

# How Should We Store Our Data?

**a guide for small and new UK charities  
to help you store your data securely  
and use it effectively**



## Summary

If you've followed parts one and two of our data guide, you should now have a good sense of the data you have, or need, and be confident that you can process it lawfully. The next question is whether the way you are storing that data is good enough.

What 'good enough' means will depend. The Data Protection Act 2018 (DPA) places some requirements on you to ensure data is secured appropriately. You also need to think about the types of data you have, and what you need to do with them. The appropriate technology will need to be secure *and* make your data work for you.

For example, if you have supporter data you may want to send regular email or postal updates and appeals, and be able to accept online donations. You may need to report on the performance of these appeals. This is all very different to what you may need to do with volunteer data, which may in turn be different to service user data.

This guide, part three in the series, gives an overview of the requirements of the DPA, and links to some useful advice. We also offer some suggestions of the types of system that may be suitable for a small charity, and some of the pros and cons of each.

The [Information Commissioner's Office \(ICO\)](#) is the official source for guidance, and they have a lot that's detailed and helpful. The [National Cyber Security Centre](#) has a lot of great advice and resources to help you keep your data secure. We'll link to resources through this guide.

© 2023 Lamplight Database Systems Limited

[www.lamplightdb.co.uk](http://www.lamplightdb.co.uk)



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Summary .....	2
Legal Requirements .....	4
Risk Assessment.....	4
Using External Processors .....	6
It's Not Just You .....	7
What Do You Need to Do with It? .....	7
How to Store Your Data .....	7
Membership List .....	8
Fundraising .....	10
Case/Client/Outcome/Service Management .....	11
Other Pointers .....	13
About Us.....	13

## Legal Requirements

*A key principle of the UK GDPR is that you process personal data securely by means of ‘appropriate technical and organisational measures’—this is the ‘security principle’.*

[Source: [ICO](#)]

This means that you need to think about *what you do*, as well as *where you store* your data. It’s no good having a massive lock on the door to your office if people wedge the door open all the time. It’s no good having military grade security systems if your password is your pet’s name. You need secure systems, and you need secure practices.

There is [more detailed guidance](#) from the ICO about how to meet the requirements of the security principle. This guidance covers everyone, from the smallest to the very largest organisations, so it can get quite deep.

## Risk Assessment

To do this properly, you should carry out a risk assessment. This means looking at each of your ‘information assets’ and thinking about how bad it would be if you lost them. Information assets can be all sorts of things; in the context of this guide, each table you completed in part one is probably an asset (‘data about trustees’, ‘data about supporters’, etc.). This should be relatively straightforward.

The loss of trustee contact details is probably pretty trivial, because they are so few and are already in the public domain on the Charity Commission website. Losing the details of all your donors might be very significant, if it meant a loss of income and reputation. A breach of the security of sensitive personal information about your service users could be very serious indeed.

‘Loss’ could mean various things. You may lose access permanently or just temporarily. The data may be corrupted (donor names and donations become disconnected, for example, so you don’t know who has given what). Other

scenarios involve unauthorised people gaining access to it—an email copied to the wrong person, or the theft of a laptop, for example.

You'd also need to assess the likelihood of loss. This is harder to put down in concrete terms. What is the chance of your computer erasing all your data? Or of being hacked? Or someone stealing the physical devices on which your data is stored? Small organisations might reasonably take the view that any of these are quite likely—these things do happen all the time. In other words, focus on the impact of loss, rather than the likelihood.

Carrying out a full risk assessment is well beyond the scope of this guide: it's a profession in it's own right. If you are a small charity holding a relatively small amount of data that has a low risk of harm if compromised, it's unlikely to be necessary for you to do a full risk assessment. In this case, you may feel that a simple assessment, and implementing some standard good practice controls, is appropriate.

Fortunately, there are some standard practices you can adopt to reduce the likelihood and/or impact of these threats, and the [Cyber Aware advice](#) from The National Cyber Security Centre (NCSC) is a great place to start:

**Action 1:** Create a strong, unique password for your email using three random words.

**Action 2:** Turn on Two-Step Verification (2SV) for your email.

**Action 3:** Save passwords in your browser.

**Action 4:** Back up your data.

**Action 5:** Update your devices.

These actions are fairly quick and easy to do, and the [guides from NCSC](#) will help you. NCSC also has [guidance specifically for charities](#), which covers most of the above, plus a little more.

If you want to take things further, you may want to look at [Cyber Essentials](#). This gives five categories of technical controls you should put in place to protect your network and devices. It is more technical and involved, but is still intended to be accessible for all organisations. NCSC currently [offers funded support](#) to charities wishing to do Cyber Essentials. How far you take this really

depends on the first step of your risk assessment: how bad would it be if we lost this?



To carry out a simple assessment, use Part One of the accompanying workbook. For each type of data, think about what the effect on your organisation would be if the data was lost. You should also think about the impact on the data subject. Then think about what you currently do to protect it, and whether there's anything more you should do to protect the data or reduce the impact of loss.

This assessment and action plan should be considered by your Trustees and be reviewed every year or two.

## Using External Processors

If you use a third party to process your data (and there's a good chance you will—even an Excel spreadsheet is part of an online service from Microsoft nowadays) you will need to ensure that the contract with that organisation is compliant with the [requirements of GDPR](#).

Most providers will have contracts that meet these requirements, but you can't assume that—you'll still need to check.



The ICO checklist is included in Part Three of the workbook accompanying this guide so that you can document compliance for any services you use.

## It's Not Just You

This needs to be an organisation-wide effort. It's no good your using two-step verification for everything if your colleague is still using 'password123' as their password to everything. Some training for trustees, staff members, and volunteers (anyone with access to any of your data) will need to be carried out.

You can pay (a lot, potentially) for this training, but NCSC provides [free introductory training](#) online. That's a great place to start.

## What Do You Need to Do with It?

There's no point having all this data if you can't use it as you need to.

For each category of data, we suggest that you write down (at a fairly high level) what your organisation needs to do with the data. Some examples:

- communicate (emails, SMS, etc.)
- see the full picture (bring all data about a person together in one place)
- manage GDPR consent
- produce numerical reports for managers/trustees
- produce numerical reports for funders/other external bodies



You may have noted some of this already in the earlier workbooks. If so, you may find it useful to bring it all together now. In the workbook, note down these requirements for each type of data you have. You may also want to check you've covered everything with your colleagues.

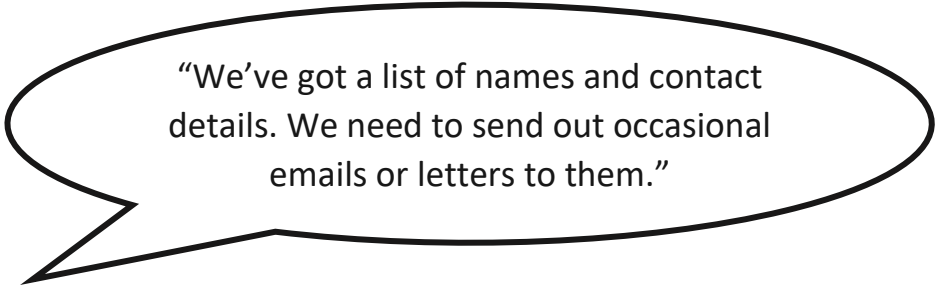
## How to Store Your Data

The following sections have some of our suggestions of different approaches for different types of data. We've only listed a handful of some of the well-

known suppliers—and only ones that provide pricing information transparently on their website. There are plenty of other providers out there though, these are illustrations, not recommendations.

Data Orchard is a non-profit helping other charities with their data. It is independent of any one supplier and has a list of CRM suppliers [on its website](#).

## Membership List



“We’ve got a list of names and contact details. We need to send out occasional emails or letters to them.”

Options you could consider:

### SPREADSHEETS (E.G. EXCEL)

#### Advantages

- + easy to set up and use
- + widely available
- + cheap
- + lots of people know how to use them

#### Disadvantages

- hard to manage long lists
- anyone can change the structure
- mail-merges can be a bit tricky
- it’s hard to track multiple records for a single person



## EMAILER SOFTWARE (E.G. MAILCHIMP)

### Advantages

- + good design and reporting functions
- + free/cheap for small numbers of contacts
- + fairly easy to use
- + good community resources

### Disadvantages

- can't store a lot of additional information
- functionality fairly limited to emailing
- likely to need to link it to other software

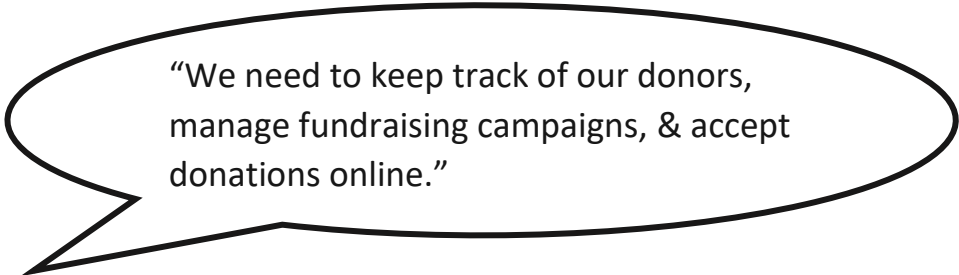
## SPECIALISED MEMBERSHIP SOFTWARE

### Advantages

- + you can store more detailed information about contacts
- + can manage membership and renewals
- + it may allow members to log in and access their details

### Disadvantages

- will get more expensive
- will need initial set-up effort



“We need to keep track of our donors, manage fundraising campaigns, & accept donations online.”

Options you could consider:

### SPECIALIST SYSTEM (E.G. DONORFY)

#### Advantages

- + focus on fundraising
- + connects to payment processing
- + manage campaigns on social media

#### Disadvantages

- can get expensive
- you'll have to learn it and document what you do

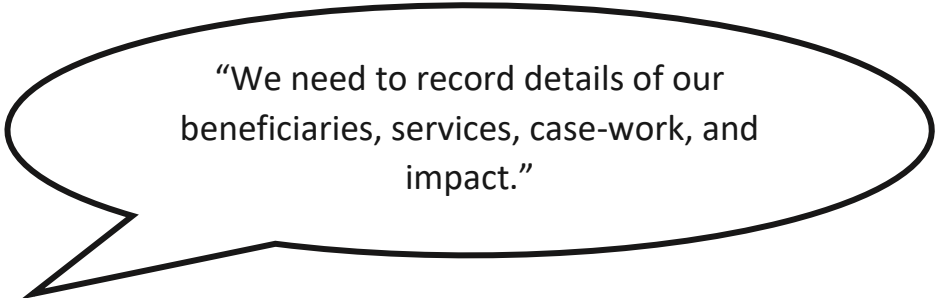
### BUILD YOUR OWN ACCESS DATABASE

#### Advantages

- + can be built just for you
- + may be cheaper (especially if a volunteer can help)

#### Disadvantages

- harder to link to e.g. payment processing or online campaigns
- you have to support and maintain it yourself
- if you rely on one person who made it, what happens if they leave?



“We need to record details of our beneficiaries, services, case-work, and impact.”

Options you could consider:

### SPREADSHEET (E.G. EXCEL)

#### **Advantages**

- + quick and easy to set up and use
- + cheap and widely available
- + easy to adapt
- + everyone knows how to use it

#### **Disadvantages**

- hard to store and view multiple records for one person
- reporting likely to be difficult
- can end up with data spread out in lots of spreadsheets

## OFF-THE-SHELF CHARITY CRM SYSTEM (E.G. LAMPLIGHT, INFORM)

### Advantages

- + software designed for specific needs of voluntary sector & suppliers know it.
- + pricing generally reasonable
- + reports and functionality based on what you and funders need

### Disadvantages

- may not do everything you need
- won't be completely customisable
- will need to learn new system

## RE-PURPOSED COMMERCIAL CRM SYSTEM (E.G. MICROSOFT DYNAMICS, SALESFORCE)

### Advantages

- + can get access to powerful software
- + may get reduced license costs for charities

### Disadvantages

- tends to be focused on sales, so may not do charity things like outcomes, very easily or well
- probably need to find someone to help setup which can be more expensive
- per-user licensing and add-ons can add up even when initial deal seems good

## Other Pointers

Whatever you do, you'll need to make sure you've covered these things:

- Security: will your data be safe? Who does backups, updates, etc.?
- Who owns your data? Can you change systems later if you need to?
- Can you get support and training? How much will it cost?
- What happens when things change? When a new project starts in two years' time? Can you update your system, build your own reports, that sort of thing?
- One system or many? Should your fundraising and case management data all be in one system? There may be some benefits to doing so, but not necessarily. What do you gain by doing so?

## About Us

Lamplight is one of the 'Off-the-Shelf Charity CRM Systems'. If that's the sort of thing you need, we'd love to hear more about what you do and see whether Lamplight might be able to help. We've been helping non-profits of all sorts and sizes with their data since 2004. Find out more at [www.lamplightdb.co.uk](http://www.lamplightdb.co.uk) or connect with us [@lamplightdb](https://www.instagram.com/lamplightdb) or on [LinkedIn](https://www.linkedin.com/company/lamplightdb).

If you've found these guides helpful, we'd love to hear about it. If you've any suggestions of how we could improve them, we'd love to hear that too.