youth SCOTLAND
The network of youth groups

Quick Guide to Data Protection and GDPR, May 2018

Data Protection and GDPR

Data Protection law will change on 25th May when the new General Data Protection Regulation (GDPR) is introduced. This will affect all organisations that collect, use and store people's information. In light of these changes, you may have to make changes to the way you use and store people's information in your youth group.

Here at Youth Scotland, we have updated our own procedures to accommodate new General Data Protection Regulation (GDPR) and our data protection policy and privacy policy explain how Youth Scotland uses, stores and protects any personal data it manages through the provision of its programmes and membership services.

We have created this Quick Guide to help you as small volunteer run member groups understand what you need to do to comply with the new legislation. This Quick Guide should be read alongside the information provide by Law at Work -Youth Scotland's legal service partners.

Law at Work (LAW): You can access an extensive suite of legal advice, guidance and templates as part of your Youth Scotland membership. Law at Work have updated their data protection offering for Youth Scotland members to include qualified legal advice and resources for the launch of GDPR. This includes documents and templates that you can use for your group. GDPR - Data Subject Rights Form

How to access this Youth Scotland member service

These services are for Youth Scotland Member Groups Only and you will be required to quote your Youth Scotland Membership number and details when accessing these services.

To register: If you have not previously registered for this membership service, go to this webpage and have your member group details and Youth Scotland membership number handy. Your Youth Scotland membership number will begin 350. LAW will also be using your primary membership contact email address.

To login: If you have previously registered for this membership service, go to this webpage and enter your details.

Changes under the GDPR

In general terms, the things you had to do under the Data Protection Act still apply but under GDPR, you also need to make sure you have additional things in place.

New data protection principles:

The GDPR contains six, rather than eight principles. These are that personal data should be:

- processed lawfully, fairly and transparently;
- only be used for specific purposes;
- be limited to what is necessary and relevant;
- accurate;
- retained for no longer than necessary;
- protected against unlawful use or loss.

This means that that you will have to review the systems you have in place and think about

- what information you have
- what you will use it for
- how long you need to keep information for
- how you will store information
- how you will destroy information that you don't need to keep.

You also need to make sure that you are keeping information safe and protecting your young people and volunteers' privacy.

Personal data is information about people that can be used to identify them. This might include:

- Name
- Address
- Date of Birth
- Email address
- Photograph
- **Sensitive personal data –** this is particularly sensitive information about things like a person's racial or ethnic origin, political opinions, religious or similar beliefs, physical or mental health, sexual orientation and their criminal record.

Keeping Information Safe – Top Tips

Keep your member information in a secure place (either hard copy in a locked filing cabinet or securely protected on a computer with passwords)

If transporting information, make sure that this is kept safe, e.g. on a device that is password protected

Make sure that you only keep personal information you really need and that it is up to date

Destroy personal information as soon as you have finished with it and don't need to have it any more – make sure you do this securely e.g. by using a shredder

Only share personal information when you have the person's consent to share this (except where there is a child protection concern)

Collecting information

As a youth group, you will probably collect information such as registration forms and consent forms, which may contain contact details and medical information.

Make sure that these forms only collect the information you really need to run the group/activities and keep the young people safe.

Make sure that you get consent to hold this data from the young person, and their parents where required. (Young people can usually give consent for their data at age 13 but for child protection reasons, you will usually require parental consent to participate in your activities for children up to 16 or 18 in some circumstances). You can add a box to your consent form for data protection, saying what you will use the information for, who you will share it with, how long you will keep it and how you will securely destroy it.

Photographs and video are also considered personal information, so make sure that you ask for permission to take photographs/films. Again you should be clear about how these will be used, where they will be stored, how long you will keep them and how you will securely destroy these. If you don't have permission, then you should not take photographs of that young person – if any are taken by mistake, you should destroy these immediately. If running a group activity, you can give young people a different coloured badge so that the person taking the photographs can identify who has permission or not.

Sharing Information

You should only share information when you have to, in the ways that you have told people you will, and for which you have permission. If you need to share data for any other reason, you need to get further consent to do so.

E.g. If you are organising an activity, you may have to share data to make the booking. If your youth group consent forms says that you will do this as part of your usual activities, then that is fine.

When you are sharing data, you must think about how to do this securely.

- If sending personal information by email, make sure that the document is password protected or encrypted.
- If giving personal information over the phone, use a private room so others can't hear you
- If sending personal information by post, use a tracked or signed for service

Within your group, you should also be clear about who will have access to what information. Think about the different roles people have and what information they will need to access.

In some situations, you can share information without consent e.g. in a medical emergency or for child protection and safeguarding reasons.

When producing publications or reports to share with funders and partners, please ensure that you have consent to use young people's names and photographs.

Using, keeping and destroying information

You need to make sure that the information you are using is accurate and up to date.

E.g. If you have consent forms with young people's personal information, you should get a new one every year to make sure that the information is up to date. You should also ask parents and young people to notify you as soon as possible if any information changes and update the information you are holding.

When you use personal data, you should only use this for the purpose for which you collected it. This will mainly be for running your group and enabling young people to participate in your activities and may include things like:

- Contacting parents/carers about meetings and activities
- Looking after young people and administering medication or emergency treatment

- Informing young people and parents/carers about activities, events, training courses
- Organising activities, outings and residentials
- Producing reports on the work you have done

All information should be stored securely e.g. in locked filing cabinet or on a computer protected by a password.

If someone has taken photographs, make sure that these have been saved securely and that the originals have been deleted from the original camera/ phone.

You should only keep information for as long as is required and you should tell people how long this will be.

You should securely destroy information when it is no longer required.

E.g. when a young person joins the group and completes a registration form and group consent form, you should say on the forms what you will use this information for, where it will be stored and how long you will keep it for. When the young people leaves the group, you should destroy their registration and consent forms – both hard copy and electronic.

Personal information should be destroyed securely e.g. by using a shredder or deleting files on a computer, making sure that files are actually deleted.

If there have been child protection incidents or accidents, you may need to keep some information beyond the usual timescales. Where relevant, and if there exists a conflict, Child Protection legislation and policy supersedes GDPR.

For further information, please visit www.youthscotland.org.uk/privacy