

## **DATA PROTECTION POLICY**

### **Data protection procedures**

#### **1) Introduction**

1. **Leasowe Play Youth & Community Association** has a data protection policy which is reviewed regularly. In order to help us uphold the policy, we have created the following procedures which outline ways in which we collect, store, use, amend, share, destroy and delete personal data.
2. These procedures cover the main, regular ways we collect and use personal data. We may from time to time collect and use data in ways not covered here. In these cases we will ensure our Data Protection Policy is upheld.

#### **2) General procedures**

1. Data will be stored securely. When it is stored electronically, it will be kept in password protected files. When it is stored online in a third party website (e.g. Google Drive) we will ensure the third party comply with the GDPR. When it is stored on paper it will be filed carefully in a locked filing cabinet.
2. When we no longer need data, or when someone has asked for their data to be deleted, it will be deleted securely. We will ensure that data is permanently deleted from computers, and that paper data is shredded.
3. We will keep records of consent given for us to collect, use and store data. These records will be stored securely.

#### **3) Mailing list**

1. We will maintain a mailing list. This will include the names and contact details of people who wish to receive , publicity and fundraising appeals from **Leasowe Play Youth & Community Association**
2. When people sign up to the list we will explain how their details will be used, how they will be stored, and that they may ask to be removed from the list at any time. We will ask them to give separate consent to receive publicity and fundraising messages, and will only send them messages which they have expressly consented to receive.
3. We will not use the mailing list in any way that the individuals on it have not explicitly consented to.

4. We will provide information about how to be removed from the list with every mailing.
5. We will use mailing list providers who store data within the EU.

#### **4) Supporting individuals**

1. From time to time, individuals contact the **Leasowe Play Youth & Community Association** to ask us to help them resolve an issue they are having with the council, relating to their housing or other local services.
2. We will request explicit, signed consent before sharing any personal details with the council or any other relevant third party.
3. We will not keep information relating to an individual's personal situation for any longer than is necessary for the purpose of providing them with the support they have requested.
4. Personal data relating to housing issues will be stored securely by a member of the committee, and not shared among the rest of the committee or with other volunteers unless necessary for the purpose of providing the support requested.
5. Details relating to individual's circumstances and housing will be treated as strictly confidential.

#### **5) Fund Raising Activities**

1. We may on occasions sell items relating to **Leasowe Play Youth & Community Association**, to help raise money for the group.
2. To order items, people complete an order form from the community centre, which includes providing a name and address for the items to be delivered to.
3. When ordering, people will be asked if they wish to be added to our mailing list (see section 3). If they do not opt to be on the mailing list, their details will be deleted within one month of processing their order, and will not be used for any purpose other than communicating with them about their order.

#### **6) Contacting volunteers**

1. Local people volunteer for **Leasowe Play Youth & Community Association** in a number of ways.
2. We will maintain a list of contact details of our recent volunteers. We will share volunteering opportunities and requests for help with the people on this list.
3. People will be removed from the list if they have not volunteered for the group for 12 months.
4. When contacting people on this list, we will provide a privacy notice which explains why we have their information, what we are using it for, how long we will keep it and that they can ask to have it deleted or amended at any time by contacting us.
5. To allow volunteers to work together to organise for the group, it is sometimes necessary to share volunteer contact details with other volunteers. We will only do this with explicit consent.

## 7) Contacting committee members

1. The committee need to be in contact with one another in order to run the organisation effectively and ensure its legal obligations are met.
2. Committee contact details will be shared amongst the committee.
3. Committee members will not share each other's contact details with anyone outside of the committee, or use them for anything other than **Leasowe Play Youth & Community Association** business, without explicit consent.

## 8) Review

**These procedures will be reviewed every two years**

Date...31 MARCH 2020

Signature (Chair).....*Jane Davies.*

Signature (Secretary).....*Jenni Jones*

## **DATA PROTECTION POLICY**

### **Data Protection Policy:**

#### **1) Definitions**

1. Personal data is information about a person which is identifiable as being about them. It can be stored electronically or on paper, and includes images and audio recordings as well as written information.
2. Data protection is about how we, as an organisation, ensure we protect the rights and privacy of individuals, and comply with the law, when collecting, storing, using, amending, sharing, destroying or deleting personal data.

#### **2) Responsibility**

1. Overall and final responsibility for data protection lies with the management committee, who are responsible for overseeing activities and ensuring this policy is upheld.
2. All volunteers are responsible for observing this policy, and related procedures, in all areas of their work for the group.

#### **3) Overall policy statement**

1. **Leasowe Play Youth & Community Association** needs to keep personal data about its committee, members, volunteers and supporters in order to carry out group activities.
2. We will collect, store, use, amend, share, destroy or delete personal data only in ways which protect people's privacy and comply with the General Data Protection Regulation (GDPR) and other relevant legislation.
3. We will only collect, store and use the minimum amount of data that we need for clear purposes, and will not collect, store or use data we do not need.
4. We will only collect, store and use data for:
  - purposes for which the individual has given explicit consent, or
  - purposes that are in our group's legitimate interests, or
  - contracts with the individual whose data it is, or
  - to comply with legal obligations, or
  - to protect someone's life, or

- to perform public tasks.
- 5. We will provide individuals with details of the data we have about them when requested by the relevant individual.
- 6. We will delete data if requested by the relevant individual, unless we need to keep it for legal reasons.
- 7. We will endeavour to keep personal data up-to-date and accurate.
- 8. We will store personal data securely.
- 9. We will keep clear records of the purposes of collecting and holding specific data, to ensure it is only used for these purposes.
- 10. We will not share personal data with third parties without the explicit consent of the relevant individual, unless legally required to do so.
- 11. We will endeavour not to have data breaches. In the event of a data breach, we will endeavour to rectify the breach by getting any lost or shared data back. We will evaluate our processes and understand how to avoid it happening again. Serious data breaches which may risk someone's personal rights or freedoms will be reported to the Information Commissioner's Office within 72 hours, and to the individual concerned.
- 12. To uphold this policy, we will maintain a set of data protection procedures for our committee and volunteers to follow.

## **4) Review**

**This policy will be reviewed every two years**

**Date...31 MARCH 2020**

**Signature (Chair).....*Jane Davies.***

**Signature (Secretary).....*Jenni Jones***

# **DATA PROTECTION POLICY**

## **GDPR INFORMATION SHEET**

### **Storing Personal Data**

#### **Personal data must be stored securely.**

If you keep personal data in computers, your computers should be password protected. You should have up-to-date software to protect them from malware and viruses. If you store information on paper, it should be filed securely.

If you store personal data on the internet (e.g. attached to emails, in Google Drive, in Dropbox, etc) you should check that the companies storing the data comply with GDPR regulations and that the data is not transferred outside of the EU. Most big companies have privacy policies which confirm they comply.

It is important that you know who is storing data on behalf of your group, and that everyone understands the need to keep it secure and up-to-date. It's best to agree a system, and to minimise the number of places you are storing data. Otherwise you can easily lose track of what you have. A simple way to do this is to have one central list of contacts, either on paper, on a computer, or securely stored online, which everyone refers to. It's best to nominate one person to look after the list. In many groups this would be the secretary's job.

*For example, your group's secretary might keep an up-to-date copy of all your members' contact details in their computer. Another committee member is organising an event, and needs to contact all the members to tell them about it. The secretary sends them the list by email. The committee member downloads the list into their own personal computer. (The computer should be password protected and have up-to-date anti-spyware software.) Once the committee member has done the task, they should delete the copy from their computer and emails, so that the group does not lose track of who is storing what information.*

Avoid keeping data for the group on an ad-hoc basis in personal phones and address books. If you write down someone's details when you are out and about, add them to the central list and then delete them from your private phone or address book.

Although it is useful to nominate one person to look after personal data for your group, it is very important that you *do not* refer to this person as a “Data Protection Officer”. This is because the term “Data Protection Officer” has specific legal meaning, and organisations that have a Data Protection Officer have additional obligations which small groups do not need to worry about.

## Keeping in touch with your committee

To organise together as a group, the core people involved in making things happen need to be able to contact one another.

Your committee, or core organising group, generally need to have one another’s contact details so that you can all work together well. This is different from the contact details of your wider membership, mailing list or other external contacts.

Even though you all need to be in touch, it is still important to work together to protect everyone’s privacy and ensure people’s details are not used in ways they wouldn’t reasonably expect. It is useful to make a clear agreement among your committee about how you will look after one another’s contact details.

### **This could include:**

- That you will not pass them onto other people without specific consent
- That you will not use them for anything other than group business without specific consent
- That if someone leaves the committee everyone will delete their details, and vice versa, unless specific consent is given to keep them
- That you will not put other people’s contact details on group publicity without specific consent.

If your committee members do not wish to share their personal contact details with each other, you could consider setting up another way for everyone to communicate. One way of doing this is to allocate each committee member with an official email address (e.g. lpyca@gmail.com). One person should still hold everyone’s personal contact details securely though, because your committee are legally responsible for your organisation so need to be contactable.

## Sharing personal data with others

You should request explicit consent if you wish to share personal data with third-parties, (unless you need to do so to fulfil a contract, comply with the law, protect someone’s life or fulfil a public task).

Third-parties might be other organisations, but they might also be members of your own group. Each individual in a group is separate from the group itself, and data should not be shared with group members to use in a personal capacity without explicit consent.

Community groups should take care not to accidentally share personal data, including with other members of the group. For example, if you send an email to everyone on your mailing list, do not simply type all the email addresses into the “To” field. By doing this you are actually sharing all the email addresses with everyone on the list. Use the “Bcc” field instead. This hides everyone’s email addresses.

This is especially important if your group members all share a particular personal characteristic (e.g. a group for people who are LGBT, or a group for survivors of domestic abuse). Accidentally sharing the names or contact details of your group members could mean revealing that they have a particular personal characteristic, which they may not wish to be public knowledge and which could affect their lives in significant ways.

## **Removing personal data**

Once you have finished using personal data for the purpose it was collected for, it should be deleted. It should not be kept indefinitely just in case you want to use it again but don’t know what for. When you delete data, make sure it cannot be accessed by someone else.

***For example,** a community group organises an outing to a theme park for local children. They collect information about the children’s health conditions and allergies, so that they can take care of them on the trip. Once the trip is over they no longer need this information so there is no need to keep hold of it. Data that was held electronically is permanently deleted from the computer. Paperwork with health information on it is shredded.*

You should also delete people’s data when they ask you to, unless you need to keep it because of a specific legal obligation. If you send out emails to a list of contacts, you must put information at the end of *every email* explaining how to unsubscribe from the list. If you use an email newsletter provider this will happen automatically. If you send ordinary emails to a list of people, create an email signature which tells people who they should contact to be removed from the list.

## **People’s right to their own data**

Individuals have a right to be given a copy of their data, and information about how it is being used. This must be provided within one month of a request. They also have



a right to have their information amended or deleted within one month of a request (unless you need to keep it for legal reasons). To help you do this, make sure you know where data is being stored, and by who.

## **If you have not protected someone's data properly**

There are lots of ways that a community group might have a "data breach". These include, for example:

- Theft of a laptop or phone with contact details stored in it
- Accidentally sending an email with everyone's email addresses visible
- Sending personal information to the wrong recipient by mistake
- Losing a paper sign-up sheet on which people have written their names and addresses

The most important thing is to recognise if something has gone wrong, so that you can take steps to reduce the impact it will have, and to avoid it in future. Try to keep data protection in mind, so that you notice if there has been a possible data breach.

If you have a data breach, the first thing to do is try to get the data back. For example, if you have accidentally emailed someone's details to the wrong person, contact that person and ask them to delete the information.

The next step depends on whether the data breach is likely to have a significant impact on someone's life. If it is not likely to have an impact, you should still record that it has happened and take steps to avoid it happening again.

***For example,** a group organising a weekly sewing meet-up keeps a list of email addresses of people who attend regularly. A group organiser stores the list on her mobile phone. Her young child is playing with her phone, and accidentally sends a meaningless email to one of the contacts. This is not likely to risk anybody's freedoms or rights, and therefore does not need to be reported to anybody. Instead, the group records what happened in the minutes of the meeting at which it was discussed, and puts in place a system to avoid it in future (by storing the list in a more secure place).*

- Some data breaches are more serious though, and need to be reported to the person whose data is affected and to the Information Commissioner's Office (ICO).

***For example,** an organisation running a support group for people recovering from drug addiction has a paper sign-up sheet on which people write their names when they*

*arrive at a session. The list clearly states the name and topic of the group, so it is clear to anyone reading it that the people named are in recovery from drug addiction. The list is then accidentally left on a public bus. This could potentially affect the individuals involved in significant ways, and should be reported to them so that they can take steps to protect themselves if they want to (e.g. by changing their phone number). It should also be reported to the ICO.*

Remember that it is much better for the ICO to hear about your data breach from you than from someone else. This will show them that you are a responsible organisation that takes data protection seriously, which makes it less likely they will have significant concerns about you or issue a penalty fine. Remember that large fines are not intended for small groups, but that data protection is for everyone.

## **Privacy notices: telling people about the data you are using**

When your group collects personal data, or uses someone's data to contact them, it should be made clear to them why you have their data, what you are using it for, and what their rights are. This means you should provide them with a privacy notice.

**A privacy notice is a piece of written information which tells people why you need or have their data. It should include:**

- the name of your group;
- what the data will be used for;
- which legal basis you have for using the data;
- how long the data will be kept;
- whether the data will be shared with a third-party, including if it will be stored on a third-party website (e.g. in Google Drive or DropBox);
- that individuals can ask to have their data removed at any time, and contact details to use to do this.

If you are collecting and using data on the basis of explicit consent, you should provide a privacy notice when you request the consent.

**For example:**

**Leasowe Play Youth & Community Association** *needs your name and email address in order to send you information about group activities. Please tick the boxes below to give consent for us to use your details.*

- *I consent for **Leasowe Play Youth & Community Association** to send me details of their events and meetings.*
- *I consent for **Leasowe Play Youth & Community Association** to send me information about their campaigns.*
- *I consent for **Leasowe Play Youth & Community Association** to send me fundraising appeals.*

*Your details will be stored securely online in our Google Drive folder, and will be removed within one month if you end your membership of **Leasowe Play Youth & Community Association**. You can withdraw your consent for us to use your information, or ask us to amend or delete your details, by emailing [pw.townley@btintenet.com](mailto:pw.townley@btintenet.com)*

If you are using data without explicit consent (because you have a different lawful basis for using it, such as legitimate interest), you should provide a privacy notice either when you collect the data or, at the latest, the first time you contact someone.

**For example:**

*Leasowe Community Art Group has your contact details because you have attended one of our craft sessions in the last 12 months. We only use these details to send you information about our future craft sessions. We do this because it is in the legitimate interest of our group to publicise our sessions to regular attendees. Your details are stored securely by our committee, and will be deleted if you do not attend a session for 12 months. You can ask us to amend or delete your details at any time by contacting the Secretary on 0151 691 1595*

## **Legitimate interests**

Your group can use personal data if it is in your group's legitimate interests. This means that you can use data in ways that are necessary in order to run your group. You should only use the minimum amount of data that you need, and you should give people the option of having their data removed from your records.

***For example,** a neighbourhood action group needs to give local residents information about upcoming meetings, at which all residents' are entitled to attend and vote. When a new resident moves into the street, it is in the legitimate interests of the association to send them a letter with information about the association and its upcoming meetings. The letter should include contact details for the association, and clear information explaining that the resident can get in touch to ask to be removed from the*

*mailing list if they do not wish to receive further news from the neighbourhood action group.*

When you use people's data to pursue your group's legitimate interests, this must be balanced against their rights and freedoms. Here are some things to check before using people's data.

1) Before contacting somebody, consider whether they would reasonably expect you to be contacting them. For example, do you have their contact details because they are involved in your group's activities? If so, you can probably safely assume they would expect to be contacted by your group. In contrast, if you have their details because they have been passed on by a third-party, and the person has never had anything to do with you before, they might not expect to be contacted by your group.

2) Can you identify a particular purpose for using the data, which is clearly in your group's interests? If so, is use of the data necessary to achieve the purpose? For example, you might need to contact people who regularly attend your group's sessions in order to tell them about a change of venue, so that people can keep attending. This is clearly in the interest of your group, and you need to use contact details in order to achieve it.

## **Consent**

Your group can use personal data if you have explicit recorded consent. Consent is only valid for the particular purpose it was gained for (e.g. if you gain consent to use someone's address to send them a newsletter, it does not mean you have consent to use this information for other purposes). People must be well-informed in order to give consent. You must explain why you need the data and what you will use it for, and that the person can ask for it to be deleted in future.

***For example,** a campaign group runs a mailing list. When people sign up to the list, they give their consent to be sent campaigning information. They should be required to actively consent to receiving this information (by ticking a box or signing something). They should be able to withdraw their consent at any time, and every message the group sends to them should include information about how to do this. If the group wishes to use the contact details for an additional purpose, (e.g. pass them onto another campaign group), people should be asked for additional, separate consent for this (e.g. a separate tick box when they are signing up). It should be*

*made easy for people to consent to one purpose (e.g. receiving group campaigns) while withholding consent for a different purpose (e.g. having details shared with a third-party).*

To use consent as a basis for using data, you must keep a clear record of who has given you consent and for what. Consent must be positively given. You cannot assume consent just because somebody has not said anything. When using tick boxes, people must be required to actually tick a box to give consent. Pre-ticked boxes do not count.

You can get verbal consent, but you should still explain specifically what the data will be used for and that they can ask for it to be deleted in future. You still need to keep a written record so that you know who has given you consent, and for what.

***For example,*** *a member of the campaign group meets someone at an event, and they ask to be added to the mailing list. The group member must make sure they understand what kind of communication they will receive (e.g. email petitions) and the person must actively confirm they are happy with this. The group member should make a written record of the consent that has been given. Information about how to be removed from the list should be sent with every message.*

Consent for children aged under 13 must be given by a parent or guardian.

## **Lawful bases for collecting, storing and using personal data**

To be legal, your group should only collect, keep or use personal data if you are doing so to fulfil a purpose which fits into one of the following lawful bases:

- To serve your group's "legitimate interests", or
- Because you have explicit consent from the person whose data it is, or
- To fulfil a contract with the person whose data it is, or
- To meet a legal obligation, or
- To protect someone's life, or
- To perform a public task.

Any time you collect, store or use people's personal data, you should be clear which of these reasons you have for doing so. Here is more information about each of them.

# What is the General Data Protection Regulation (GDPR)?

There are rules set out in law which all organisations, including community groups, must follow in order to help protect people's data and privacy. **From 25th May 2018**, the previous legislation, the Data Protection Act, is replaced by a new piece of legislation: the General Data Protection Regulation (GDPR).

A lot of the GDPR is very similar to the Data Protection Act, but there are some changes. This page provides information your group needs to comply with GDPR. If you had not already thought about data protection, there will be lots that are new to you. If you were already on top of your data protection responsibilities you may still need to make some small changes to how you collect, store and use people's data.

You may have heard that the GDPR includes a substantial increase in the level of fine that can be enforced on organisations that are not compliant. It's important to remember that the maximum fine amounts are likely only to be used for very large multinational organisations. **Small community groups should not panic that they are going to be issued with a fine.** Instead, they should focus on developing a culture within their organisation of respecting and taking care of people's personal information, and not keeping information they do not need. This is the heart of data protection.