Our lawful bases for the collection and use of your data

Our lawful bases for collecting or using personal information as part of staff recruitment, administration and management are:

- Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
- Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
- Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.
- Legitimate interests – we're collecting or using your information because it benefits you, our organisation or someone else, without causing an undue risk of harm to anyone. All of your data protection rights may apply, except the right to portability. Our legitimate interests are:
    - we collect racial or ethnic and gender because LAWRS\' recruitment is open to Latin American Women only in accordance with the Equality Act 2010

For more information on our use of legitimate interests as a lawful basis you can contact us using the contact details set out above.

Our lawful bases for collecting or using personal information as part of managing salaries and pensions are:

- Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
- Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

Where we get personal information from

We collect your information from the following places:

- Directly from you
- Referees (external or internal)
- Pension administrators or government departments (eg HMRC and DWP)

How long we keep information

	PROCESSING ACTIVITY	Art 6 lawful basis	Art 9 special-category condition	Typical data held	Retention trigger period

1	Advice, advocacy and casework support	6(1)(b) Contract (service requested by user)	9(2)(d) Not-for-profit with safeguards	Contact details, immigration status, health, children's details, referrals, case notes	6 years after last case entry (Creche contract details stored in Google Drive will be deleted 1 year after last access to the Creche service)
2	Safeguarding referrals or disclosures (not registered in Lamplight as specified in LAWRS Safeguarding policies)	6(1)(d) Vital interests	9(2)(c) Vital interests	As above + risk notes	Until statutory investigation concludes + 1 yea r
3	Recruitment	6(1)(f) Legitimate interests	Art 10 basis DPA 2018, Schedule 1, Part 1, para 1 – Employment & safeguarding	CV, contact details, interview notes, application forms	6 months after recruitment ends
4	Equal-opportunity and impact monitoring (staff and volunteers job applicants)	6(1)(f) Legitimate interests	9(2)(g) Substantial public interest – equality	Ethnicity, sexual orientation, disability	Anonymise after annual report, then delete raw data
5	Email, SMS & postal updates on LAWRS services	6(1)(a) Consent	n/a (no special-categor y data)	Name, email, language preference	Until consent withdrawn or 2 years of inactivity
6	HR & Volunteer management	6(1)(b) Contract	9(2)(b) Employment & social-security law	References, DBS checks, health info, Volunteers application forms (Google form)	6 years for staff and 2 years for volunteers - after employment/volu nteering ends

7	Board & governance records	6(1)(c) Legal obligation (Companies Act, Charities Act)	n/a	Trustee contact details, minutes	Board minutes – permanent; personal data – 6 years after tenure
8	Health and safety incident records	6(1)(c) Legal obligation	9(2)(f) Legal claims	Injury reports, witness statements	40 years from incident (Employers' Liability regs)
9	Google form responses for events	6(1)(a) Consent	n/a (no special-categor y data)	Name, email address, phone number, Date of Birth, Language	Include anonymised data in Lamplight and delete data after event
10	Google form (referrals)	6(1)(a) Consent	n/a (no special-category data)	Name, email address, phone number, Date of Birth, Language,	Upload response in Lamplight and delete response
11	Complaint Records	6(1)(f) Legitimate interests	N/A (unless complaint includes special category data – then 9(2)(f) Legal claims)	Complainan t name, contact details, incident details, case notes, outcomes	3 years after complaint resolution
12	Research and evidence collection	6(1)(f) Legitimate interests	9(2)(j) Research purposes with safeguards (if personal data is used)	Survey responses, anonymised service user data, demographi c info	5 years after publication
13	Suppliers, providers and contractors information	6(1)(b) Contract	n/a	Name, business contact details, contract	6 years after contract end (per Limitation Act 1980)

				terms, payment records	
14	Accounting and financial information	6(1)(c) Legal obligation (Finance Act 1998, Companies Act 2006)	n/a	Invoices, payroll, receipts, budget reports	6 years from end of financial year (per HMRC guidance)
15	Insurance policy contracts	6(1)(c) Legal obligation	n/a	Policy documents, coverage terms	6 years from policy expiry
16	Employers' liability insurance policies	6(1)(c) Legal obligation	n/a	Policyholder name, cover details, certificate numbers	40 years from policy expiry
17	Supporting documentation for EU-funded projects	6(1)(c) Legal obligation (EU/UK grant conditions)	n/a	Project plans, staff records, budgets, participant registers	five years after the last EU payment/recovery for the project.

For more information on how long we store your personal information or the criteria we use to determine this please contact us using the details provided above.

Who we share information with

In some circumstances, we may share information with the following organisations:

- Training suppliers
- HMRC
- Employee benefit schemes
- Health and benefit suppliers
- External auditors
- Suppliers and service providers
- Professional consultants

Data processors

We use the following data processors for the following reasons:

Lamplight

This data processor does the following activities for us: add and remove database operators, service users management database.

Bright HR

This data processor does the following activities for us: employees and volunteers training online courses.

How to complain

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy notice.

If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the ICO.

The ICO's address:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Helpline number: 0303 123 1113

Website: https://www.ico.org.uk/make-a-complaint

Last updated July 2025

Appendix 7: Data Protection Impact Assessment (DPIA)

Project/Service Information

Title of project/service/activity	
Project Lead	
Funder (if applicable)	
Will personal data be processed	**☐ Yes ☐ No (if no, DPIA ends here)**

Summary of Activity

Briefly describe the purpose of the project or service, why personal data is needed, and what will be done with it.

Data requirements

Whose data will be processed? **☐ Service users ☐ Staff ☐ Volunteers ☐ Children ☐ Public**
Approximate number of people: **☐ 1–50 ☐ 50–100 ☐ 100–300 ☐ 300+**
What Personal Data Will Be Used? (e.g. name, email, phone number etc)

Sensitive (special category) or criminal conviction data? ☐ Yes ☐ No
If yes, please specify:

Legal basis for processing

Personal data (non-sensitive)		Sensitive (special category data)	
Consent	☐	**Explicit consent**	☐
Contract	☐	**Employment (social law)**	☐
Legal obligation	☐	**Vital interests (safeguarding)**	☐
Vital interests (safeguarding)	☐	**Criminal data (DPA Schedule 1: Lawrs is required by law)**	☐

Use of Data

Where will data be stored? ☐ Google Drive ☐ Lamplight

Who will access it? (List roles, not names):

Will data be shared with anyone outside LAWRS? ☐ Yes ☐ No

If yes, who and why:

Will it be transferred outside the UK? ☐ Yes ☐ No

If yes, how is it protected?

Security and retention

How will the data be protected? (e.g. encryption, passwords, role-based access):

Retention period:

How will the data be securely deleted after use?

Transparency and rights
Has the Privacy Notice been shared with data subjects? ☐ Yes ☐ No
Can individuals withdraw consent or opt out? ☐ Yes ☐ No

Risk Assessment
What could go wrong (e.g. data leak, unauthorised access)?

What steps will be taken to reduce the risk?

Review and Sign-off

Completed by (project lead): _____

DPO reviewed: _____

Date of completion: _____

Next review due: _____ (usually 1 year)