Ethical & Responsible Data Usage

CONSIDERATIONS FOR SMALL CHARITIES

#DatawiseLondon

datawise
LONDON

Our mission is to help you unlock the value of your data.

superhighways
harnessing technology for community benefit

COALITION
FOR EFFICIENCY

Makerble

DataKind UK

hear
humanity. equality. rights.

london plus

What we'll cover today

- ✓Data Protection compliance
- ✓Research ethics appropriate for small charities
- ✓Informed consent
- ✓Data sharing
- ✓Responsible Data Lifecycle - templates

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

?

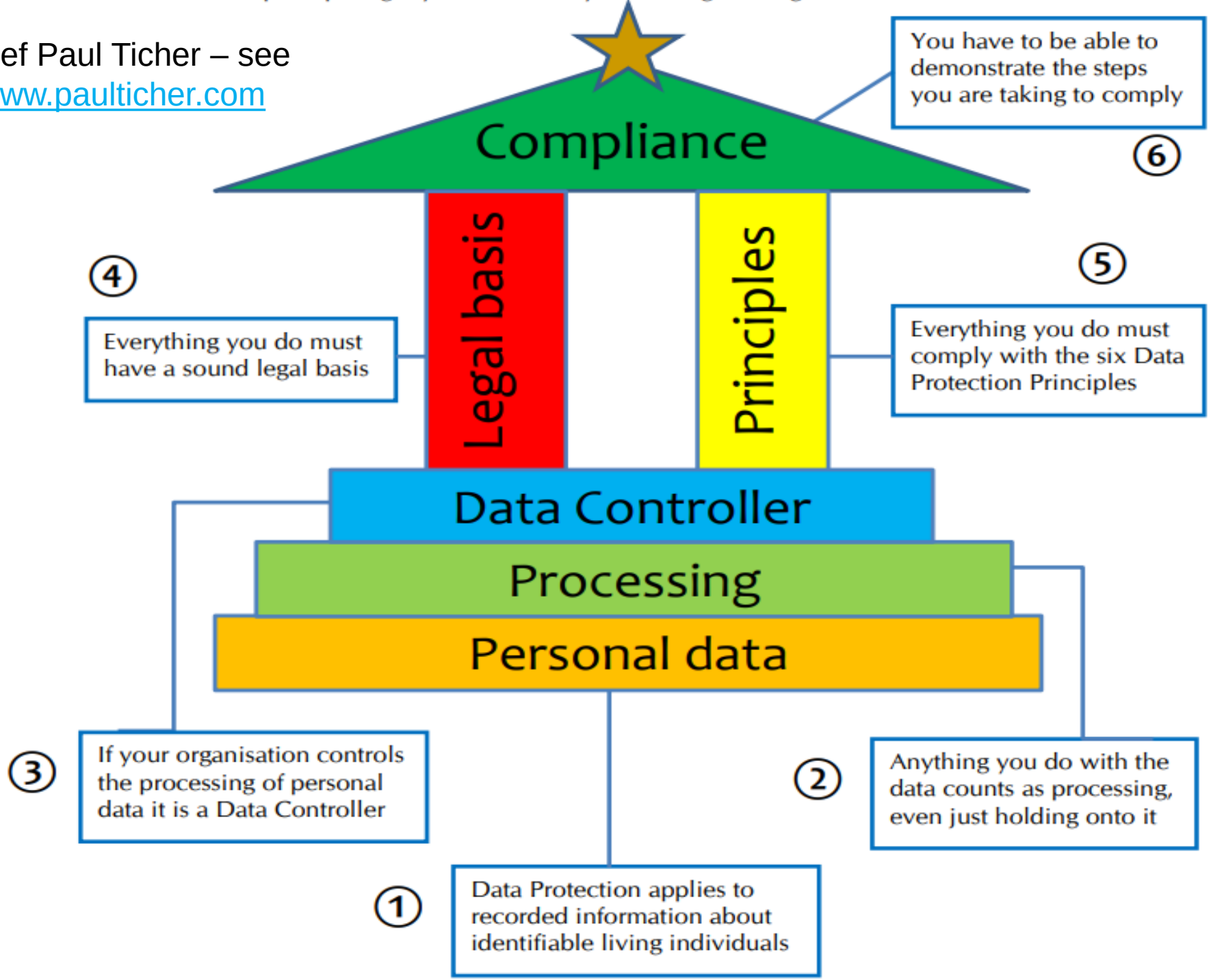
Agree / Disagree

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



Personal data definition

Special categories

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

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

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.

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

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.

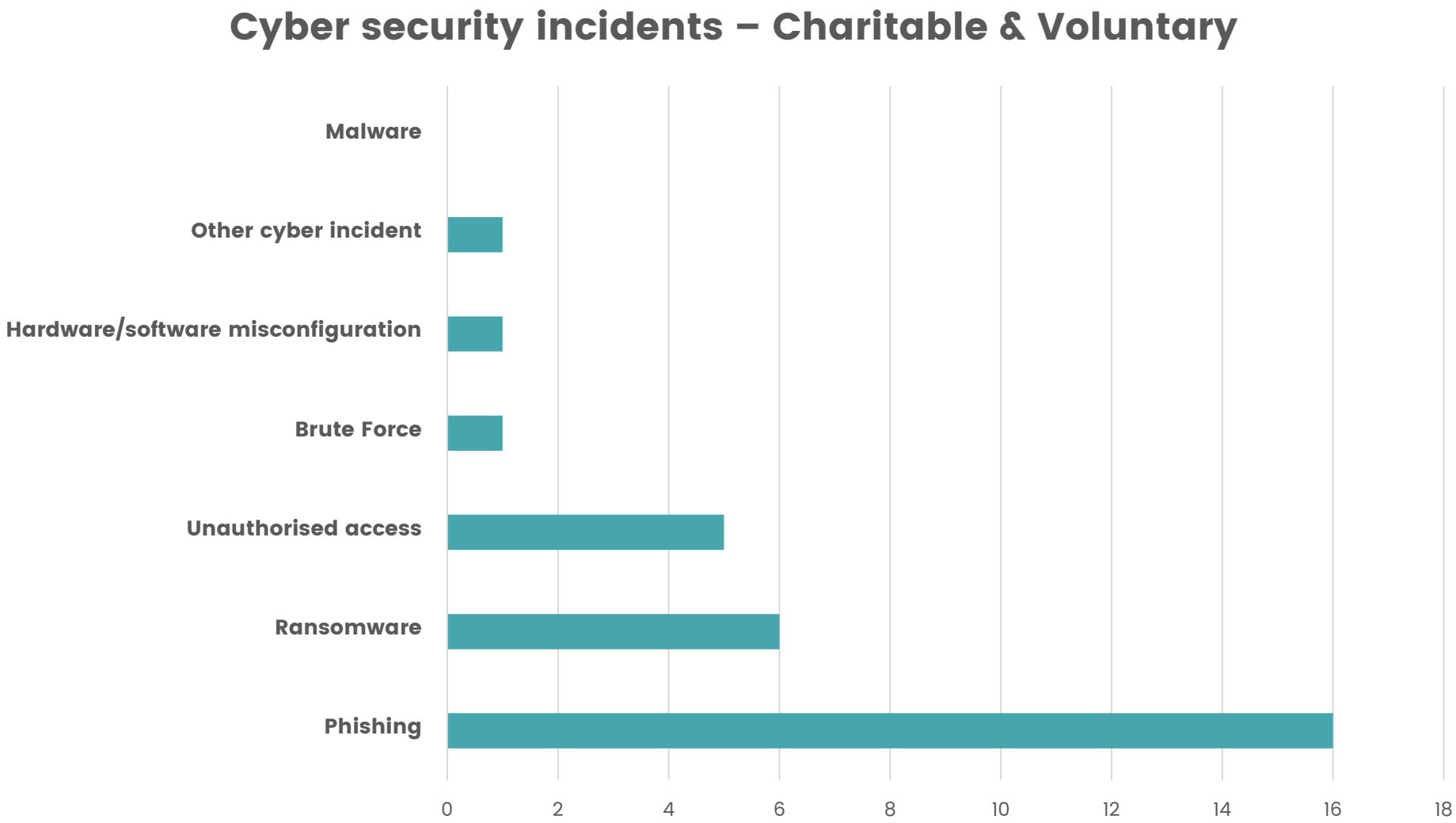
- ✓ **Make sure your staff are adequately trained**
  New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.

- ✓ **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.

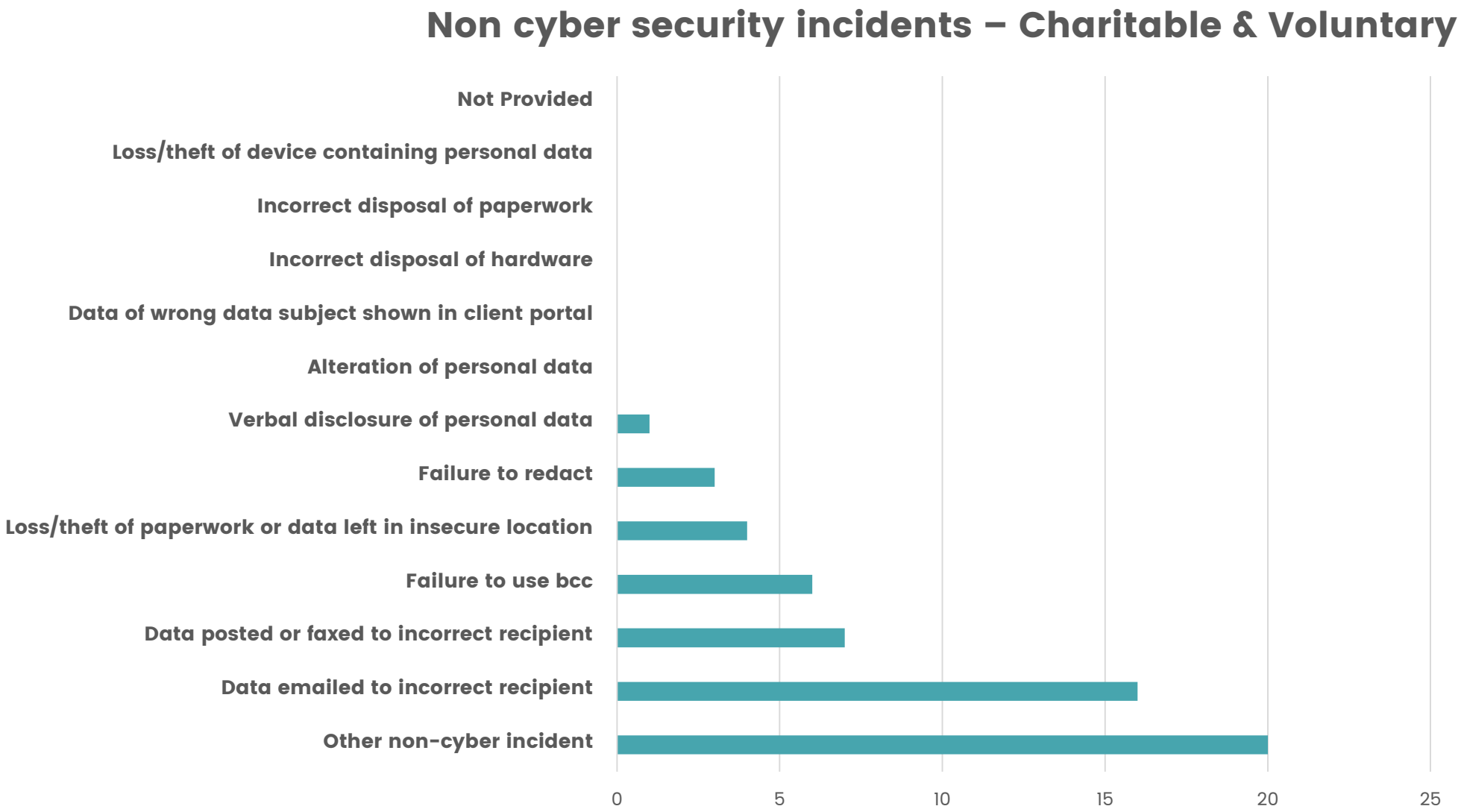
- ✓ **Encrypt all portable devices**
  Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

- ✓ **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.

ICO Data security incident trends – Q1 2020



ICO Data security incident trends – Q1 2020



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.

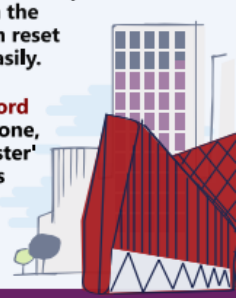
Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

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.



Research ethics

Research Ethics

- ✓Sampling
  - ✓Who?
  - ✓Why?
  - ✓Where?
- ✓Information
  - ✓What?
  - ✓Why?
  - ✓How?
- ✓Consent
- ✓Sharing

Scenario

Your organisation supports asylum seekers through one of your projects and you want to find out how they feel about living in the local community and how this is linked to their well-being and access to services.

You also work with other organisations in your area and you want to ask them about the support they can offer to this group, their levels of knowledge and ability to support your clients.

You know that some of the asylum seekers in your project have experienced some barriers and negative attitudes from other organisations.

Group 1

You are conducting the research with organisations. Given the background above think about:

- ✓How would you choose who to interview (construct your sample)?
- ✓What information would you need to provide? What might participants be concerned about?
- ✓Would individual interviews or focus groups be more useful? What might be the advantages and disadvantages of each?
- ✓What would you need to consider about your own position as a researcher, how you are perceived? How might this influence the responses?
- ✓How could you make participants feel comfortable and gain their trust?

Group 2

You want to speak to people who are going through, or have recently gone through, the asylum system.

- ✓What might be the difficulties with this?
- ✓What might participants be concerned about if they participate?
- ✓What might help them feel more comfortable, trust the process?
- ✓What information would be important for you to provide?

Issues to consider

- ✓Trust
- ✓Accessibility
- ✓Power
- ✓Avoiding 'leading' questions, using a framework
- ✓Researcher 'interference'
- ✓What isn't being said? Why?

Data sharing

#DatawiseLondon

Intended & unintended consequences

Case study: You support refugees and asylum seekers with a range of services. To better understand the needs of these communities in London, the GLA requires data on who you serve, which locations & clients specific requirements.

- ✓What are the potential consequences?
- ✓The positive & negative
- ✓The intended and potential unintended
- ✓How can we mitigate negative consequences?

10 minutes in Breakout rooms

Positive consequences

- ✓Enable better targeting of services
- ✓Sharing of where to go for support
- ✓Help identify gaps: geographically & service provision
- ✓Data for campaigning
- ✓Support creation of services
- ✓Better showcase your work
- ✓Could reduce repetition (for service users)

Negative consequences

- ✓Data used for politics
- ✓Impact on service users - deportation, loss of financial support etc
- ✓Loss of trust / reputation of charities or community groups
- ✓Reduction in numbers of people accessing services
- ✓More data sharing - an increased chance of data breaches?

- ✓https://doteveryone.org.uk/project/consequence-scanning

Mitigating negative consequences

- ✓Have clear, unambiguous written purpose for the use of the data
  - ✓What are the benefits & risks for charities / organisations & service users?
- ✓Don't share identifiable data
  - ✓Anonymisation can be hard – you may need trusted support to do this
- ✓Be clear on who else the data will be shared with
- ✓Beyond ethical principles - need a legally binding contract that stops personal data being used for tracking. **Is this possible?**

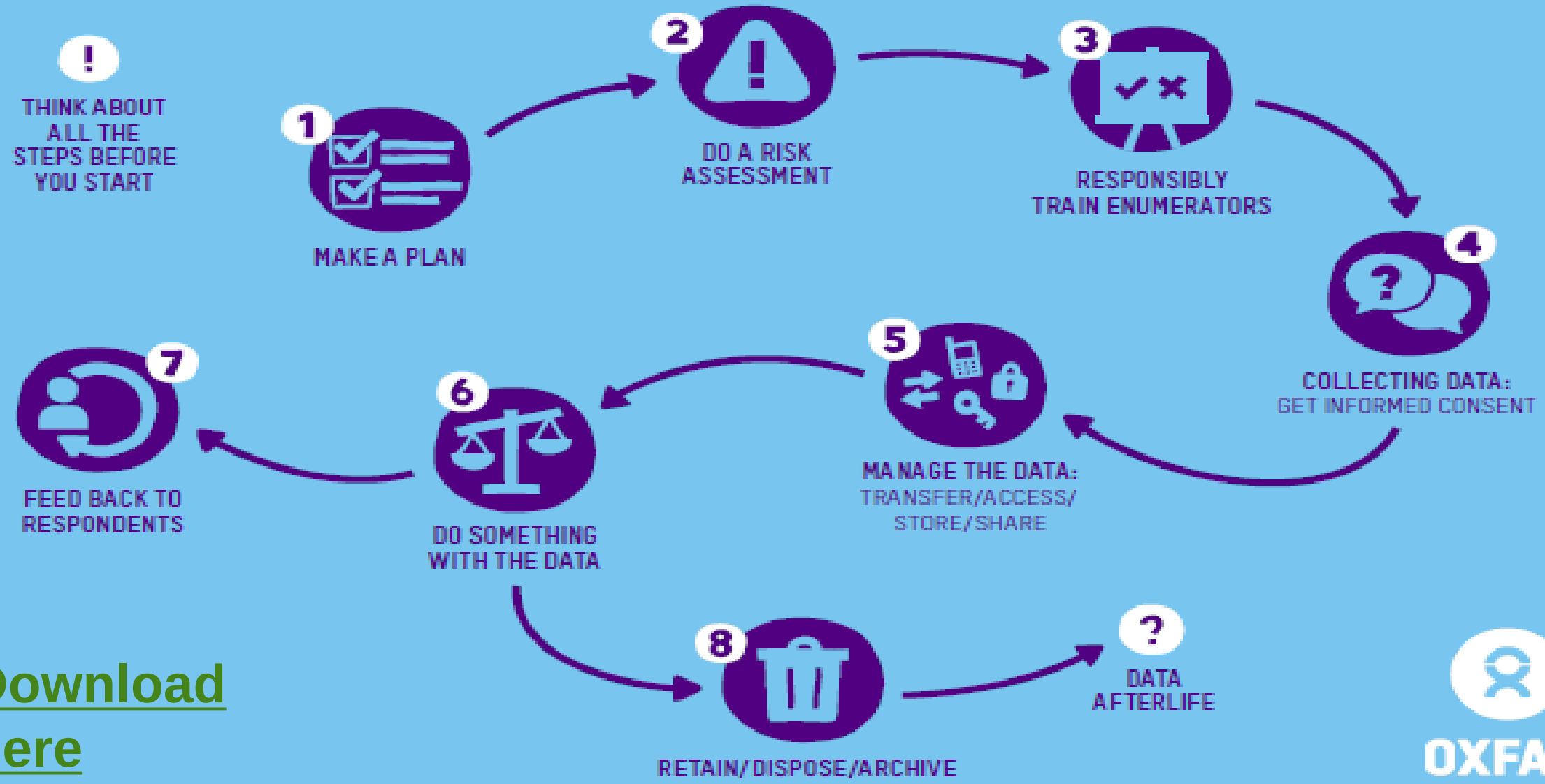
Responsible data lifecycle

#DatawiseLondon

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



[Download here]

OXFAM

Data Ethics Canvas

2019-05

Data sources

Name/describe your project's key data sources, whether you're collecting data yourself or accessing via third parties.

Is any personal data involved, or data that is otherwise sensitive?

Limitations in data sources

Are there limitations that could influence your project's outcomes?

Consider:

- bias in data collection, inclusion/exclusion, analysis, algorithms
- gaps or omissions in data
- provenance and data quality
- other issues affecting decisions, such as team composition

Sharing data with others

Are you going to be sharing data with other organisations? If so, who?

Are you planning to publish any of the data? Under what conditions?

Ethical and legislative context

What existing ethical codes apply to your sector or project? What legislation, policies, or other regulation shape how you use data? What requirements do they introduce?

Consider: the rule of law; human rights; data protection; IP and database rights; anti-discrimination laws; and data sharing, policies, regulation and ethics codes/frameworks specific to sectors (eg health, employment, taxation).

Rights around data sources

Where did you get the data from? Is it produced by an organisation or collected directly from individuals?

Was the data collected for this project or for another purpose? Do you have permission to use this data, or another basis on which you're allowed to use it? What ongoing rights will the data source have?

Your reason for using data

What is your primary purpose for collecting and using data in this project?

What are your main use cases? What is your business model?

Are you making things better for society? How and for whom?

Are you replacing another product or service as a result of this project?

Communicating your purpose

Do people understand your purpose – especially people who the data is about or who are impacted by its use?

How have you been communicating your purpose? Has this communication been clear?

How are you ensuring more vulnerable individuals or groups understand?

Positive effects on people

Which individuals, groups, demographics or organisations will be positively affected by this project? How?

How are you measuring and communicating positive impact? How could you increase it?

Negative effects on people

Who could be negatively affected by this project?

Could the way that data is collected, used or shared cause harm or expose individuals to risk of being re-identified? Could it be used to target, profile or prejudice people, or unfairly restrict access (eg exclusive arrangements)?

How are limitations and risks communicated to people? Consider: people who the data is about, people impacted by its use and organisations using the data.

Minimising negative impact

What steps can you take to minimise harm?

How could you reduce any limitations in your data sources? How are you keeping personal and other sensitive information secure?

How are you measuring, reporting and acting on potential negative impacts of your project?

What benefits will these actions bring to your project?

Engaging with people

How can people engage with you about the project?

How can people correct information, appeal or request changes to the product/service? To what extent?

Are appeal mechanisms reasonable and well understood?

Openness and transparency

How open can you be about this project? Could you publish your methodology, metadata, datasets, code or impact measurements?

Can you ask peers for feedback on the project? How will you communicate it internally?

Will you publish your actions and answers to this canvas openly?

Ongoing implementation

Are you routinely building in thoughts, ideas and considerations of people affected in your project? How?

What information or training might be needed to help people understand data issues?

Are systems, processes and resources available for responding to data issues that arise in the long-term?

Reviews and iterations

How will ongoing data ethics issues be measured, monitored, discussed and actioned?

How often will your responses to this canvas be reviewed or updated? When?

Your actions

What actions will you take before moving forward with this project? Which should take priority?

Who will be responsible for these actions, and who must be involved?

Will you openly publish your actions and answers to this canvas?


DATA
SCIENCE:
A GUIDE FOR SOCIETY

The 3 questions to ask:

Q1. Where does it come from?

Q2. What assumptions are being made?

Q3. Can it bear the weight being put on it?

DigiSafe

- ✓A step-by-step digital safeguarding guide for charities designing new services or taking existing ones online

- ✓https://digisafe.thecatalyst.org.uk/

Becoming more Datawise

- ✓ Complete our session evaluation
- ✓ Register for Datawise London support
- ✓ Check training opportunities on our Eventbrite page
- ✓ Sign up to our eNews