LATIN AMERICAN WOMEN'S RIGHTS SERVICE
Servicio por los Derechos de la Mujer Latinoamericana
Serviço pelos Direitos da Mulher Latino-americana

Confidentiality and data protection policy

Updated on: May 2022	**Next review**: May 2023
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 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, beneficiaries, members and donors (Individual and collectively Individuals).

Contents:

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 held 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 and filing policy. 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. Volunteers will be required to sign the Volunteer's confidentiality agreement (Appendix 1) during induction. 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 the 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, videotaped, as audio or in any other available and lawful form.

LAWRS Administrators are the designated Data protection officer (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

LAWRS will require consent (verbal or written) from Individuals before collecting any personal data (see Appendix 2). The consent shall be freely given, specific and informed. Therefore, Individuals must understand how the data will be used, with what purpose and how long it will be kept for.
The information collected by LAWRS will:

- Reflect the user's requirements

- Be factual information about what has been discussed and the relevant implications to the case
- Be free of any prejudice
- Be relevant
- Be legible and recorded accurately
- Be 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.

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 beneficiary (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.

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 3) 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 3) 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

Individuals have the right to request access to their personal information free of charge, unless unfounded or excessive information is requested. LAWRS will provide the personal information in writing within 30 working days.

Subject Access requests can be made to any member of staff, who shall:

- Explain the next steps and time frame of the request to the requestant;
- Complete and send the Personal data request form (Appendix 3) 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 inform them of the request.

The relevant Senior Manager will gather the data requested and assess what potential risks it may present to the service user (eg: produce evidence against oneself) and inform the DPO, within 15 working days from the date of request.

Within 20 working days from the date of request, the DPO will inform the requestant of potential risks and confirm if she wishes to proceed with the request.

If she does, the DPO will send (via email, if possible) the information requested to the service user within 30 working days and will then update LAWRS' case management system.

LAWRS will seek to resolve requests within 30 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.

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' computers and cloud.
- The DPO is responsible for monitoring the change of passwords.

4.1 Casework and work records

A copy of this policy is available upon request to any Individual.

Staff shall keep written records of all the sessions held with a user in accordance with LAWRS' Recording and filing policy. These records are confidential.

The folders containing the users' casework and work records should remain at LAWRS at all times and/or kept within the LAWRS' case management system.

Only staff and the Director are to have access to the users' casework folders and the LAWRS' case management system. Volunteers may access a casework folder and the LAWRS' case management system only when they are working on a specific case and are being directly supervised by a member of the staff.

The Senior Management Team is responsible for ensuring that all the cases are kept locked and properly stored in the LAWRS' case management system. All filing cabinets should be locked and all staff should be logged out of the LAWRS' case management system at the end of each working day.

If at any moment a member of staff meets a user outside LAWRS' premises in a situation that is not related to her support (e.g. by chance, social gathering, etc.), she should abide by the principles outlined in this policy. In this situation, no reference should be made to the information held about the user. There should be no reference to work or any details pertaining to her case.

4.2 Staff

The staff members' personal files will be kept in the Cloud. Management of files will only be done by the Administrators and Senior Management Team. In exceptional circumstances, the Board may have access to a member of staff personal files.

4.3 Volunteers

The Volunteers' coordinator will manage the volunteers' personal files. The Administrators and Senior Management Team will also have access to volunteers' personal files.

4.4 Members

Members' personal information will be kept in LAWRS' Case management system. 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 Cloud. 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.

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 Operations Manager or the Fundraising and Development Manager, 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 beneficiaries".

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. The post addressed to the staff shall be placed in each of their pigeonholes. 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. In some cases, it is also legally privileged. If you are not the addressee any disclosure, reproduction, distribution or other dissemination or use of this communication is strictly prohibited. If you have received this transmission in error please contact us immediately by telephone or email so that we can arrange for its return or delete your email address from our database".

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 4) 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 on the GDPR, which was enforced from the 25th of May 2018, when it superseded the UK Data protection Act 1998. Therefore, the collection, processing and storage of personal information is done in accordance with such law.

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. 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:

- Documents relevant to staff recruitment will be kept for six months, after which they will be destroyed.
- Information about staff will be kept for six years after their contract has ended, that includes information kept as hard-copies or in digital format containing such information.
- Information about creche workers will be kept for six years after their last working day.
- Information about children attending the creche service will be kept for 1 year after their last session.
- The information given to LAWRS by our members will be kept for one year after their membership has expired, except if they have accessed any of the services provided by LAWRS within the last six years. In that case, information will be kept for six years after they last accessed LAWRS services. After one year or six years, whichever translates the member's journey through LAWRS, the file will be destroyed
- User's casework, work records and any other personal information will be kept for six years after the last entry in the LAWRS' case management system, after which it will be destroyed.
- Volunteers' personal information will be kept for two years after their programme has ended, after which it will be destroyed.
- Complaint records will be kept for 3 years from the date of the complaint, after which it will be destroyed.
- Research evidence will be kept for five years after its publication.
- Providers and Contractors' information will be kept for six years after their service has ceased or the contract has ended.
- LAWRS' accounting and financial information will be kept for six years, after which it will be destroyed.
- Insurance policy and contracts will be kept for 6 years after its expiring date, after which it be destroyed
- For EU funded projects, supporting documentation, including accounting and financial information and outcome monitoring must be kept for at least 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).

Approved by LAWRS' Management Committee:

_____	_____
Chair Signature	**Secretary Signature**

Appendix 1: Volunteers' confidentiality agreement

VOLUNTEERS' CONFIDENTIALITY AGREEMENT

The nature of LAWRS' work and its Confidentiality and data protection policy require that all volunteers maintain strict confidentiality at all times. The following agreement outlines our expectations of volunteers at LAWRS to maintain confidentiality.

By volunteering with LAWRS you are accepting to abide by this guidance and LAWRS policies. This does not in any way formulate a legal contract of employment.

1. Confidential information includes: identification by name or other significant personal information; personal address/ telephone number or email; nationality; family members; immigration and marital status; discussion of an individual case. This list is not exhaustive. Confidential information is not to be shared with a third party or taken outside LAWRS premises, unless as an exception covered by LAWRS Confidentiality and data protection policy. Volunteers may not contact LAWRS' service users unless explicitly required.

2. We have a duty under the law to report cases of child or vulnerable adult abuse or situations where a child or a vulnerable adult may be at risk to the relevant authorities. Volunteers must follow LAWRS' procedures and approach the most relevant member of staff with such cases for instructions prior to contacting third party organisations.

3. The disclosure of confidential information related to a client, another volunteer, a trustee or staff member is permissible only in accordance with the provisions of LAWRS Confidentiality and data protection policy. Express consent from the client, volunteer or staff member must have been sought prior to sharing any personal information. Please ask a member of staff for approval.

4. If in a social setting with a client, volunteer or member of staff, individual cases must not be discussed.

5. Information controlled under the Data protection act 1998 and the General data protection regulation (GDPR) require (among other points) that: information is solely used for the purpose for which it was acquired; it is kept secure; and is used in accordance with the rights and requests of the person to whom it belongs.

6. Working from home: service users information should not be stored outside LAWRS Team Google Drives (e.g. your hard drive, desktop, personal phone,etc.). If using a personal device, ensure a separate LAWRS user account is created and the device is password protected. All work carried out for LAWRS should be done from this separated user

account. When calling from a personal mobile phone, make sure not to show your ID Caller and to delete any information from equipment as soon as you finish.

7. N
ever leave your device unattended. If you have to leave it for any reason, make sure to lock the user.

8. E
specially when working from home, make sure to regularly update firewalls, virus protection or other applicable security systems and provide suitable information to service users to enable them to protect their end of the communications as well.

9. C
ontact GDPR Officer (administrators) whenever in doubt & if you have any suspicion of personal data leak

10. V
olunteers' own personnel files are maintained locked or safely secured in staff computers. This information is kept strictly confidential and is accessible only to relevant staff (volunteer, Volunteers' Coordinator, Director, Operations and Development Manager, Administrator, Communication Officers, and relevant project coordinators) only. For further information about the way in which LAWRS handles your personal information, please refer to LAWRS Confidentiality and data protection policy.

LAWRS uses anonymised data, to improve services, for research purposes, to promote its work, and to increase awareness of donors, partners, the general public and others about the problems affecting its beneficiaries. Anonymisation involves removing all identifying information so the individual can no longer be recognised.

Caution should always be exercised as the smallest amount of information can identify a person to someone who knows them well.

	I agree to abide by the terms of this agreement.
	I understand the content of this document and agree to adhere to LAWRS Confidentiality and data protection policy, a copy of which has been provided to me as part of the induction to my volunteering role along with a copy of the Safeguarding and child protection policy and procedure and Safeguarding Adults policy and procedure.
	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 my photos and footage of me recorded while participating in activities organised by LAWRS in publications, campaigns, material, adverts, display material, electronic material, media work, etc.
	I understand that edited information, that would not identify me, may be included in LAWRS public communication.

Volunteer's Name:

Volunteer's signature:

Date:

Form last updated: May 2022

Appendix 2: Client consent form

Client consent form

In accordance with current legislation (Data Protection Act 1998 and GDPR), LAWRS requires your express consent to process, record, and store your personal information, including any relevant sensitive data.

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 beneficiaries.

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. Beneficiaries' 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 3: 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 be Forgotten Request
	Subject Access Request

Requestant's details:

Name:		
Telephone:		
Address:		
Email:		
Preferred communication means:	**Post**	**Email**

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, withdraw 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	up to 90 days of date of request

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: May 2022

Appendix 4: 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

Form last updated: May 2022