Data Protection template policy - Notes

We have developed a template Data Protection policy for use by our member groups. It has been designed as a starting point so that you can simply add your specific details (e.g. group name) in the relevant places, or use it as a structural guide for tailoring it more substantially.

To help you understand, use and adapt the policy we have provided some brief notes on key areas. We also recommend that you use read our general guidance *Data Protection: what are your responsibilities?*, before using the template policy.

Notes on using the policy

General: all parts in [square brackets] need to be adjusted to suit you group's needs.

Overview and Roles and Responsibilities Sections

Generally speaking we do not anticipate that groups will need to change much in this section. The main things to consider are:

- the lists of people you work with and that the policy applies to
- types of data you will be collecting

We do not recommend removing anything from these lists – even if they are not currently relevant to your group they will not do any harm being in the policy. But you might want to add extra examples particular to your group that are not included.

Data protection principles section

We fairly and lawfully process personal data & We only collect and use personal data for specified and lawful purposes.

You may need to make adjustments in these sections to reflect the specific activities of your group. The key thing is that you detail when you will collect data from individuals and how that data will be used.

A good rule of thumb is that it is OK to collect and use contact details for practical purposes in relation to the way you are working with an individual. Where you will be collecting and using information to generally promote your activities, specific consent is needed

- Collecting and using member's data for contact regarding membership and group activities is fine.
- If someone books a ticket it is OK to collect and use the data in relation to that booking (e.g. confirmation and reminder emails).
- It would not be OK to use that data to promote another concert three weeks later – unless they have expressly given consent for this.

We ensure data is not kept longer than necessary

We have set the 12 month limit as a reasonable and practical time limit for keeping data. It is hard to think of a reason to keep data on file longer then this (other than legal requirements) and is enough

time to ensure effective procedures can be in place for removing data. We do not recommend you increase this limit – but you could reduce it.

An example of a legal requirement for keeping records for longer than 12 months might be financial records (such as payments made to your MD) which should be kept for 6 years

Examples of us for 'legitimate purposes relating to our involvement with the individual' during the 12 month period might include keeping a members or volunteers data for reporting purposes or to contact them about their past membership/volunteer duties.

It is also worth considering what data you need to remove after the 12 months period. It would be acceptable to keep the name of a member as a record of membership – but probably not their address and contact details.

We process data in accordance with individuals' rights

The response times in brackets can be changed in this section. Best practice is to action any request as quickly as possible - but this has to weighed against the practical capabilities of voluntary groups. We think 14 days is reasonable – anything over 30 days would be too long.

In the last point in this section (relating to objections to storage and use) it states that the objection has to be considered only – not necessarily actioned. There would have to a clear and reasonable reason for refusing the objection. For example:

- A former member askes to have their details removed:
    - If they still have membership fees owing it would be fair to keep the details.
    - If they have paid all their fees and want no further involvement with the group it would be hard to justify keeping their details
- A current member asks that you stop contacting them by email
    - If email is your chosen method of communication it would be fair to say you need to contact them about key administrative issues – e.g. rehearsal schedules.
    - But it might be acceptable for them to request other types of use to stop – such as promoting an optional social event.

Transfer to countries outside the EEA

This includes online third-party services that may be hosted outside the EEA. This does not mean you cannot use them, it just means you have to be sure they have adequate data protection for individuals. For example:

Using MailChimp for emails or Google Docs for sharing documents (both housed in the USA) – would be OK – they are well-established reputable companies housed in a country with recognisable and thorough data protection laws.

If you are looking to use a less well known online company for these types of services, where their credibility is less clear and they are housed in a country with less well established data rights for individuals you should ask yourself if you can really guarantee the data is protected to the same level as is required under UK/EEA law.

Member-to-member contact

Membership bodies often facilitate members contacting each other. This part of the policy sets out that any requests for data form members will be dealt with as and when they arise – with permission being given on a case by case basis.

You could consider detailing a policy where members give prior consent (e.g. when they first join) for their details to be shared with other members. If you do this you must include the option for members to subsequently remove their prior consent.

Direct Marketing

This section sets out the key things you should be doing in relation to collecting and using email data for Direct Marketing.

We suggest you also read the ICO's best-practice guidance and The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) – especially if you are taking part in any other type of direct marketing (e.g. telephone).

Cookies on your website

Cookies might be used for tracking (e.g. Google Analytics or Wordpress) to monitor what pages users are looking at; to manage core functionality (e.g. to provide the ability for users to 'log in' to access parts of your website); or for other reasons.

If you collect data on your website in this way then this data also falls under data protection and direct marketing rules. The most common way to manage this is to have a clear cookie and privacy policy accessible on your website (which explains which cookie types you use and what they are used for) and to have a method for users to opt-out of their cookies being collected.

Many common website platforms (e.g. WordPress) will have modules available to take care of the latter of these for you. If you are working with a professional to build/maintain a website they should also be able to make suggestions on how to deal with this.

If you do not have cookies on your site you can remove this part form the policy.