Introduction to Data Protection for small charities

superhighways

harnessing technology for community benefit

What we will cover today

1. Intro to GDPR
2. Principles & Legal Bases
3. Data protection policy & Privacy Notices
4. Data audits & planning templates
5. Security best practice

1. How many GDPR principles are there which should govern your use of data? (Single choice)

- ◯ 4
- ◯ 6
- ◯ 7
- ◯ 10

6 principes, with a 7th requiring you to be accountable for the 6 (i.e. you have to be able to prove your compliance)

2. Do you always need to get consent from individuals when collecting and processing their data?

(Single choice)

- ◯ Yes
- ◯ No

No. Consent is required to process personal data where no other legal basis for processing applies. However where processing Special category data, explicit consent is required

3. What percentage of charities in the latest annual DCMS survey report a data breach or security hack in the last 12 months? (Single choice)

- ◯ 24%
- ◯ 30%
- ◯ 66%

30%. It was 24% and then 32% previously and for medium & high income charities it's higher (but could be because larger charities are more likely to know that they've been attacked)

✓Superhighways Agree / Disagree cards

Agree / Disagree

Good Data Protection practice means that we should only ever use people's data in ways they have agreed to.

Agree / Disagree

?

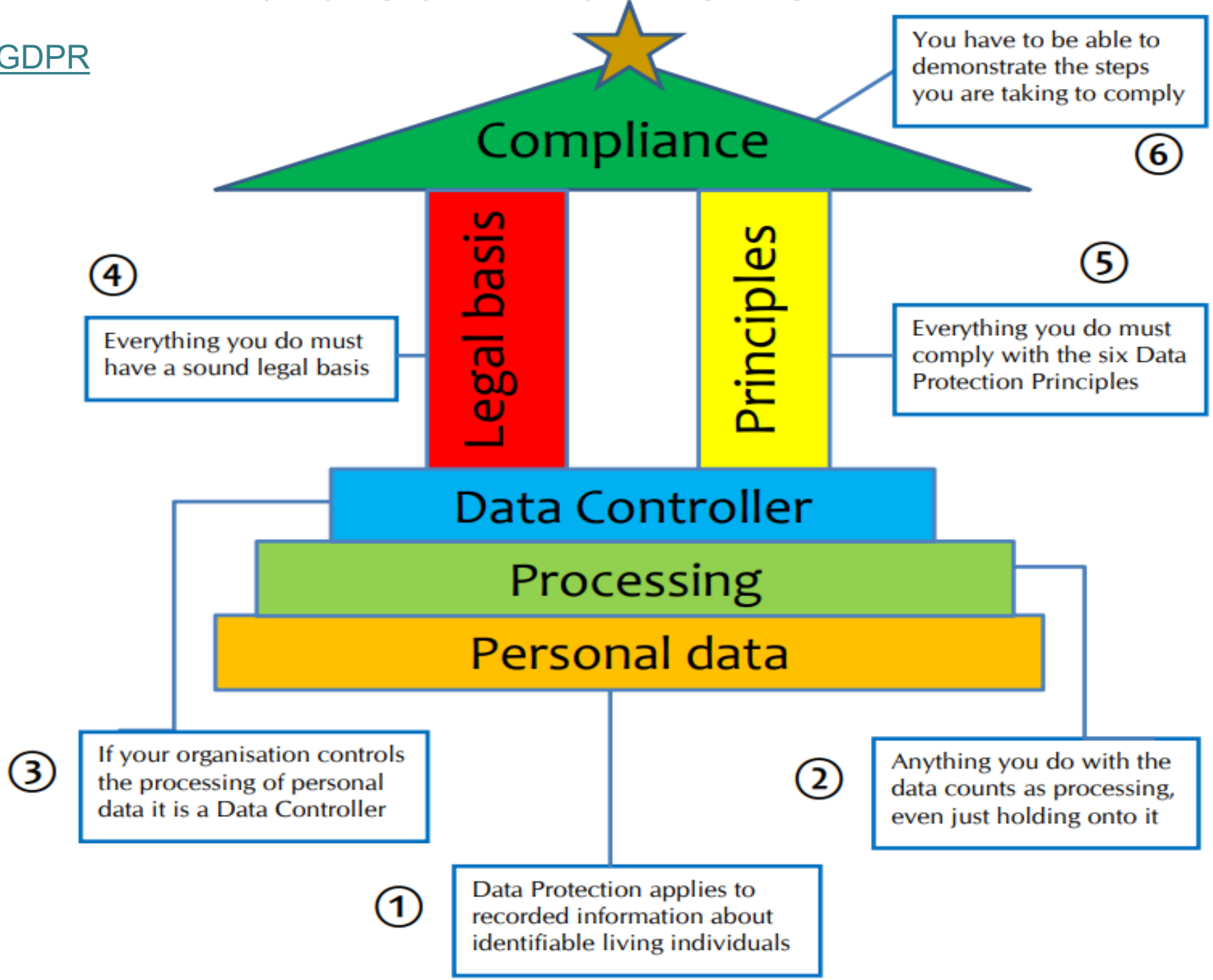
Agree / Disagree

Data' only means what we hold on our database or in a spreadsheet; it doesn't apply to emails, letters or reports.

Agree / Disagree

The most important thing about Data Protection is keeping information secure; as long as our IT is protected we should be OK.

[Paul Ticher's GDPR explainer]



ico.
Information Commissioner's Office

The ICO exists to empower you through information.

Cymraeg

small charities

Home | For the public | For organisations | Make a complaint | Action we've taken | About the ICO

For organisations / Advice for small and medium organisations

Advice for small and medium organisations

Here you'll find advice and guidance for small-to-medium-sized enterprises, start-ups, sole traders, small charities, groups and clubs. Use our easy self-serve tools to get answers to your questions and generate tailored advice, or read our helpful bitesize guidance and tips.

Is your direct marketing compliant?

We've recently announced a fine for a sole trader who was sending spam text messages without valid consent. We understand direct marketing can be important for your business. However, you must understand the rules and respect people's information rights.

Don't get caught out, use our direct

Register and pay your fee

Contact us

News, blogs & events

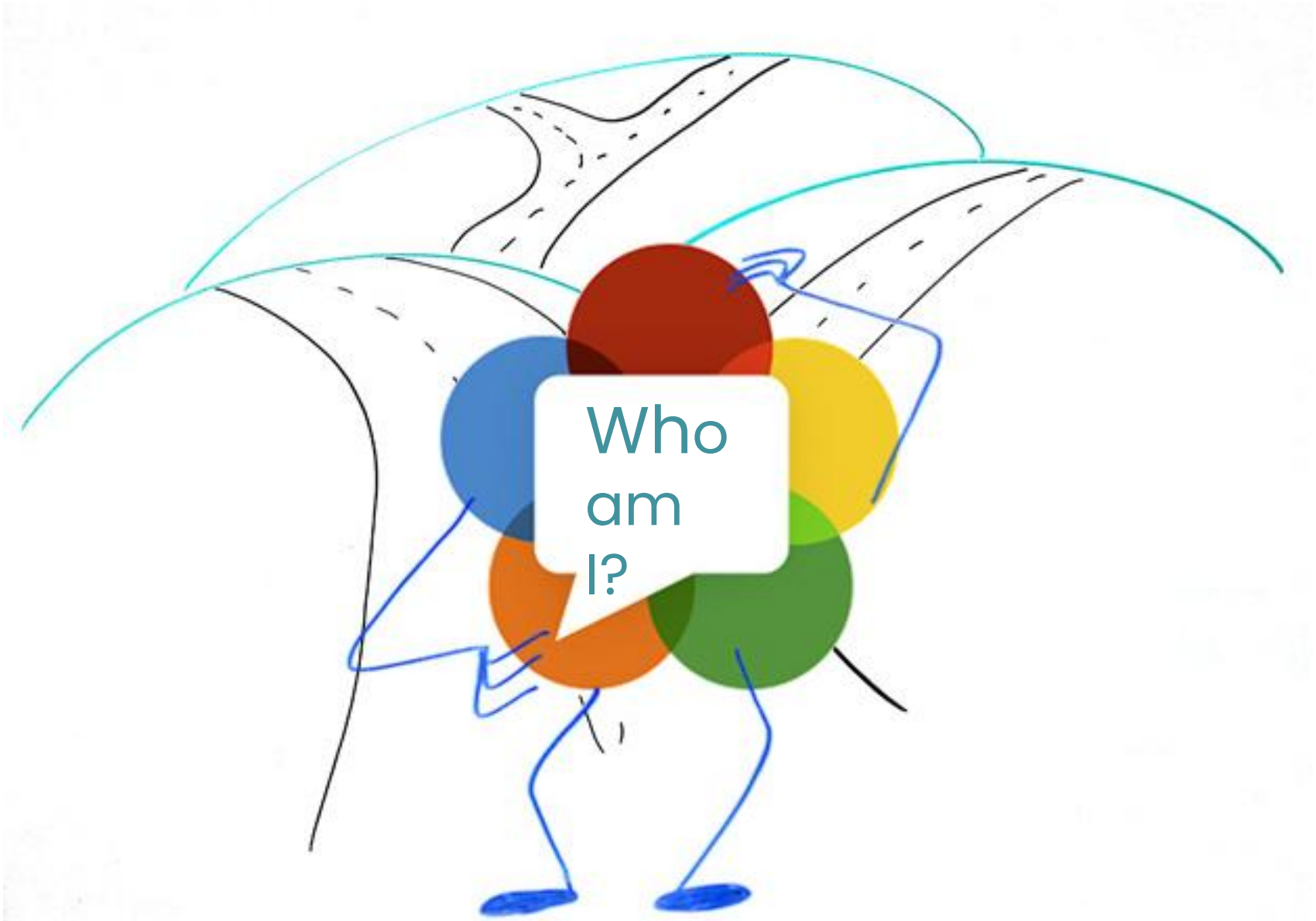
Data (Use and Access) Act 2025

[ICO's advice for small organisastions]

Data Use & Access Act (DUAA) 2025

- ✓ The **DUAA** is a new Act of Parliament that updates some laws about digital information matters
- ✓ It amends, but does not replace:
  - ✓ the UK General Data Protection Regulation (UK GDPR)
  - ✓ the Data Protection Act 2018 (DPA)
  - ✓ the Privacy and Electronic Communications Regulations (PECR)
- ✓ Changes will be phased in between June 2025 and June 2026
- ✓ New requirements relate to provision of online services to children and data protection complaints
- ✓ Soft opt in' for charities: if you're a charity, it allows you to send electronic mail marketing to people whose personal information you collect when they support, or express an interest in, your work, unless they object

See ICO guidance


Who
am
I?

Service users

Staff

Newsletter subscribers

Donors

Volunteers

Trustees

Any others?

Personal data

> "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

- ✓ So personal data is information that relates to an individual
- ✓ That individual must be identified or identifiable either directly or indirectly from one or more identifiers or from factors specific to the individual

Personal data definition

Special Category data

UK GDPR defines special category data as personal data revealing:

- ✓ racial or ethnic origin
- ✓ political opinions
- ✓ religious or philosophical beliefs
- ✓ trade union membership
- ✓ genetic data
- ✓ biometric data (where used for identification purposes)
- ✓ data concerning health
- ✓ data concerning a person's sex life
- ✓ data concerning a person's sexual orientation

ICO guidance including article 9 conditions

6 GDPR principles

1. Process lawfully, fairly and in a transparent manner
2. Collect for specified, explicit and legitimate purposes
3. Only keep what is adequate, relevant and limited to what is necessary
4. Store accurate information and keep up to date
5. Retain only for as long as necessary
6. Process in an appropriate manner to maintain security

Accountability the controller shall be responsible for, and be able to demonstrate, compliance with the principles

Legal basis for processing…

Has to meet at least one of the following 6 Conditions…

- ✓**Consent** – the individual has given clear consent for you to process their personal data for a specific purpose
- ✓**Contract** - the processing is necessary for a contract you have with the individual
- ✓**Legal obligation** - the processing is necessary for you to comply with the law (not including contractual obligations)
- ✓**Vital interests** – the processing is necessary to protect someone's life
- ✓**Public task** - the processing is necessary for you to perform a task in the public interest or for your official functions
- ✓**Legitimate interests** - the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests

Legitimate interests

Applying the three part test:

- ✓Purpose test – is there a legitimate interest behind the processing?
- ✓Necessity test – is the processing necessary for that purpose?
- ✓Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms?

ICO Guidance

Consent

- ✓Review how you are seeking, obtaining & recording consent
- ✓GDPR references consent & explicit consent (e.g. relating to special categories)
- ✓ Both need to be:
  - ✓Freely given
  - ✓Specific
  - ✓Informed
  - ✓Unambiguous
- ✓A clear positive indication of agreement to personal data being processed has to be given
- ✓Controllers must be able to demonstrate consent was given

ICO Consent Checklist

Subject access rights

1) **Right of Access:** find out what kind of personal information is held about them
2) **Right of Rectification:** ask for information to be updated or corrected.
3) **Right to Data Portability:** receive a copy of the information which has been provided so they can provide that information to another organisation.
4) **Right to Restrict Use:** ask for personal information to stop being used in certain cases.
5) **Right to Object:** objecting to use of information (where a party is processing it on legitimate interest basis) and to have their personal information deleted.
6) **Right to Erasure:** in certain circumstances, they may also have their personal information deleted.

ICO Registration & Breach notifications

ICO Registration

- ✓Organisations processing personal data should register with the ICO (fees from £40 annual renewal) Note that some exemptions apply.
- ✓You can check if you are already registered in this publicly searchable list

Data Breaches

- ✓Develop procedures to detect, report and investigate a personal data breach
- ✓You have a breach notification duty to report within 72 hours
- ✓Not all breaches need to be notified – only ones where the individual is likely to suffer some form of harm e.g. identify theft or a confidentiality breach
- ✓Check on the ICO website here for further information *(you can phone the Helpline too)*

Data security breaches reported to ICO

Home

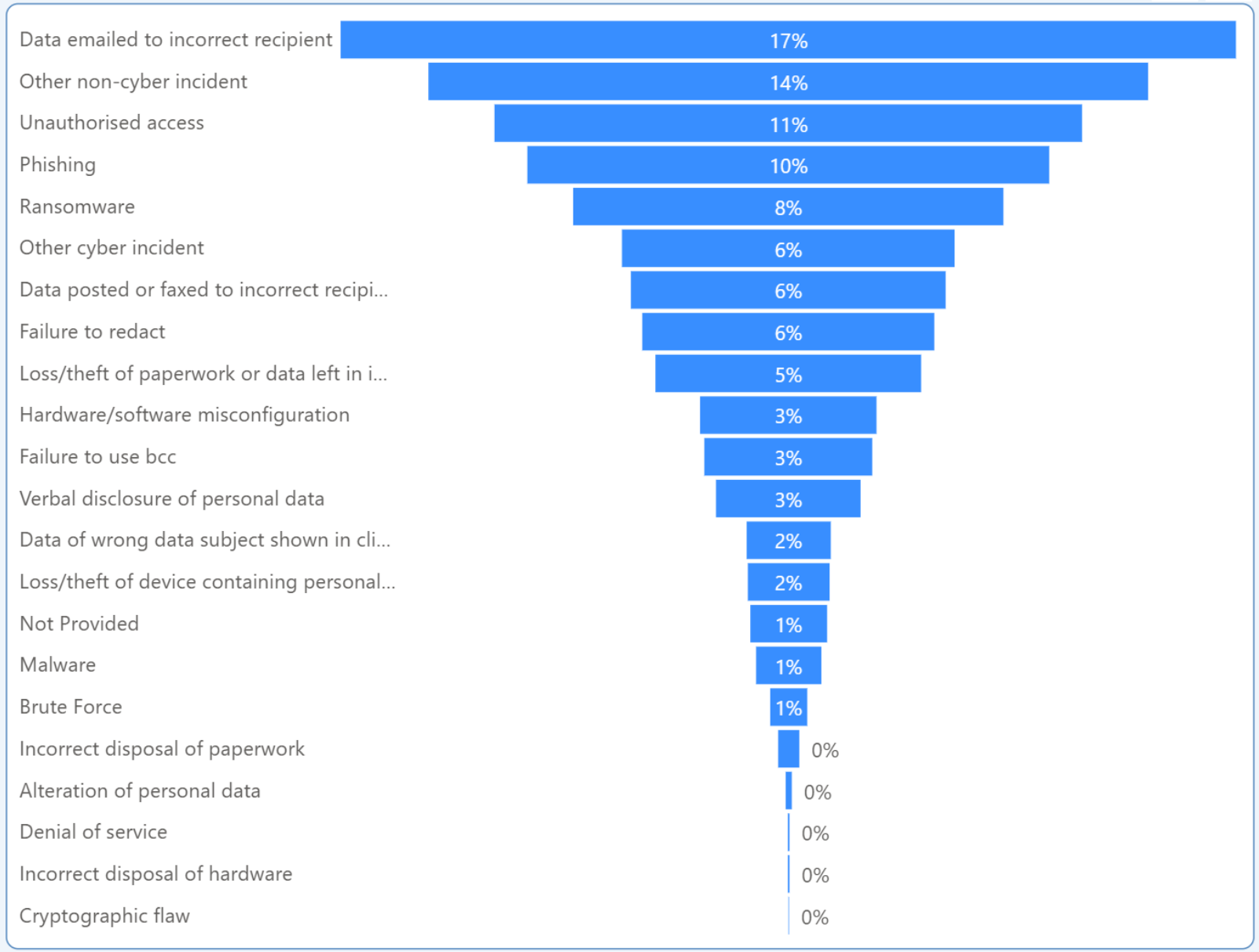
Narrative

Time Series

Breakdown

Cross-Tabs

Proportion of Incidents Reported



Category of Data

- ○ Data Subject Type
- ○ Data Type
- ○ Decision Taken
- ○ Incident Category
- ◉ Incident Type
- ○ No. Data Subjects Affected
- ○ Sector
- ○ Time Taken to Report

Date

- ☐ 2019
- ☐ 2020
- ☐ 2021
- ☐ 2022
- ■ 2023
- ■ 2024
- ■ 2025

Bar Chart -

Funnel Chart -

Organisational checklist

1. Recommendation to have a nominated lead (some organisations are required to have an official Data Protection Officer)
2. Do you have a Data protection policy? (Should include or reference elsewhere to IT security procedures e.g. could be in a Computer usage policy)
3. Do you have a Privacy notice?
4. Have you carried out a data audit (documentation of what data you hold, where it's stored, how it's used, if it's shared with anyone etc)
5. Do you know what to do if you have a suspected or actual data breach?
6. Do you regularly train your staff, trustees and volunteers?

What your Data Protection Policy needs

- ✓ Commitment to the legal principles
- ✓ Commitment to the people's rights relating to your data
- ✓ Intention to ensure that lawful processing is carried out.
- ✓ Intention to minimise data collection.
- ✓ Retention: how long you'll keep data and how you'll delete it
- ✓ Security of your systems: where data can be stored, what people can / can't do with the data and computers/ devices the data is processed on
- ✓ Implementation: system and processes for ensuring staff/volunteers are trained and up to date.

NCVO – Writing a data protection policy and procedures

Communicating privacy information

- ✓Review current privacy notices
- ✓GDPR requires the following to be communicated:
  - ✓Explain your purposes + legal basis for processing the data
  - ✓State data retention periods
  - ✓Point out people have a right to complain to the ICO if they think there is a problem with how you are handling their data
- ✓Consider a layered approach - key points to be presented at point of data capture – e.g. paper or online forms. Full details included in an accessible and understandable privacy policy or statement
- ✓Full details should be included in a publicly available, accessible and understandable privacy policy or statement
- ✓ICO Privacy Notice Generator (for smaller organisations including charities)

Suggestions for your Privacy notice

- ✓Use clear, normal everyday language, avoiding confusing terminology or legalistic jargon
- ✓Adopt a style that your audience will understand
- ✓Don’t assume that everybody has the same level of understanding as you
- ✓Consider providing separate notices for different audiences
- ✓Ensure all your notices are consistent and are updated when needed

How to provide privacy information

Use a range of media & locations:

✓Orally

Face to face or when you speak to someone on the telephone (it's a good idea to document this)

✓In writing

For example, on printed documents and forms

✓Through signage

For example, an information poster in a public area

✓Electronically

In text messages, on website, in emails, in mobile app or online forms

WHAT WE DO WITH PERSONAL DATA WHEN YOU...

MAKE A COMPLAINT

- To investigate and take regulatory action in line with our statutory duties
- Information from you to investigate your complaint properly
- Necessary to perform our public tasks as a regulator

MAKE AN ENQUIRY

- To fulfil our regulatory responsibilities
- Enough information to respond to your enquiry
- Necessary to perform our public tasks as a regulator

REGISTER FOR A WEBINAR

- To facilitate the event and provide access to it
- Contact information
- Consent

MAKE AN INFORMATION REQUEST

- Fulfil your information request
- Contact information and enough information
- Necessary to comply with a legal obligation to which we are subject

SUBSCRIBE TO OUR E-NEWSLETTER

- So we can email information to you
- Name and address
- Consent

ARE BEING INVESTIGATED BY THE ICO

- To establish whether a criminal offence has occurred and take any appropriate legal action
- Information compiled during our investigation of an alleged offence
- Necessary to perform our public tasks as a regulator

PAY A FEE

- To communicate with you about the fee and any related issue
- Contact and address information for your business, and DPO name if relevant
- Necessary to perform our public tasks as a regulator

REPORT A NUISANCE CALL OR MESSAGE

- Investigate and take regulatory action in line with our statutory duties
- Phone number you received the call on and the first part of your postcode, contact information is optional
- Necessary to perform our public tasks as a regulator

ATTEND AN EVENT

- To facilitate the event and provide you with a good service
- Contact information, organisation name. If offered a place, dietary requirements or access provisions. We may also ask for payment if there is a charge to attend.
- Consent

REQUEST OUR PUBLICATIONS

- So we can post information to you
- Name and address
- Consent

KEY

- PURPOSE OF PROCESSING PERSONAL DATA
- the INFO WE NEED
- LAWFUL BASIS for USING YOUR DATA

For further information on how and why we use your personal data, including how long we keep it, your rights, who we share it with, and how you can contact us, please read our full privacy notice at:

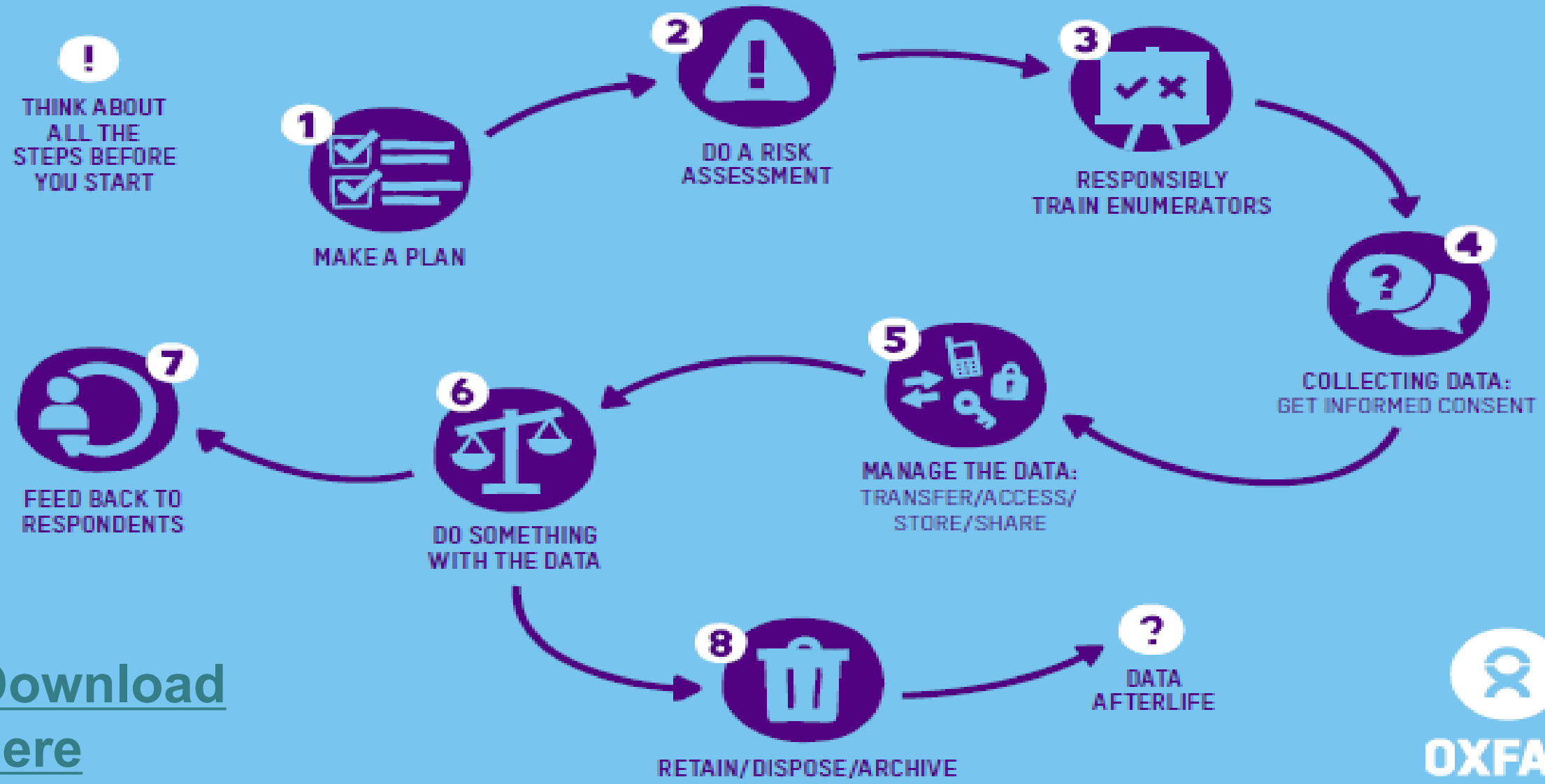
ico.org.uk/privacy-notice

ico.
Information Commissioner's Office.

An organisational data audit

When do we collect data?	What data do we collect?	What is the purpose of collecting data?	Where do we store the data?	When & how do we ask for consent?	How long do we store the data for? And how do we dispose of it?	What risks are associated with collecting, storing and using this data? And how can we mitigate them?
At sign up people complete a form & sign the register when joining the session in person or on Zoom	Name, email, contact number, organisation, job title, ethnic origin, access requirements, level of knowledge, geographical location, areas of	To know how many people will be attending, to make sure we cater for their requirements for this session and understand our audience	In our event management database, on Zoom (registrations, chat & recordings), On paper if in person sign up, On digital cameras & folders in Sharepoint if taking	On the application form we request consent to store their data, consent to be in photos if a live event, newsletter sign up. If on Zoom we ask for consent to	In our Events management database we store data for 6 years and fully anonymise in the 7th year – removing all personal information connected to the booking.	There is a risk training data might be exported into Excel for analysis – this can be mitigated by ensuring that everyone saves Excel files to a secure environment e.g. SharePoint or Teams not to their local hard drives Photos from events are saved into folders & might be forgotten about. Folders with

THE RESPONSIBLE DATA LIFECYCLE



[Download here]

OXFAM

MAKING A DATA PLAN

What is your purpose? What are you going to do with the data?		**What methods/tools will you use to collect the data?**
How will you get informed consent?	**SCENARIO**	**Who will you collaborate with?**
How will you train your team? How will you involve your service users / community?		**What are the risks and how will you manage them?**

Download the matrix

ICO's 5 top tips for small charities

✓ **Tell people what you are doing with their data**
People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.

✓ **Make sure your staff are adequately trained**
New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.

✓ **Use strong passwords**
There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves.

✓ **Encrypt all portable devices**
Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

✓ **Only keep people's information for as long as necessary**
Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

Some context about Cyber Attacks

Question:

In the annual DCMS survey 2025, what percentage of charities reported having a cyber security breach in the last 12 months?

24% 30% 32% 66%

30%

Official Statistics

Cyber security breaches survey 2025

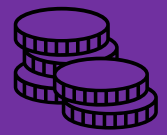
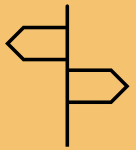
Updated 19 June 2025

Attacks causing the most disruption

Type	Businesses	Charities
Phishing attacks, i.e. staff receiving fraudulent emails or arriving at fraudulent websites	85%	86%
Others impersonating, in emails or online, your organisation or your staff	34%	35%
Organisation's devices being targeted with other malware (e.g. viruses or spyware)	18%	14%

Why are charities at risk?

National Cyber Security Centre

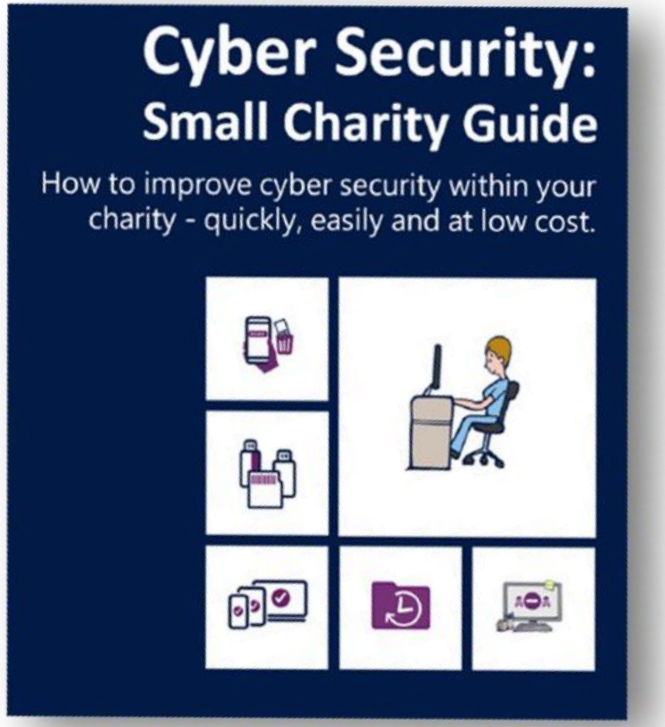
Charities...	Hold funds 	Personal, financial and commercial data of interest or monetary value 	Data is sensitive, valuable and vulnerable to attack 
Impact.... Data gets lost 	You have to stop operations 	Financial/Time cost to recover 	Reputation 

What can you do to protect your charity?

The National Cyber Security Centre's

5 quick, simple, free or low cost steps

1. Backing up your data
2. Protecting against malware
3. Securing your mobile devices
4. Password best practice
5. Avoid phishing attacks



Download the full guide

Download the infographic

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/charity** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.

Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.

Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

Blog post and Sway on our website

Cyber Security Basics for everyone - Superhighways

Other cyber security resources

- ✓What is phishing
- ✓CyberAware – advice for individuals
- ✓Cyber Security online training for small organisations
- ✓Exercise in a Box
  - ✓Identifying and reporting a suspected phishing email
  - ✓Using passwords

- ✓Superhighays free monthly Cyber security for everyone sessions
- ✓Check out Charity Digital webinars too

Other data protection resources

- ✓NCVO – Writing a data protection policy and procedures
- ✓Information Commissioners Office – guidance for small organisations
- ✓ICO Checklist for small organisations
- ✓ICO's guide to dealing with Subject Access Requests

- ✓NCVO – regular Essentials and Advanced training sessions

About Superhighways....

A project of Kingston Voluntary Action, we provide digital, data & tech advice, support & training to the sector, including:

- ✓ Tech Support
- ✓ Training
- ✓ Websites
- ✓ Digital, data & tech strategy
- ✓ Digital inclusion
- ✓ Consultancy
- ✓ Digital leadership
- ✓ Datawise London

Sign up to our newsletter for free training offers https://superhighways.org.uk/e-news/

Thanks for listening

superhighways
harnessing technology for community benefit

Kate White
info@superhighways.org.uk
www.superhighways.org.uk