This toolkit is designed for small charities and organisations and covers the 12 key steps to work towards Data Protection Compliance.

We have tried to provide examples, good practise, templates, and straightforward advice to save you time and effort. Nevertheless, it is important to note that although we have a lot of training and experience in Data Protection every organisation is different.

If you are unsure or have a specific concern, do not hesitate to get in touch with your nearest support organisations (see www.10gm.org.uk for your nearest one) or seek legal advice.

General Resources & Information

- ICO Guidelines for Data Protection - https://ico.org.uk/for-organisations/guide-to-data-protection/
- ICO General Data Protection Regulation (GDPR) FAQs for charities - https://ico.org.uk/for-organisations/in-your-sector/charity/charities-faqs/
- ICO Helpline (for small organisations under 250 staff) - 0303 123 1113 and select option 4 to be diverted to staff who can offer support

Cyber Security

- Cyber Aware (support resources) - https://www.cyberaware.gov.uk/
- National Cyber Security Centre Small Charities Guide - https://www.ncsc.gov.uk/charity
- Get Safe Online – General Advice and Support re Cyber Security - https://www.getsafeonline.org/

Specific Information

- Fundraising and data protection: a survival guide for the uninitiated - http://2040training.co.uk/wp-content/uploads/2017/03/Fundraising-DP-guide.pdf
- Parish Resources (Faith Based Perspective) - http://www.parishresources.org.uk/gdpr/
- Scouting Organisations - https://members.scouts.org.uk/supportresources/search/?cat=55,888
- Children and GDPR (ICO Consultation Document) - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/

1.	Do you know exactly what information you hold, why you hold it, where you store it and whom you share it with? Producing a record of what information you hold is a great start to identify where you may need to make changes or improvements. For some organisations it is also a requirement under data protection legislation.	Yes / No / Not Sure	**Record of Processing Activity / Data Audit** There is no set format for these but you must show what information you hold, the purpose (why), you condition for processing and who you share the information with as well as how long you keep it and how you dispose of it. **ICO Guidance** The ICO provide guidance and templates on how to document your activities - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/ **National Archives – Template** http://www.nationalarchives.gov.uk/documents/information-management/iar_template.xls **ICO Lawful Basis Guidance Tool** - https://ico.org.uk/for-organisations/resources- and-support/getting-ready-for-the-gdpr-resources/lawful-basis-interactive-guidance-tool/

2.	Do people know you have their personal data and understand how you use it?	Yes / No / Not Sure	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. A privacy notice or statement should include: • The name of your group or organisation and the person responsible for data protection. • Why you hold the personal data and what 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 you keep the data for. • How people can request access to, or correction or deletion of, their data. • How to complain to the ICO. • Whether you make any automated decisions or do profiling based on the data you hold. Examples and tools to help you – • **ICO Privacy Notice Template** https://ico.org.uk/media/for-organisations/documents/2259798/pn-template-microbusiness-201908.docx • **Privacy.Org Notice Generator** https://www.privacy.org.nz/further-resources/privacy-statement-generator/ (this isn't based on UK legislation so it will need reviewing to make sure it contains all the bullet points above but it provides a good start if you have nothing in place yet)

			• **Scouts Privacy Notice Guidance** https://members.scouts.org.uk/documents/GDPR/Sept18/GDPR%20Guidance%20for%20local%20Scouting%20on%20the%20creation%20of%20a%20privacy%20notice-web.doc • **White Fuse – Privacy Notice Template for Small Charities** https://whitefuse.com/sites/default/files/files/Privacy%20Policy%20template.docx 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. **White Fuse –Cookie Consent -** https://whitefuse.com/blog/law-cookie-notices-and-cookie-consent
3.	Do you only collect the personal data or 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? 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.

4.	Do you only keep personal data for as long as it is needed?		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? 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. **Shred-it Guide to Data Retention** https://www.shredit.co.uk/getmedia/79634da2-8885-461f-9c6e-195c617a0562/Doc_Retention_Guide_UK_E.aspx?ext=.pdf **Missionbox Document Retention Overview for UK Charities** https://www.missionbox.com/article/453/document-retention-an-overview-for-uk-charities
5	Do you securely delete or destroy personal data as soon as you no longer need it?		How you delete data will depend on what format it is in but it is important that data is deleted or destroyed safely. **ICO Information -** https://ico.org.uk/your-data-matters/online/deleting-your-data-from-computers-laptops-and-other-devices/ **NHS England Bite Sized Guide to Media Disposal -** https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ Bite-sized%20GPG_Media%20Disposal.doc

6	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? 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 information quickly if asked by an individual?
7	Do you keep personal data secure?		• Do you keep personal data secure in the office, for example by 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? For example, 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? Also see the cyber security resources at the start of this guide

8	Do you have a way for people to exercise their rights regarding the personal data you hold about them?		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 newsagent) is asked by a customer in the shop for the balance of her account. 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. **ICO SARs Checklist** https://ico.org.uk/for-organisations/business/sar-checklist-for-smes/ **ICO Right of Access Guidance** https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
9	Do your volunteers & staff (if you have any) know your data protection responsibilities?		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 **National Cyber Security Centre – Top Tips for Staff Free E-learning** https://www.ncsc.gov.uk/static-assets/training/top-tips-for-staff-web/story_html5.html

10	Is information governance / data protection discussed at a committee level?	Yes / No / Not Sure	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.
11	Do you know if you are obliged to pay a data protection fee?	Yes / No / Not Sure	**ICO Current Registration Self-Assessment Tool** (a free 5 minute online tool to assess if you need to register) https://ico.org.uk/for-organisations/register/self-assessment/
12	Do you have a data protection / information governance 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. Some useful templates and examples • http://community.lincolnshire.gov.uk/Files/Community/436/DataProtectionpolicytemplate.doc • http://www.slough.communitydatabase.co.uk/haymill/data/files/SLOUGHP007-Example%20Data%20Protection%20Policy.pdf • https://whitefuse.com/sites/default/files/files/Data%20Protection%20Policy%20template.docx