



BURY
VOLUNTARY,
COMMUNITY
& FAITH
ALLIANCE

Keeping Data Safe

Data Protection Toolkit for Small Organisations

This toolkit is designed for small charities and organisations and covers the 12 key steps to help keep personal data safe and secure

Introduction

At the heart of all our work is being "person-centered". This includes keeping people's data and personal information safe and secure

This toolkit is designed for small charities and voluntary organisations and covers the 12 key steps to work towards that will help keep people's data safe and secure.

We have tried to provide examples, good practice, templates, and straightforward advice to save you time and effort.

As you go through this workbook you might need to ask other people in your group or organisation for support. That's normal data protection isn't one person's job - its a bit like health and safety. Everyone has a role to play.

Just remember every organisation is different. If you are unsure or have a specific concern, do not hesitate to get in touch with us at Bury VCFA or seek legal advice



This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit the [Creative Commons website](https://creativecommons.org/licenses/by-nc-nd/4.0/) or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Background & Legislation

What information does Data Protection Legislation apply to?

Data Protection applies to 'personal data', Personal Data is any information relating to a person (called a 'data subject' in the legislation/guidance) who can be identified, directly or indirectly, This could be by obvious things such as their name or address but can also include things like identification numbers e.g. NHS Number or National Insurance Number. It can also include things specific to your physical, cultural or social identity such as your race or religion.

What is the law?

GDPR is probably the piece of legislation everyone has heard about. It stands for the General Data Protection Regulations and is an EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It was brought into UK law via the Data Protection Act 2018.

The legislation introduced in 2018 builds on rules we have had in place for a number of years but refreshes to reflect new technologies and ways we use data and information. Post-Brexit the legislation is still essentially in place.

There are other laws that impact data protection including PECR (Privacy and Electronic Communication Regulations) which covers things like electronic marketing as well as the Freedom of Information Act (although it doesn't often apply to VCSE organisations it is often used by the sector to get information from public sector bodies).

Ultimately don't panic - keeping data safe in practice is less about being a "legal eagle" and know the legislation. It's more about how your work on a daily basis, good policies and procedures and a dash of common sense!

Isn't this just for business and large organisations?

Data Protection is important to organisations, charities and groups of all shapes and sizes as most of us handle personal data. For example, if you have a membership, send a newsletter to your users, fundraise or have to provide data to a funder or commissioners then these are all examples of work that requires good information governance and are affected by data protection regulations.

What Data Do You Hold?

It's very hard to know how to keep data safe unless you know what you hold.

Why do you hold it, where do you store it and whom do you share it with?

Producing a record of what information you hold is a great start to identifying where you may need to make changes or improvements.

Yes

No

Not Sure

There is no set format for how to do create a record but generally, they must show what information you hold, the purpose (why), your condition for processing (the lawful basis for using it) and with whom you share the information with. As well as how long you keep it and how you dispose of it.

- The ICO provides [guidance and templates](#) on how to document your activities.
- The National Archives also have [their own template](#)
- The CIO has also created [a tool to help you identify your lawful basis/condition for processing](#).

Do people know you have their personal data?

Do people know you have their personal data and understand how you use it?

This can be in paper format such as through leaflets, posters or as part of membership forms or it can be online through something called a privacy notice or statement.

Yes

No

Not Sure

A privacy notice or statement should include:

- Name your group or organisation and the person responsible for data protection.
- Why do you hold the personal data and what do you do with it?
- Where you got the data from (e.g. from the individuals when they joined)?
- If you share the data with anyone and how you do this?
- How long do you keep the data for?
- How people can request access to, or correction or deletion of, their data?
- How to complain to the Information Commissioners Office?
- Whether you make any automated decisions or do profiling based on the data you hold?

- [ICO Privacy Notice Template](#)
- [Privacy.Org Notice Generator](#) (this isn't based on UK legislation so it will need revising but it provides a good starting point)
- [Scouts Privacy Notice Guidance](#)

PS Do not forget your website too – It is important that people know about any cookies or site uses. Most sites are built with cookie notices and pop-ups but it is worth checking with your provider.

Do you only collect the information that you need?

Do you only collect the information you need to work with and use?

Do people know the difference between information they need to provide and information that is optional?

Yes

No

Not Sure

For example - Crinklebottom Bowls Club collect the name, address and contact telephone, age and gender of their members in order to run the club and arrange the bowls club teams.

They would also like to collect demographic information such as ethnicity to support their application to a local grants programme.

As this is not necessary for them to run the club, members have the option not to say or complete this part of the membership form



When starting a new project or programme always think about what data you need as part of your planning.

You may need data to run the service but also to help you show the impact you are making as well as to report to funders or commissioners

How long do you keep data for?

Have you decided and documented how long you will hold the personal data you collect? Do you refresh or destroy personal data after specified periods of time?

Yes

No

Not Sure

How long you keep data depends on its purpose. This might be based on a statutory requirement (e.g. finance, safeguarding etc.), contractual (e.g. how long the commissioner or funder want you to keep it) or your business case (how long you need it).

The key thing is justifying why you are keeping it and recording it. This document is your retention policy or record. It could be an appendix to your data protection policy rather than a completely separate document.

Check your contracts or funding agreements - some may say how long you have to keep things related to the funding or project for

The most common length of time to keep records for at least 6 years which covers the standard time limit for any civil legal action.

[The Chartered Institute of Professional Development](#) has a guide to the statutory retention time for things relating to staff and HR

Do you securely delete or destroy personal data as soon as you no longer need it?

Yes

No

Not Sure

How you delete data will depend on its format, but it is important that data is deleted or destroyed safely. But don't panic this doesn't have to be complicated or expensive.

For small amounts of paper records you can buy a cross cutting shredder from high street stationary or electronic stores. Although larger organisations may buy in specialist companies to destroy their documents as it's more time efficient.

For electronic records things can vary a little bit - you may initially just delete them but if you need to sell or recycle your devices there are some additional steps to take to make sure no data is left on it such as restoring to factory settings or taking it to a specialist.



ICO Guide - [Deleting your data from computers, laptops and other devices](#)

Do you keep personal data accurate and up to date?

Do you regularly check that the personal data you hold is accurate and up to date?

Yes

No

Not Sure

For example - Kevin is the manager of a local football team. Every month he emails the team about upcoming matches. Kevin should regularly check with the team members that the email addresses are still accurate. Can you update you information quickly if asked by an individual?

Easy steps to keep information up to date are from things like annual membership forms or when people sign up to activities.

For most groups updating information will be about common sense as you will know the people you are working with.

But, if you are unsure of the identity of the person you can ask for more information to help make sure you update the right records. e.g. asking for a Date of Birth if you have two Bob Smiths.



Top Tip - Don't forget mailing lists - mailing list software can allow people to update their own records and some can link to your databases. But many groups have a manual list - these needs to be kept up to date too.

Do you keep personal data secure?

Yes

No

Not Sure

How you keep data secure will depend on the format it's held - digital or hard copy. But for example -

Do you keep personal data secure in the office? e.g. using lockable filing cabinets and locking or logging off computers when away from your desk?

Do you take steps to keep personal data secure before you take it out and about or send it somewhere else? e.g. do you only take with you the data you need or send it in advance by secure methods?

Do you keep paper documents secure, say by using lockable storage and disposing of paper records securely?

Do you keep electronic data secure, say by encrypting mobile devices, using passwords and backing up the data?

National Cyber Security Centre (NCSC) - [Guide for Small Charities](#)

NCSC - [Free Cyber Security Training for Charities and Small Organisations](#)

NCSC Cyber Aware - [Cyber Action Plan for Small Organisations](#)

Action Fraud - [Reporting Online Fraud or a Cyber Attack](#)

[Cyber Essentials](#) - A Government backed certification scheme to help you demonstrate good practice for cyber security.

Do you have a way for people to exercise their rights regarding the personal data you hold about them?

Yes

No

Not Sure

Individuals have a range of rights regarding how their personal data is used. Including -

- The right to request a copy of their data you hold.
- The right to have inaccurate data corrected.
- The right to ask you to delete / destroy their data.
- The right to limit the amount or type of data used.
- The right to request you stop using their data.

A request could be made over the phone, in an email, or face to face. It does not have to be made formally in writing by letter. If you can, treat requests that are easily dealt with as routine matters, in the normal course of business. For example:

- Simon, a local rugby-team manager, receives a call from a player asking for details of all the matches he has played in the last year. This can be dealt with as business as usual.
- Peter (the group secretary) is asked by a member if her membership is up to date and paid. This can be dealt with as business as usual

You would probably want to treat the following requests in a more formal way:

- One of Susan's ex-volunteers requests a copy of the reference she gave about him to a prospective new employer.
- Jake manages a youth group and receives a request from one of the children's parents for a copy of the information held on their child.

The ICO [Subject Access Rights Checklist](#)

ICO [Right of Access Guidance](#)

Do your volunteers & staff know their data protection responsibilities?

Yes

No

Not Sure

For key staff or volunteers this may be formal training depending on their role. Think about how data protection is covered in inductions and if everyone is aware of your policies. Ensure any training given is recorded either through personnel files or minutes of team meetings, 1:1 etc

The NHS E-Learning Platforms for volunteers may be suitable if your organisation delivers health and wellbeing services - [visit their website for more information.](#)

The [National Centre for Cyber Security](#) provide free online training for staff and volunteers within charities and small organisation.

The [ICO](#) have also shared their internal staff training resources to support your own training programmes.



Is data protection discussed at a committee level?

Information Governance and Data Protection is a compliance issues in the same way as finance or health and safety. Policies, incidents and risks should all be discussed and minuted at this level as part of good governance and help you demonstrate the processes you've done.

Yes

No

Not Sure

Do you know if you are obliged to pay a data protection fee?

Under the Data Protection legislation individuals and organisations that process personal data need to pay a data protection fee to the Information Commissioner's Office (ICO), unless they are exempt. The exemption for charities and VCSE organisations is quite narrow and focus around managing your membership and the direct delivery for your members or those you have regular contact with. Once you start employing staff, trading (including hiring rooms etc) or taking part in significant organised fundraising. administering activities for either the members or those who have regular contact with it.

The [ICO Current Registration Self-Assessment Tool](#) is a free 5 minute online tool to assess if you need to register)

Do you have a data protection policy?

Does it link to other policies and procedures in your organisation?

Yes

No

Not Sure

The Data Protection Policy is an internal statement of how your organisation protects the personal data it processes and almost all charities and organisations should have one. However, it does not sit alone and it may link to a number of within your organisation including IT usage, volunteers recruitment etc. so you may need to refresh these to include elements of data protection.

NCVO Guidance - [Writing Data Protection Policies and Procedures](#)

White Fuse - [Data Protection Policy Template](#)

Northern Ireland Council for Voluntary Action - [Templates and Guidance](#)





BURY
VOLUNTARY,
COMMUNITY
& FAITH
ALLIANCE

Contact us to find out more:

0161 518 5550

buryvcfa.org.uk

admin@buryvcfa.org.uk

Registered Charity No. 1182039



This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit the [Creative Commons website](https://creativecommons.org/licenses/by-nc-nd/4.0/) or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.