AN INTRODUCTION TO KEEPING PERSONAL DATA SAFE

Charities hold lots of personal data about their supporters, staff and beneficiaries. Protecting it from accidental, negligent or malicious loss and theft should always be a high priority.

HELPSHEET

Introduction

Personal data and how it's used is a hot topic in both personal and professional settings. As a charity you are accountable to your supporters, fundraisers, volunteers, beneficiaries and staff for the way you handle their data – and they will want to know that it is being looked after responsibly.

The safeguards your charity needs to put in place will depend on the type of information and the risks to the data subject should it be lost or exposed. This can be a real challenge, especially for small charities with limited funds who support vulnerable individuals and need to hold sensitive data in order to do so.

WHY IS IT IMPORTANT?

Keeping data safe – and using it only in ways that are expected by individuals – is vital to ensure that your organisation doesn't fall foul of the law, leading to fines and reputational damage. But more importantly, charities have a duty to their beneficiaries to look after their best interests, and that includes looking after their information and only using it in ways that they would expect.

What is personal data?

Personal data is any information relating to an individual which can be used (directly or indirectly) to identify the individual. This includes (but is not limited to) a person's name, phone number, personal email address, job title, twitter handle, age, gender, bank account number and partner's name.

There are also special categories of personal data which are likely to be of a private nature and could be used in a discriminatory way. This includes (but is not limited to) a person's medical history, political preferences, ethnic background, religion, sexual orientation, and affiliation with any trade union.

Common risks

Personal data can be compromised in a wide variety of ways.

- External parties may try to take it from you, or make it inaccessible to you, for financial gain. This could be through a technical attack or by simply calling your office and asking for it.
- Internal parties lose data either accidentally, negligently or maliciously.
- A system, human or process failure leads to data being made accessible to people who should not see it.
- Data is updated or overridden incorrectly.
- System outages or corruption of data leads to it no longer being available. This is especially concerning if you are supporting vulnerable individuals.

Basic controls

These safeguards should always be in place.

- Ensure that all personal data is collected, stored and disposed of securely.
- Personal data is only kept for as long as necessary.
- Personal data is made accessible only to members of the charity who need to have access to it.
- Anyone who has access to personal data understands that it is their responsibility to keep it secure.
- Anyone who has access to personal data has been subject to appropriate checks.

CHARITY FRAUD AWARE

IN MORE DETAIL ...

Restrict access to personal data stored on paper
Store paper in a place that restricts access. In practice, this can mean something simple like a drawer with a lock on it. By leaving personal data unattended and available to others (eg, in your car, on a coffee table at home or in a meeting room) you increase the risk of it being taken or going missing.

Never leave personal data unaccompanied at an event
At events, ensure there is always a manned sign-in process. If your charity is collecting forms that contain personal details, the individuals themselves should hand the forms to a volunteer or staff member or post them into a secure box (that is locked with a key).

Keep sensitive information separate (where possible) to limit exposure
For example, at the end of an event count the forms collected and record the details separately to the forms themselves. If the information goes missing this allows you to assess the situation and agree remediation quickly and easily.

Follow good data protection and cyber security practices
This will reduce the risks to personal data stored electronically and on paper. In the UK follow the guidance issued by the National Cyber Security Centre (NCSC) and the Information Commissioner's Office (ICO).

Taking action

If you suspect a data breach act promptly. Knowing what you will do if something goes wrong can reduce the risks to data subjects and will also help your organisation to feel in control.

- Think through what you would do in the event of a breach and write it down – in the heat of the moment it's easy to make mistakes, forget key steps, or find that everyone is trying to do the same things at once.
- Focus on identifying what has caused the breach and containing any data leak. Isolate systems affected and call in experts to help if necessary.
- Remember the ICO reporting requirements. Call them and discuss what is going on. They will advise if you need to report and how much information they need.
- Consider what you will say to the affected parties. Never try to minimise a breach.

CHECKLIST

BUILDING YOUR CHARITY'S DEFENCES

ASK YOURSELF:

- ☐ Have we identified all of the personal data we hold and where it is located?
- ☐ Who has access to our information? Pay special attention to individuals who have privileged access to data and systems and make sure there is a strong process for leavers and movers.
- ☐ Have we thought about the ways in which the personal data we hold might be compromised, and what could we put in place to limit this happening?
- ☐ Do we have a policy or other set of rules that explains what our staff (and volunteers) can and cannot do with personal data?
- ☐ Do we have a dedicated reporting line that all staff and volunteers are aware of?
- ☐ Do we have data sharing agreements in place with any individuals or organisations that we share personal data with?
- ☐ What training and support do we provide for our staff, and how often do we refresh this?
- ☐ Do we have a plan for making improvements?
- ☐ Do we know what we will do if something goes wrong?

OTHER RESOURCES

The UK's Information Commissioner's Office has produced guidance for small and medium-sized organisations and charities. See **'Data protection self-assessment on information security'** and **'Top five tips'** for small and medium-sized charities.

The UK's National Cyber Security Centre has produced guidance for charities on how to improve cyber security quickly, easily and at low cost. See **'Cyber security: small charity guide'**.

Charity Fraud Awareness Week 2019. **'An introduction to cyber security'** (helpsheet).

ACKNOWLEDGEMENT

This helpsheet was kindly prepared by Cancer Research UK.