



Policy Number	Review Date	Next Review Date
7	March 2026	March 2027

Little Village Data Protection and Retention Policy and Procedures

Introduction

Little Village is committed to a policy of protecting the rights and privacy of individuals. Little Village needs to collect and use certain types of Data in order to carry out our work. This personal information must be collected and dealt with appropriately.

The Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) May 2018 governs the use of information about people (personal data). It was amended by the Data Use and Access Act 2025 (DUAA). Personal data can be held on a computer or in a manual file, and includes, but it not limited to, email, minutes of meetings, and photographs. Little Village will remain the Data Controller for the information held. Little Village and volunteers will be personally responsible for processing and using personal information in accordance with the GDPR.

Alongside UK GDPR we also work to the guidelines of the PECR (Privacy and Electronic Communications Regulations)

Trustees, employees and volunteers running Little Village who have access to personal information, will be expected to read and comply with this policy.

Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username

	It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Purpose

The purpose of this policy is to set out Little Village's commitment and procedures for protecting personal data. Little Village regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

1. We want to collect limited personal information of clients to fulfil a referral request.
2. We want to use (1) to contact individuals about deliveries, product safety recalls or other information critical to completing our referral service.
3. We want to use (1) to contact individuals who have received our support to inform them about changes to our service or events which might be of interest to them.
4. We want to collect personal information from our referral partners and volunteers in order to ensure good communication.
5. We want to maintain a list of people who donate to us to thank them and so that we can contact them to let them know what difference their support has made and ask them to consider further donations.
6. We want to maintain a list of people who have donated physical items to say thank you and to ask if they would like to hear from us further.
7. We want to claim gift aid on a person's donations where appropriate.
8. We want to research and build profiles of donors to better understand them and target our communications appropriately and with the most relevant information.
9. We want to maintain accurate records of clients to anonymise data to use in funding applications and publicity.
10. We want to maintain accurate records to ensure we comply with legislation concerning Safeguarding and/or Health and Safety recording and/or for insurance purposes.
11. We want to use the limited personal data we collect and store for 5 years before anonymising for long term use to assess the impact of our services.
12. We want to maintain a list of people who have explicitly told us that they don't want to be contacted by us again.
13. We want to maintain contact information for anyone who has volunteered for Little Village so we can contact them about future volunteering opportunities.
14. We want to keep our volunteer, client and referrer database information up to date.
15. We want to maintain accurate staff records, in line with our HR suite of policies.
16. We want to keep a list of people who have expressed an interest in/given permission for their photos and/or stories to be used for media purposes, either anonymously and/or named.

The UK GDPR

In line with the UK GDPR principles, Little Village will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specific and lawful purpose.
- Be adequate, relevant but not excessive.
- Be accurate and kept up to date.
- Not be held longer than necessary.
- Be processed in accordance with the rights of data subjects.
- Be subject to appropriate security measures.
- Not be transferred outside the UK. If transferred outside the UK, it meets the processing guidelines as stipulated in UK GDPR law.
- Wherever possible personal data will not be kept and/or will be anonymised.

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes paper based personal data as well as that kept on computer/electronic devices.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

Type of Information Processed

Little Village processes the following personal information (information that allows a person to be identified):

- Volunteer name, address, email and contact number, date of birth, next of kin details, ethnicity and religion (optional), plus medical conditions if they choose to disclose.
- Referrer name, email address and contact number, name and type of their organisation, as well as their role.
- Client name, email address, phone number, address, sex and age of children, date of birth, ethnicity, language and religion (optional), and housing association name where relevant (optional).
- Sensitive, referral specific data (Special Category Data) to assist processing the referral itself and/or requested signposting and guidance to other services.
- Donor (kit and financial) name, email address, phone number and address.
- Information required by HMRC in relation to financial donations subject to Gift Aid
- Publicly available researched information on individuals and organisations.
- Employee name, address, email, contact number, medical information, next of kin, payroll and bank details.
- Trustee name, address, email, contact number, medical information and next of kin.
- We also collect photos and stories used for advocacy and publicity. We always obtain specific written consent for these materials before collection and sharing.

Personal information (including at time Special Category Data) is entered onto a secure form by the referrer, volunteer or donor and is transferred via a third party application to the client database. If paper requests of referrals or volunteer applications are received they are uploaded to the client database upon which the paper copy is destroyed.

Information may be shared with us by fundraising sites like JustGiving, Enthuse or Virgin Money Giving or by event organisers such as the Royal Parks Half Marathon. These independent third parties will only do this when a person has specified that they wish to support Little Village and give their clear consent.

Information may be shared with us via referrals from trustees, volunteers or employees when a person gives their consent to do so.

Employees' data including personal and financial records are only available to the People team, CEO, Finance Manager, Finance Board Member and payroll. Employee Special Category Data is only available to the People team and, in some circumstances and only with their permission, shared with a data subject's line manager. Employee name and salary level is available to the Remuneration Committee of the Little Village Board.

Additionally, the organisation's Data Controller and IT support services are able to access personal data only under special circumstances, for example to meet legal obligations under a Subject Access Request.

Groups of people within the organisation who will process personal information are:

- Trustees, employees, and volunteers

PECR Remit for the purposes of data protection

There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Applying the UK GDPR within Little Village

Whilst access to personal information is limited to the aforementioned employees and volunteers at Little Village, volunteers at Little Village may undertake additional tasks which involve the collection of personal details from members of the public.

In such circumstances we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

Correcting data

Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress or to stop marketing information being sent to them.

Responsibilities

Little Village is the Data Controller under the UK GDPR, and is legally responsible for complying with the UK GDPR, which means that it determines what purposes personal information held will be used for.

The Board of Trustees, and employees where delegated through Little Village's Governance Framework, will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information,
- Meet its legal obligations to specify the purposes for which information is used,
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- Ensure the quality of information used,

- Ensure that the rights of people about whom information is held, can be fully exercised under the GDPR. These include:
 - The right to be informed that processing is being undertaken
 - The right of access to one's personal information
 - The right to prevent processing in certain circumstances and
 - The right to correct, rectify, block or erase information which is regarded as wrong information
- Take appropriate technical and organisational security measures to safeguard personal information,
- Ensure that personal information is not transferred abroad without suitable safeguards,
- Keep a record of any breaches or potential breaches of data, including full action to remedy the situation,
- Risk assess and, where necessary, report to the ICO any relevant breaches within 24-hours of the Director of Operations being made aware,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information. Set out clear procedures for responding to requests for information.

Transfer of Data outside of the UK, following the UK's exit from the EU

Following the UK's exit from the EU, Little Village is mindful of the transfer of data outside of the UK. The UK GDPR regulations broadly mirror the EU GDPR regulations. However, during a transition period post-exit, the EU has adopted an 'adequacy regulation' whilst it waits the outcome of a final decision on data transfers. As Little Village does not currently process any data from outside of the UK, it will follow the principal of the UK GDPR rules. For all data transfers from the UK to the EEC and other international destinations, it will be monitored on a case by case basis and adequate safeguards put in place.

In line with Article 30 of the EU GDPR, we will conduct a full data audit to produce a data processing record, including the destination of any data. In line with Article 49, this record will include a full list of safeguards.

As useful quick reference to information relating to updated UK GDPR, following the UK's exit from the EU can be found here: <https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/navigating-the-data-sharing-code/>

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Little Village data protection issues.

The DPO is also the first point of contact for individuals whose data the organisation processes, and for the ICO.

Little Village has an independent data protection officer service supplied by Global Policing Limited. Global Policing is an organisation run by ex-senior police officers who specialise in working with schools and have

vast experience in data protection matters. If you have any questions or comments or wish to make any requests under the Regulations, you should contact them directly:

Telephone (answerphone) 0161 510 2999
Email data@globalpolicing.co.uk
Website www.globalpolicing.co.uk/data

The Data Protection Officer(s) will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

- Ensuring everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Ensuring everyone processing personal information is appropriately trained to do so
- Ensuring everyone processing personal information is appropriately supervised
- Ensuring anybody wanting to make enquiries about handling personal information knows what to do
- Dealing promptly and courteously with any enquiries about handling personal information
- Describing clearly how Little Village handles personal information
- Regularly reviewing and auditing the ways Little Village holds, manages and uses personal information
- Regularly assessing and evaluating Little Village's methods and performance in relation to handling personal information
- Ensuring all employees and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the UK GDPR.

All data protection enquiries within Little Village should be addressed to Data Manager, Emily Compston, emily@littlevillagehq.org.

Training

Training and awareness raising about the GDPR and how it is followed in this organisation will take the following forms:

On induction: all volunteers are given a copy of our data protection policy and asked to sign the Volunteers' Agreement to show they have read and understood it. Specific induction is given regarding volunteer roles that deal with personal data. Only specific employees and trustees have access to passwords and locked files.

General training / awareness raising: Before every session attended by families we support and/or picking and packing, there is a reminder briefing in which the responsibilities of the volunteer and data protection are highlighted.

All staff undertake an online data protection training course. Training records are maintained.

Further training is available to trustees and employees through outside agencies where necessary and a training log is kept of those who have attended.

Additional training is available to employees and volunteers to reflect an increase in homeworking. Additional mobile phone devices have been provided where possible to minimise the use of personal phones when contacting families and referral partners. All employees and volunteers using their own mobile devices follow strict safeguards to ensure that calls are made from withheld numbers and any numbers called are deleted from their phones on a regular basis.

All staff will receive training at least every 2 years.

Data collection

Before personal information is collected, we will consider:

What information we need in order to deliver our service efficiently

What information we need in order to show the impact of our service

What information we need in order to secure the financial sustainability of the charity

What information we need in order to meet our legal and statutory obligations

How long we will keep the information on record -

- We will keep data on clients for a maximum of 5 years from the client's last use of our service.
- We will keep volunteer data for 5 years after their last contact with us, then it will be deleted.
- We will keep data on Gift Aid declarations for 6 years, in accordance with HMRC regulations.
- We will keep donor records for a maximum of 6 years from the last contact with them
- Anonymised data and aggregate totals will be maintained beyond the destruction of individual records so we can assess the impact of our services.
- We keep some data on employees for up to 15 years, as an insurance requirement (Safeguarding), when they have had access to children or vulnerable adults.
- We will keep employee data relating to accounting records such as payroll information and expenses for 6 years in accordance with government guidelines and for compliance purposes
- We will keep data on children we have hosted at a creche facility for 20 years, to meet legal requirements.

We will inform people whose information is gathered about the following:

- That we need key information in order to deliver our service.
- That their information will be recorded in our Client Database, which is only accessed by employees, specific types of volunteers and trustees and is password protected.
- That by ticking the box on the referral form, they consent to Little Village using their anonymised data.
- That by ticking the box on the referral form, they can opt in to our communications about future events, etc.
- That by ticking the box on the referral form, they consent to being contacted in order for us to complete our service (such as making an appointment, delivery, product recall, out of stock items).
- That donors who donate will need to explicitly opt into our communications, that they can opt out at any time and how to get in touch to do so.

- That employees will have relevant financial and personal information kept in the HR files in order to enable Little Village to meet legal and contractual obligations.
- Employee Special Category Data will only be held in order to meet legal and/or for compliance purposes and will be held in a secure file, only accessible on a need to know basis. In usual circumstances, this means it will not be accessed by employees other than the People team, nor will it be disclosed to others without the express consent of the data subject.

Data Security

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- All referrals are made to a secure web form, which only employees have access to. That data is transferred electronically to our database/CRM, which is password-restricted and two-factor authentication is enabled. Only employees and specific volunteers working in family liaison/Signposting have access to that database.
- 3rd party IT and tech support may also have access to this data. All 3rd party data processors are required to provide a copy of their own data security policies and agree that they process data in line with UK GDPR.
- Clients are requested to give their full address for the purposes of delivery only. Clients are asked to give their email address and phone number, to enable appointments to be made directly at some sites and for follow-up communication regarding their online order and/or to confirm address and delivery date. The data is also used to verify whether the client is a duplicate and/or a repeat or new referral.
- Volunteers are sometimes required to collect the above data from clients and record on a paper referral form. All volunteers are specifically told in their induction and reminded at each session briefing that all paper copies of referral documents should be given to the Hub Manager or Referrals Manager at the end of each session.
- Any paper referrals that are taken by family liaison volunteers are passed to the Referrals Manager who will shred them once the information has been uploaded to the client database.
- All volunteer information is contained on a secure database, which is only accessible to certain employees and volunteers.
- Financial Donor information is contained on a secure password protected online platform, Beacon. A limited volume of data remains on spreadsheets and within relevant electronic folders which are only accessible to certain employees with access to the relevant Microsoft Teams site. During 2026 there will be a process to dispose of personal data previously held in spreadsheets.
- Kit donor collection information is contained in separate spreadsheets and is only accessible to certain employees with access to the relevant Microsoft Teams site. Some kit donor details are entered via the Beacon platform as part of arranging a collection service and associated payment.
- We do not keep paper copies of DBS Certificates and only a record of DBS numbers and their date of issue is kept on a spreadsheet, stored in a secure area of Microsoft Teams.
- Little Village will use our best efforts to ensure that any outside agencies or contractors used to process data (such as payroll, fundraising etc.) also comply to the law and will adhere to the UK GDPR regulations.

- Photographs taken on site are carefully coordinated to ensure that no personal information has been inadvertently displayed (eg box labels showing names/addresses)
- Photographs of individuals are only taken and stored with their express consent. Photos are deleted from devices after they have been uploaded to a password protected database.

Use of Artificial Intelligence (AI)

Little Village may use approved artificial intelligence tools to support our administrative and operational work. AI systems will only be used in ways that comply with this policy, the UK GDPR, and our internal AI Use Policy. No personal data — particularly beneficiary, volunteer, donor or employee information — may be entered into AI tools unless the tool has been approved for that purpose, meets our data-security standards, and offers appropriate safeguards. All staff and volunteers must follow the AI Use Policy when using AI tools in the course of their work.

Information and Cyber Security

Little Village maintains a separate Information Security and Cybersecurity Policy outlining the technical and organisational controls in place to protect personal data. This includes system security measures, device management, incident response, cyber resilience, password and authentication standards, and supplier security checks. All staff and volunteers must comply with these requirements alongside this Data Protection Policy.”

Existing Records

Little Village intends to use the “legitimate interest” principle of the GDPR in relation to information about volunteers and donors which was collected and stored before the date of this policy. Appendix 1 details the circumstances in which legitimate interest will be applied.

Data Breach

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary action being taken.

The trustees are accountable for compliance of this policy. A trustee could be personally liable for any penalty arising from a breach that they have made.

Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.

If a volunteer or employee is made aware of a data breach they should notify their line manager who will then inform the Director of Operations.

Any serious data breaches or data loss will be reported to the Information Commissioners Office and the Charity Commission. This includes:

- Charity data that has been accessed by an unknown person and/or deleted.
- A charity device, containing personal details of beneficiaries or employees, has been stolen or gone missing and it’s been reported to the police;
- Charity funds lost due to an online or telephone ‘phishing scam’, where trustees were conned into giving out bank account details;

- A Data Protection Act breach has occurred and been reported to the ICO.

Data Subject Access Requests (SARs)

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. When a SAR is received we may only make searches that are reasonable and proportionate, as advised under the DUAA 2025. Any person wishing to exercise this right should apply in writing to the Director of Operations, Emily Compston (emily@littlevillagehq.org).

We currently contract a third party Data Specialist – Global Policing – to manage any Subject Access Requests. All SARs will therefore be forwarded to Global Policing, who will undertake ongoing correspondence with the requester, and redact documents where appropriate and lawful to meet our obligations to other individuals.

The following information will be required before access is granted:

- Full name and contact details of the person making the request
- Relationship with the organisation and applicable timescales

We may also require proof of identity before access is granted. The following forms of ID will be required: passport, birth certificate.

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 28 days required by the UK GDPR from receiving the written request.

Disclosure

Little Village may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Little Village to disclose data (including sensitive data) without the data subject's consent.

These are:

1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person
3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion

6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. a safeguarding concern for the welfare of the child or adult
7. There is a contractual basis, such as to meet a contract with that person.

Little Village regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Volunteers should be aware that they can be personally liable if they use clients' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of Little Village is not damaged through inappropriate or unauthorised access and sharing.

Further information

If members of the public/or stakeholders have specific questions about information security and data protection in relation to the Little Village please contact the Head of Operations.

The Information Commissioner's website (www.ico.gov.uk) is another source of useful information.

Signed:

Sophie Livingstone,
CEO, Little Village

Reviewers:
Emily Compston, Director of Operations, Trustee

Review Date: March 2026

Appendix 1: Little Village GDPR Approaches

Background and Definitions

CONSENT

Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the Act gives effect) defines an individual's consent as:

...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Under the GDPR, organisations using consent as the basis for contact or data processing, will need to actively collect and then maintain consents (opt-ins) from existing and new contacts in order to store information, or before any contact can be made (using personal data). The bar is set very high on the quality of this consent.

LEGITIMATE INTEREST

Under the UK GDPR, Little Village may continue to rely on “legitimate interests” as a lawful basis for some processing activities where this is necessary to support our operational functions, where individuals would reasonably expect such processing, and where these interests are not overridden by the rights and freedoms of the data subject.

The Data (Use and Access) Act 2025 introduces an additional lawful basis called **Recognised Legitimate Interests (RLI)**. For specific, legally defined purposes—including disclosures to public bodies carrying out public tasks, safeguarding vulnerable individuals, crime prevention, national/public security and responding to emergencies—we may rely on **Recognised Legitimate Interests** without needing to complete the traditional balancing test. For these purposes we must still document that the processing is **necessary**, but are not required to undertake a full Legitimate Interest Assessment (LIA).

For all other circumstances where Little Village relies on standard legitimate interests—such as contacting active volunteers and referrers, maintaining operational records, or undertaking administrative analysis—we will continue to complete an appropriate Legitimate Interest Assessment (LIA) and ensure that our interests do not override the rights and expectations of the individual.

DUAA 2025 also introduces an extended **soft opt-in** for charities, allowing us to send certain electronic marketing messages to supporters whose details were obtained through engagement with our charitable purposes, unless they opt out. This is distinct from legitimate interest and is covered within our marketing and communications section.

Our Records of Processing Activities (RoPA), privacy notices and staff training will be reviewed and updated to reflect the introduction of Recognised Legitimate Interests and the extended soft opt-in for charities.

Proposed Approaches for Little Village

Our updated Data Protection Policy outlines the personal information we collect on various groups that come into contact with our charity, why this is collected and how and why it is held. We have updated all of the forms we use to collect this information to contain a robust set of consents around storing data and opt-ins for future contact for relevant reasons depending on the group of people using the form. Given consents will be recorded and stored securely.

To judge which route should apply, and to enable us to articulate these to others, we set out to establish some principles.

- We believe we have a legitimate interest to contact volunteers and referrers which enable us to operate.
- We would balance the interests of volunteers and referrers with our need to operate.
- Where we are using legitimate interest we would ensure we are staying within the realms of what people might expect.
- We would use legitimate interest as a basis to contact engaged volunteers and referrers with materials consistent with their current behaviour.
- We would use legitimate interest to contact existing volunteers and referrers with newsletters and through this route invite further participation via consent.
- We would use consent for all new contact service users, volunteers and referrers.
- We would use legitimate interest to contact families via email if they have given their consent for the purposes of making an appointment.

Fundraising

We believe the collection and use of donors' personal information is necessary and in the charity's legitimate interests so that Little Village can engage with supporters effectively, use resources efficiently and raise funds to support our beneficiaries.

Currently we rely on explicit opt-in for marketing communications. However, this is under review on an ongoing basis and we may at a later date reply on the "soft opt-in" approach:

Under the Data (Use and Access) Act 2025, the "soft opt-in" exemption has been extended to charities. This allows us to send electronic marketing communications (such as emails or SMS messages) to individuals whose contact details we obtained in the course of their engaging with our charitable purposes — for example donating money, donating kit, taking part in events, or expressing interest in our work — provided that:

- the communication relates only to furthering our charitable purposes;
- the individual was given a clear opportunity to opt out at the point their information was collected; and
- an unsubscribe/opt-out option is included in every message.

For supporters who do not fall within the soft opt-in conditions, we will rely on explicit consent before sending electronic marketing.

We will continue to rely on legitimate interests for communications with corporate donors, charitable trusts and funding bodies, where the communication is relevant to their existing relationship with Little Village.

We will record and securely store supporter consents and opt-outs, ensure our CRM distinguishes between soft-opt-in and consent-based contacts, and provide clear privacy information explaining how donors' data is used and their rights.