Data Protection Basics

Trust for London

Tackling poverty and inequality

superhighways

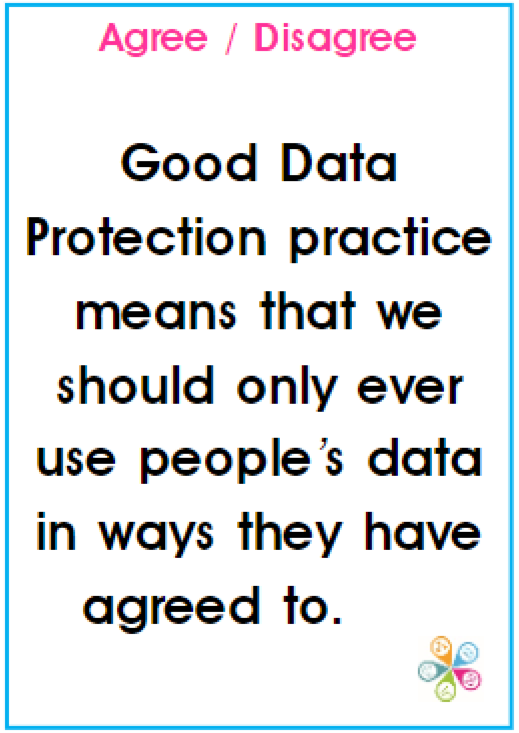
harnessing technology for community benefit

What we'll cover today

- ✓ GDPR compliance
  - ✓ Principles
  - ✓ Legal Basis
  - ✓ Data audit template
  - ✓ Privacy notice template
- ✓ IT Security
- ✓ Responsible Data Lifecycle

What do we know already?

- ✓Zoom poll
- ✓Superhighways Agree / Disagree cards

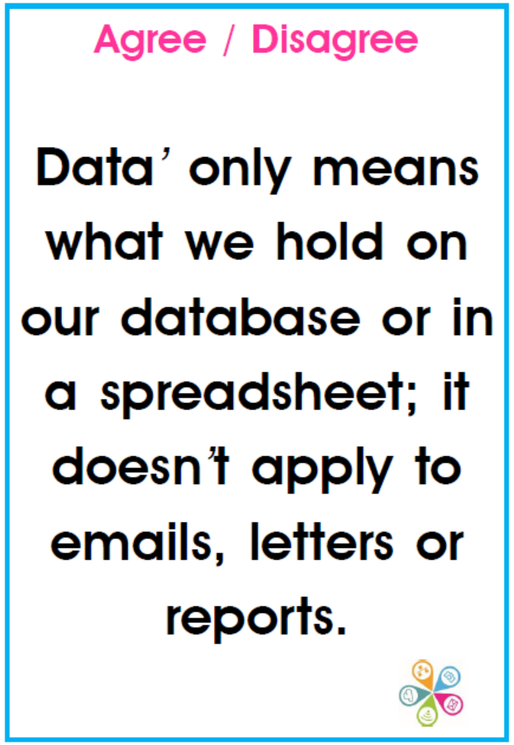


Agree / Disagree

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

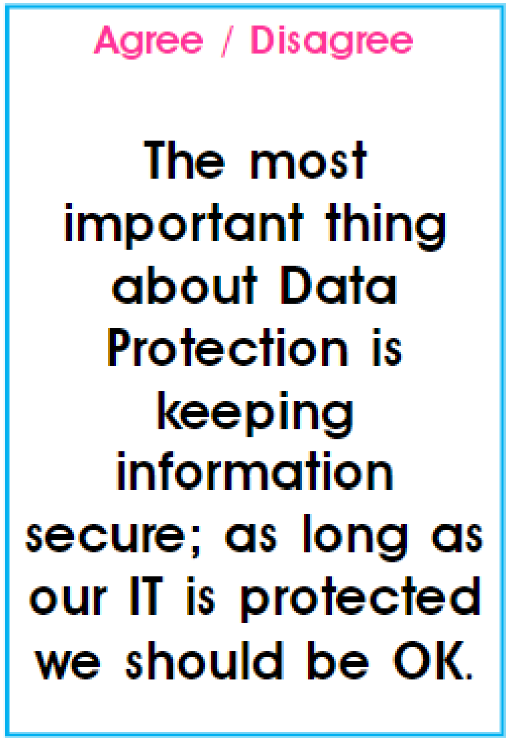
Agree / Disagree

?



Agree / Disagree

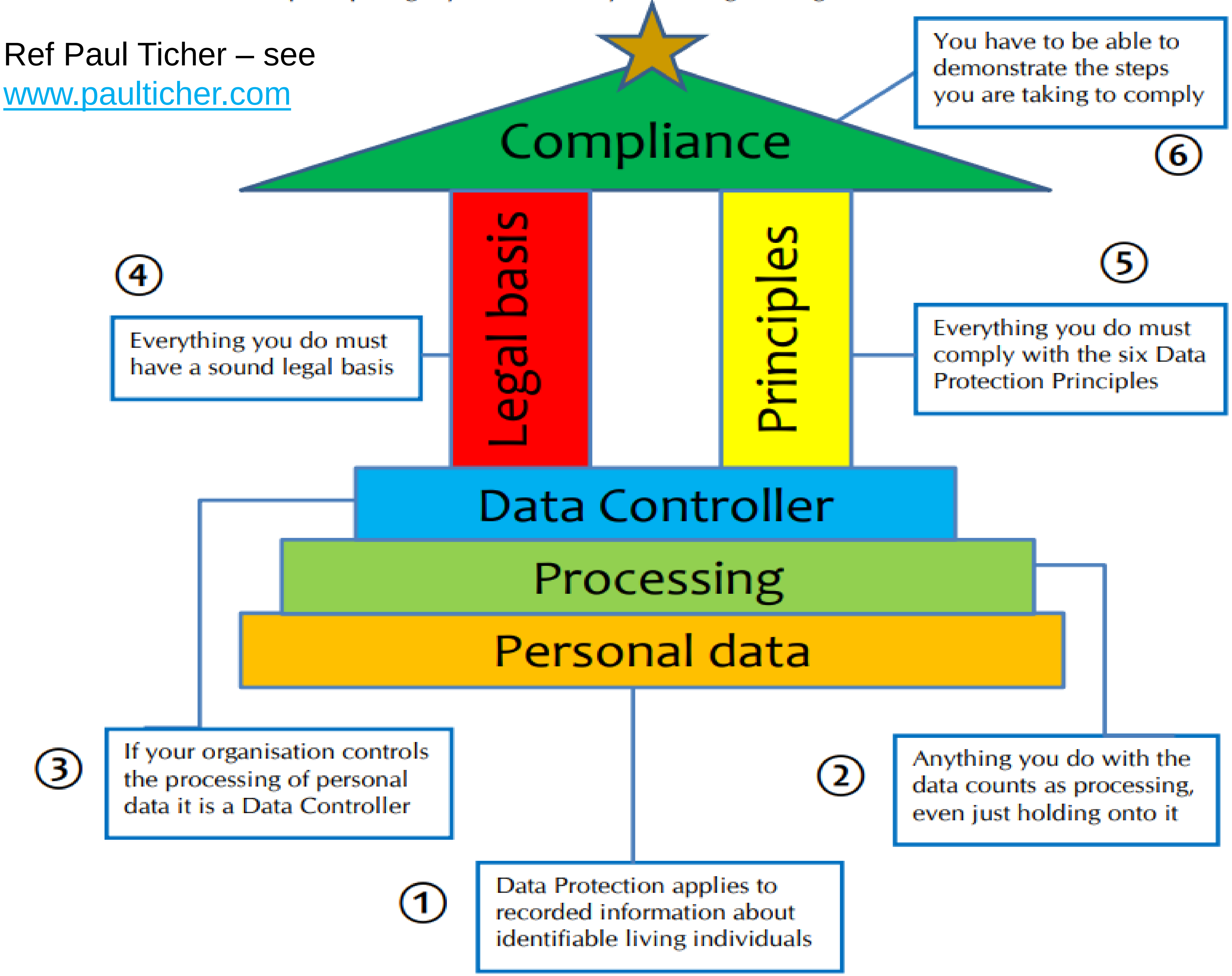
Data’ only means what we hold on our database or in a spreadsheet; it doesn’t apply to emails, letters or reports.



Agree / Disagree

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

Ref Paul Ticher – see www.paulticher.com



Compliance

Legal basis

Principles

Data Controller

Processing

Personal data

1 Data Protection applies to recorded information about identifiable living individuals

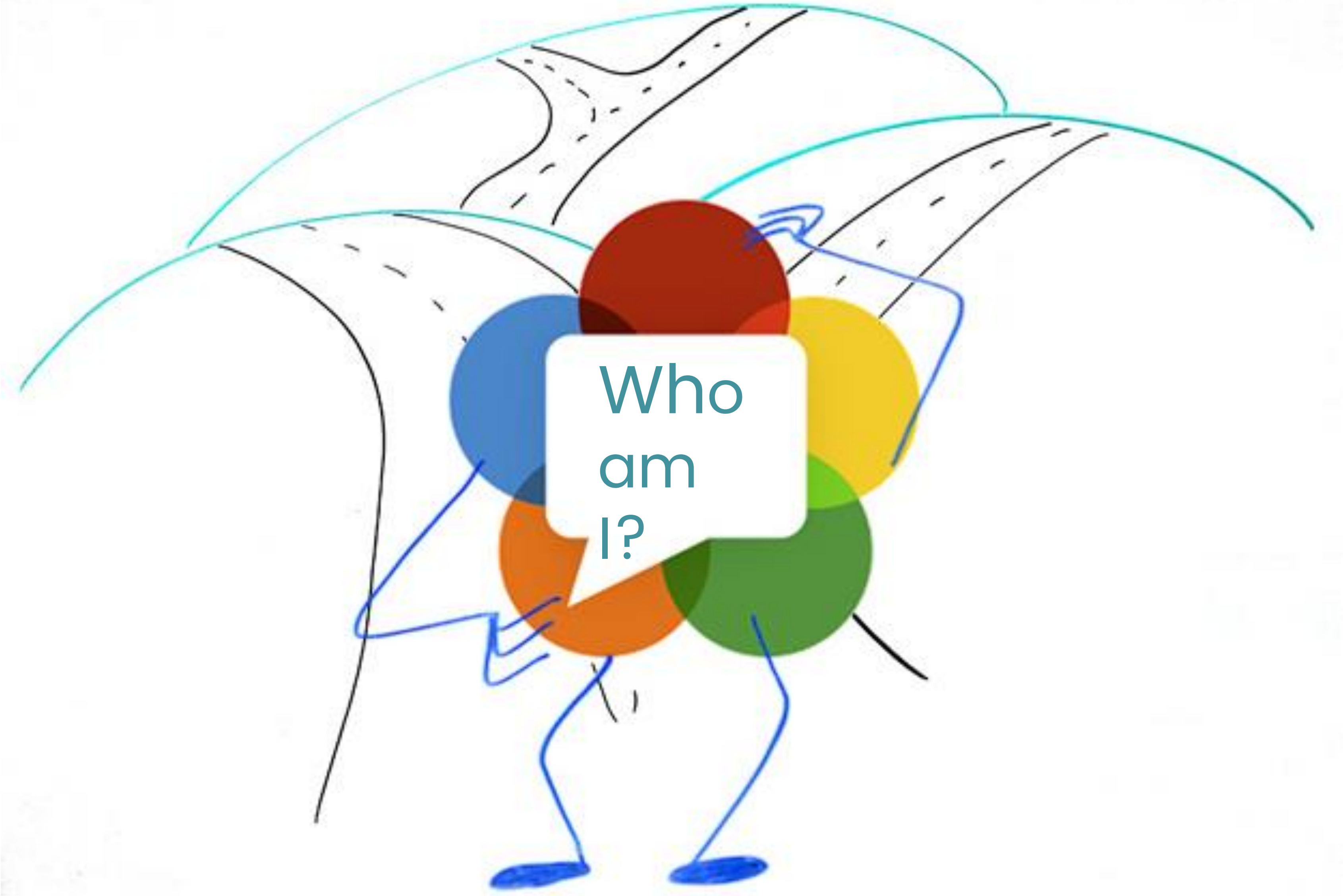
2 Anything you do with the data counts as processing, even just holding onto it

3 If your organisation controls the processing of personal data it is a Data Controller

4 Everything you do must have a sound legal basis

5 Everything you do must comply with the six Data Protection Principles

6 You have to be able to demonstrate the steps you are taking to comply



Personal data definition

Special categories

Personal data?

1. Check in list for organisations attending training including email & phone numbers

2. Database of previous mayors going back over the last two centuries

3. Spreadsheet with client details including ethnicity and health information

4. A map with ‘pins’ showing client locations for the service you’re delivering in a specific borough

Data processing…

- ✓How are you processing personal data?

The 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

7. *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

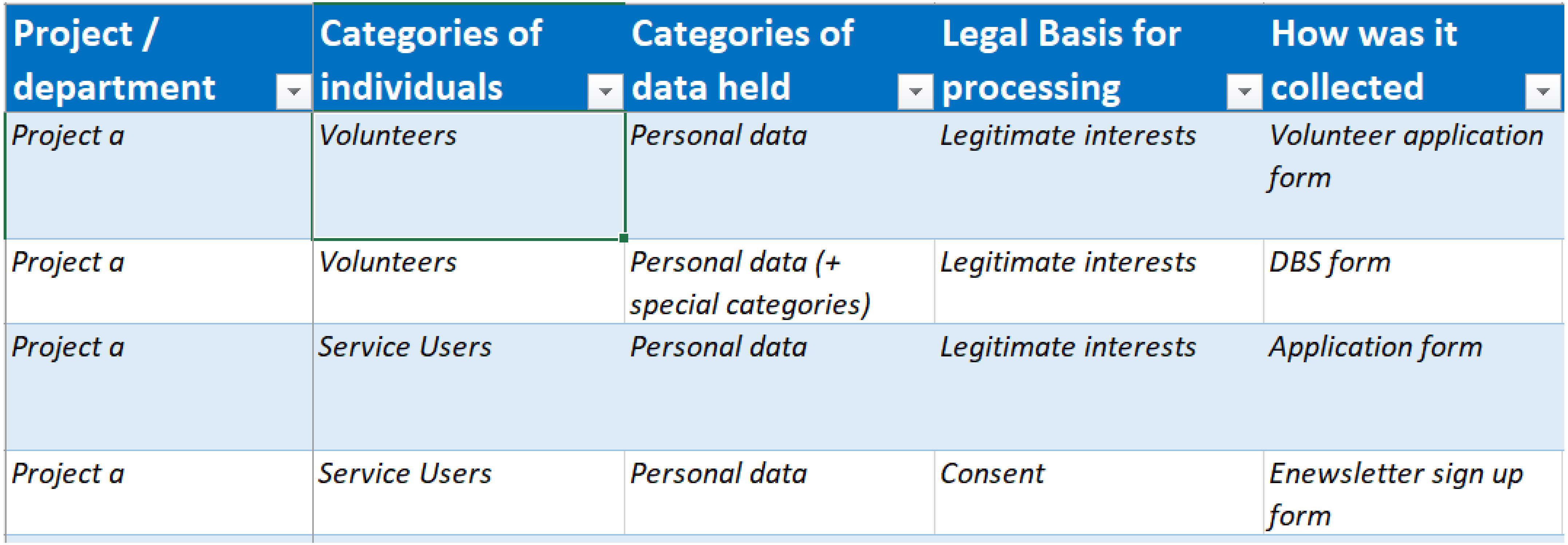
Legitimate interests

✓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

Data audits



Project / department	Categories of individuals	Categories of data held	Legal Basis for processing	How was it collected
Project a	*Volunteers*	*Personal data*	*Legitimate interests*	*Volunteer application form*
Project a	*Volunteers*	*Personal data (+ special categories)*	*Legitimate interests*	*DBS form*
Project a	*Service Users*	*Personal data*	*Legitimate interests*	*Application form*
Project a	*Service Users*	*Personal data*	*Consent*	*Enewsletter sign up form*

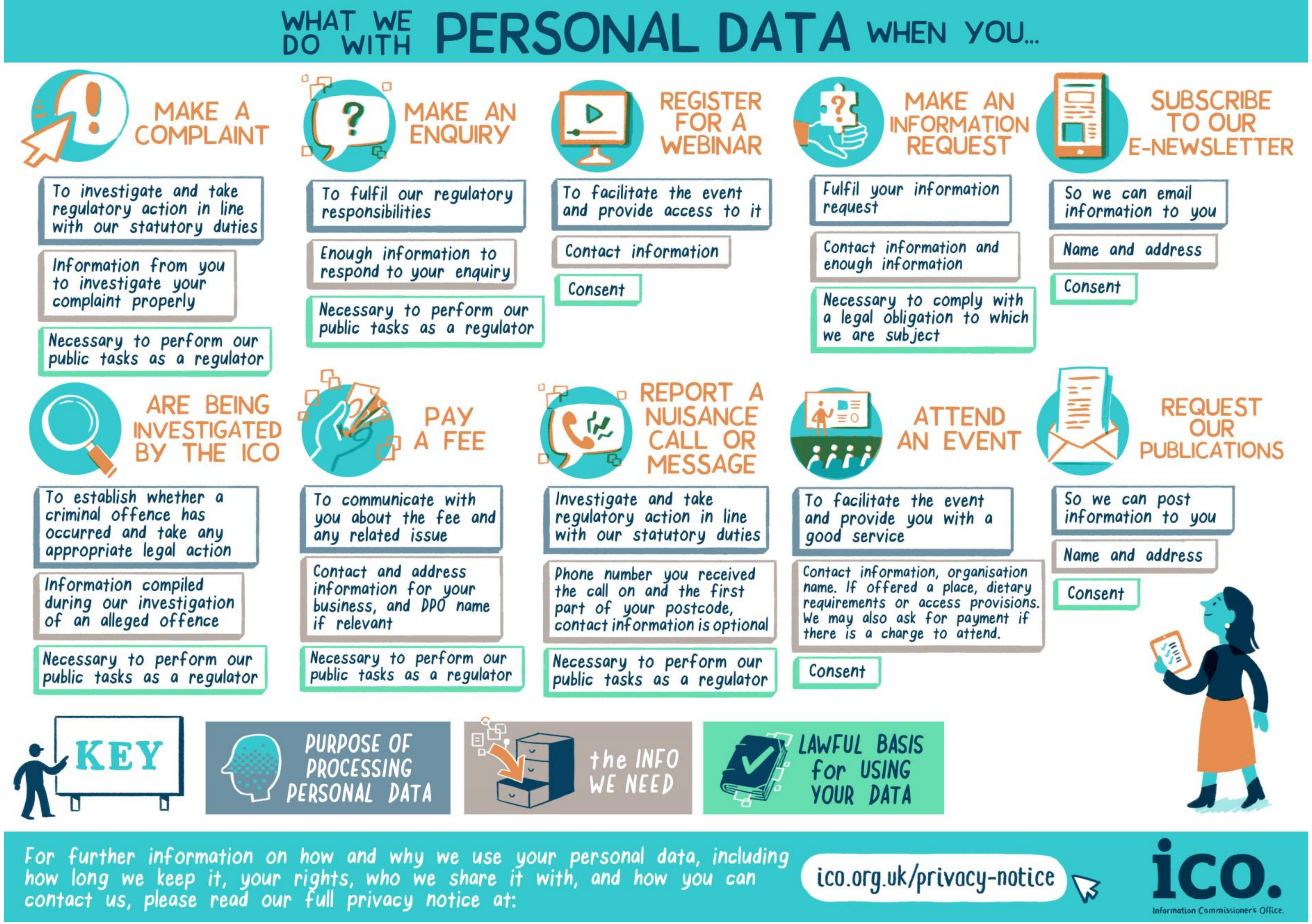
Communicating privacy information

✓Review current privacy notices – do you have one?

✓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



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 Privacy Policy Template to download and use

Consent

- ✓Review how you are seeking, obtaining & recording consent
- ✓GDPR references consent & explicit consent (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

Organisational Accountability

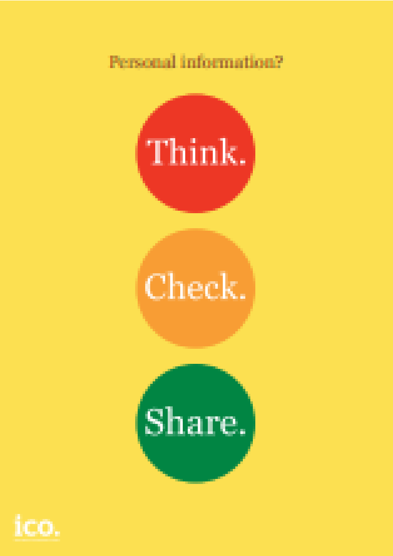
Raising awareness

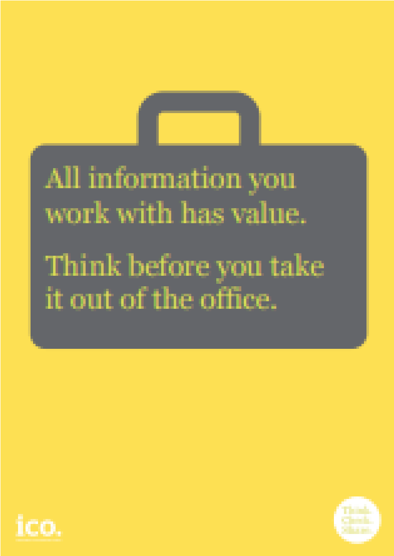
- ✓Update trustees, staff & volunteers – check everyone knows and understands your Data Protection Policy (see here for template)
- ✓Identify areas where you may have compliance issues
- ✓Look at your risk register?

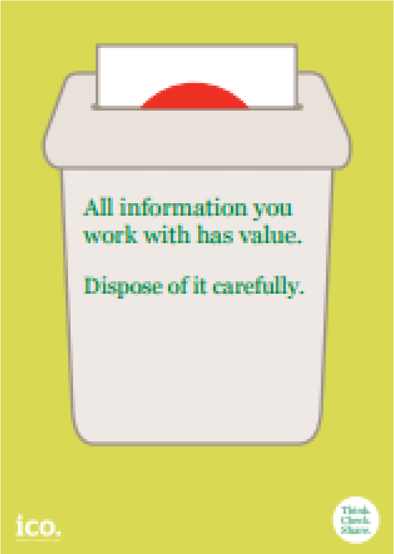
Review the information you hold

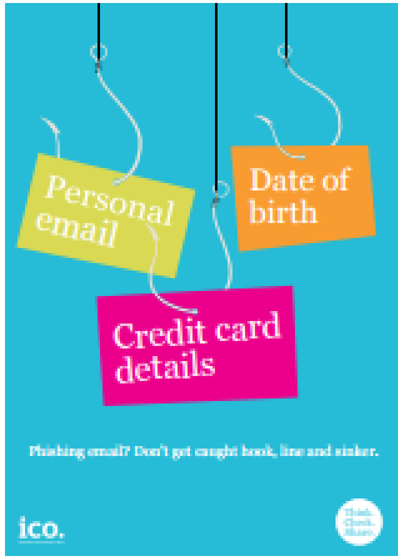
- ✓Document the personal data you hold
- ✓Where it came from
- ✓Who do you share it with - you are expected to be able to update an organisations you've shared data with about an inaccuracy which needs correcting

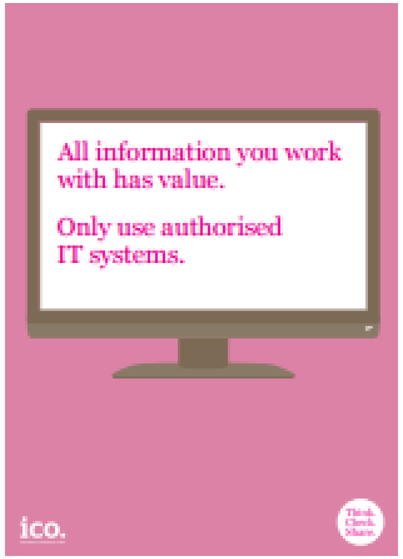
Think. Check. Share toolkit

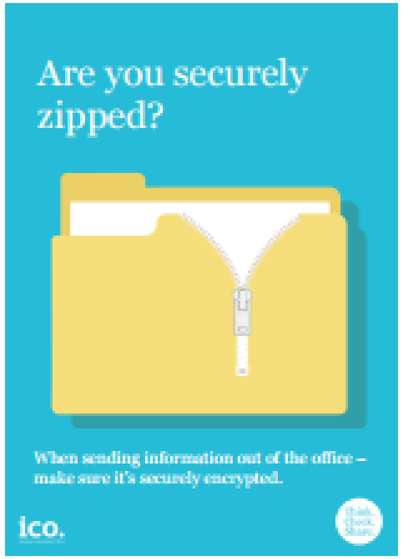


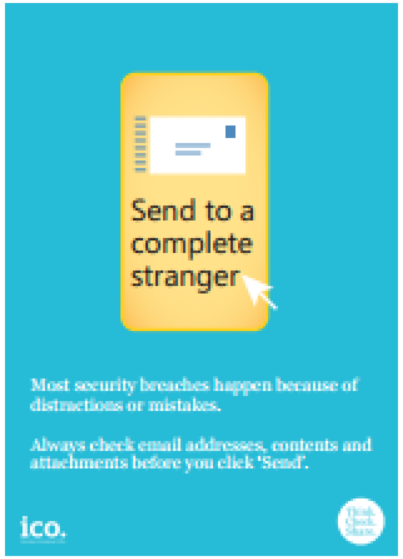

All information you work with has value.
Think before you take it out of the office.
ico.
Think. Check. Share.

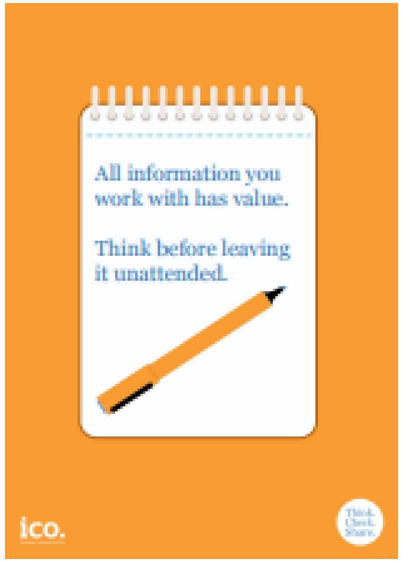


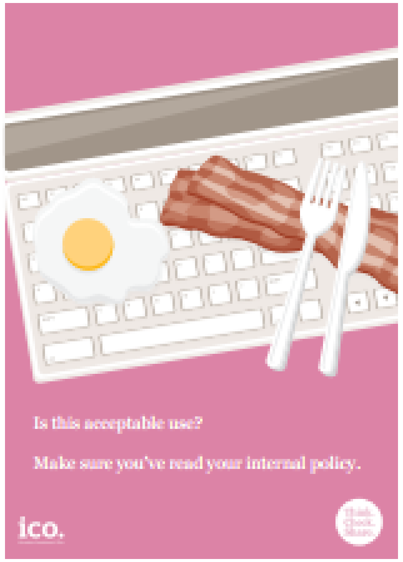


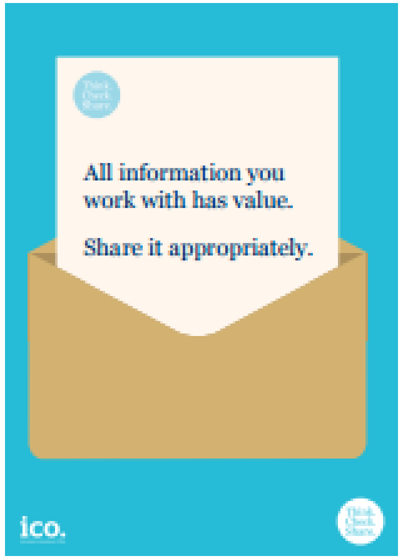

All information you work with has value.
Only use authorised IT systems.
ico.
Think. Check. Share.


Are you securely zipped?
When sending information out of the office – make sure it's securely encrypted.
ico.
Think. Check. Share.


Send to a complete stranger
Most security breaches happen because of distractions or mistakes.
Always check email addresses, contents and attachments before you click 'Send'.
ico.
Think. Check. Share.


All information you work with has value.
Think before leaving it unattended.
ico.
Think. Check. Share.





Data Controller vs Processor

Data Controller

- ✓ The ‘person’ legally responsible for complying with the Data Protection Act
- ✓ Can be an individual, but usually the organisation (Staff & volunteers are ‘agents’ of the Data Controller)

Data Processor

- ✓ An organisation that work is outsourced to, which involves accessing and processing Personal Data.
- ✓ The Data Controller remains responsible for what happens to the data
- ✓ There must be a *written* contract with the Data Processor, setting out:
  - ✓ what they are to do
  - ✓ what the relationship is
  - ✓ security measures

ICO Registration & Breach notifications

ICO Registration

- Organisations processing personal data should register with the ICO (fees from £40 annual renewal)
- But there are exemptions for charities and community groups. Take the registration self assessment here to see if you are exempt

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 damage e.g. identify theft or a confidentiality breach
- Check on the ICO website here for further information (you can phone the Helpline too)

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.

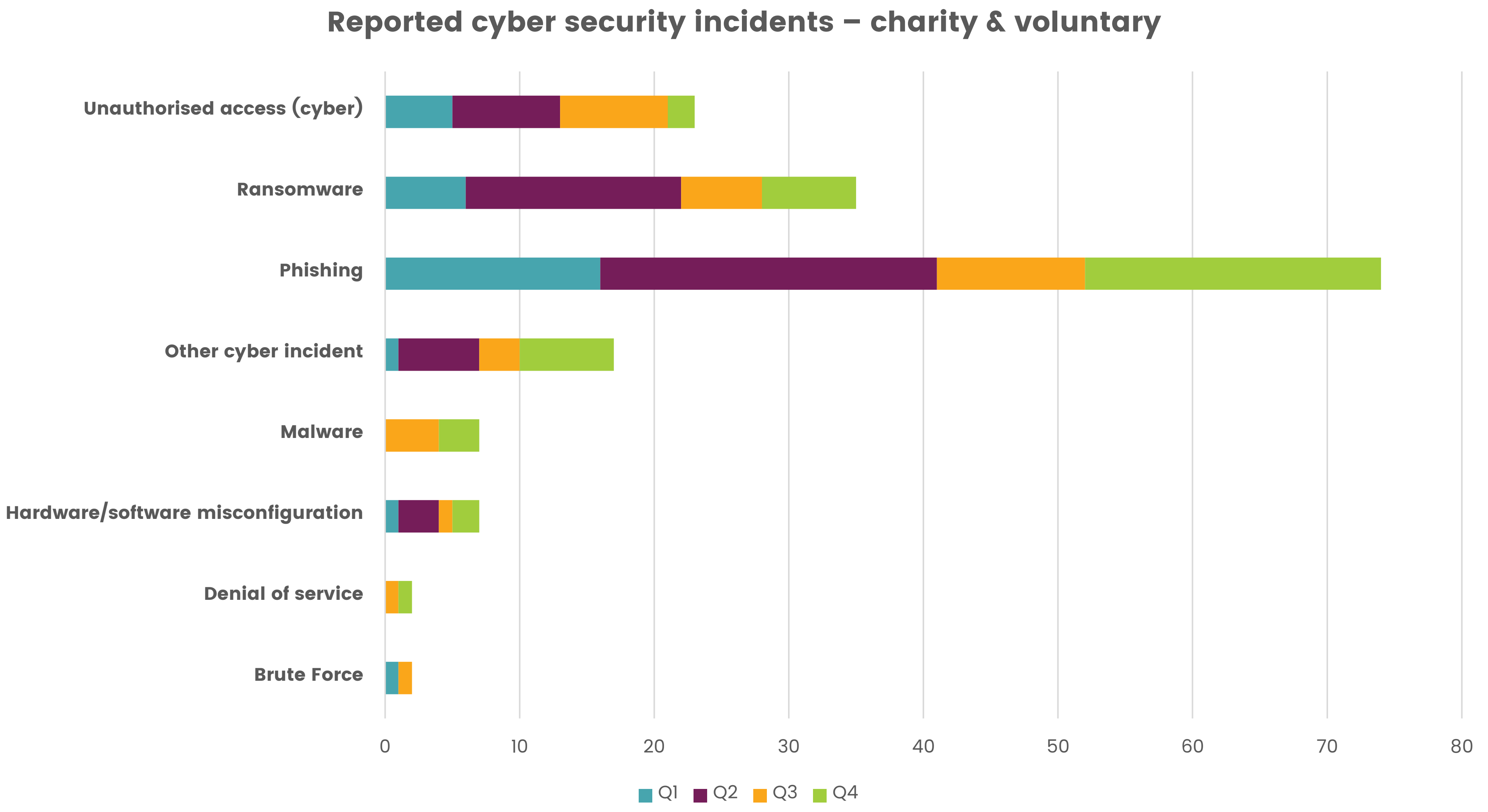
✓ **Use strong passwords**
There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves.

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

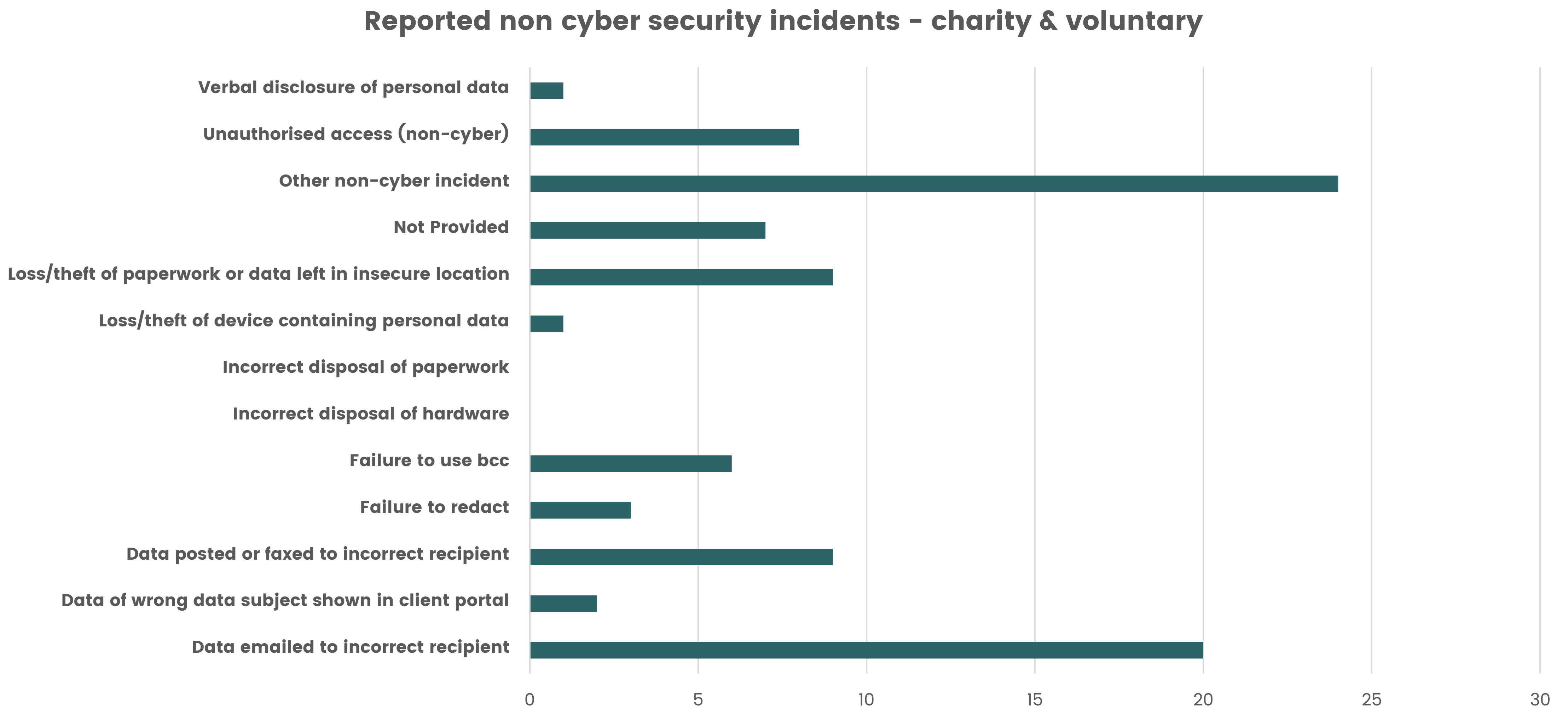
✓ **Only keep people's information for as long as necessary**
Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

IT Security

ICO Data security incident trends – 2020/21



ICO Data security incident trends – Q4 2020/21



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.

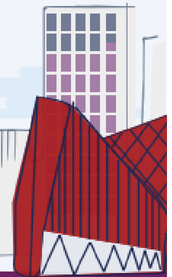
Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

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.



Help the homeless

A local homeless support charity with 8 trustees, 4 full time members of staff (CEO, Services Manager, Homeless Advisor, Office Assistant) and 1 part time finance manager (who works Tuesday, Wednesday, Thursday). All staff have a work laptop and mobile phone.

In addition they have 25 volunteers who assist with the charities activities supporting the homeless, they all have a charity email address which they access from their own devices through an online log-in form.

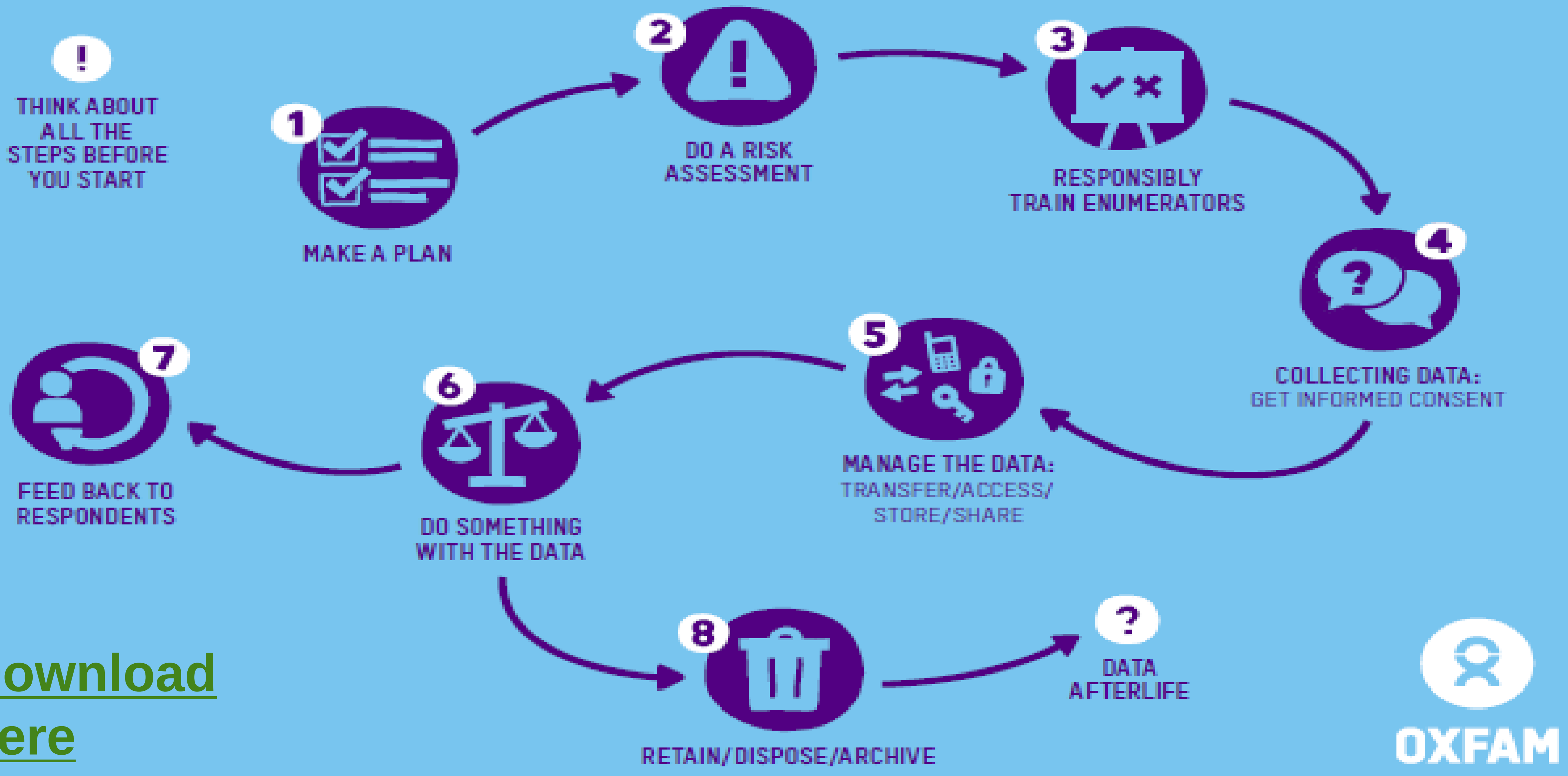
The charity has an annual income of £200,000 and assets which include a night-shelter, which also doubles as the charity's office.

Responsible data lifecycle

RESPONSIBLE DATA MANAGEMENT?

- Treating the people whose data we manage with respect and dignity, and ensuring that we always act in their best interests
- A constantly evolving process about deciding when and how to collect data and how to manage risks
- A policy is not enough alone, we need to *practice* responsible data management
- More than just about following rules and complying with the law - it's also about our culture and individual attitudes towards managing and handling data.
- We must also consider our organisation's internal policies as well as the growing body of legislation around data management

THE RESPONSIBLE DATA LIFECYCLE



! THINK ABOUT ALL THE STEPS BEFORE YOU START

1 MAKE A PLAN

2 DO A RISK ASSESSMENT

3 RESPONSIBLY TRAIN ENUMERATORS

4 COLLECTING DATA: GET INFORMED CONSENT

5 MANAGE THE DATA: TRANSFER/ACCESS/ STORE/SHARE

6 DO SOMETHING WITH THE DATA

7 FEED BACK TO RESPONDENTS

8 RETAIN/DISPOSE/ARCHIVE

? DATA AFTERLIFE

OXFAM

Download here

Thanks for attending

- ✓ Complete our session evaluation
- ✓ Check training opportunities on our Eventbrite page
- ✓ Sign up to our eNews