GDPR & IT Security – Overview & Policies

Nov 2018 www.superhighways.org.uk

about Superhighways

Providing tech support to the sector for 20 years

- Support
- Training
- Consultancy
- Digital inclusion

impactaloud
monitor | evaluate | communicate

- E-news sign up

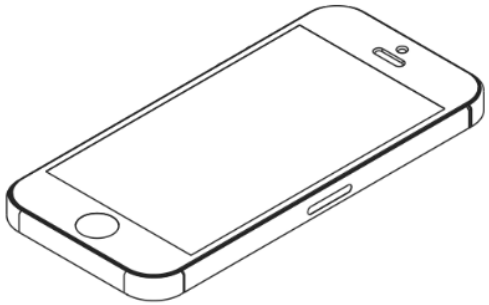
https://superhighways.org.uk/e-news/

Over to you…

Session objectives

- ✓ Overview of the GDPR
  - Principles
  - Legal basis for processing
  - Accountability requirements
- ✓ IT security best practice
  - Checklist of security basics
  - Review current practice
  - Identify actions
- ✓ Review and update relevant policies
  - Data protection policy
  - IT security policy
  - Privacy policy

Go to **www.menti.com** and use the code **44 03 52**

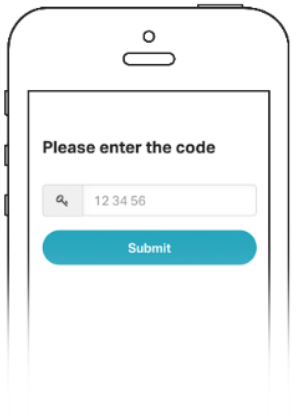


1

Grab your phone

2

Go to www.menti.com



3

Enter the code **23 45 26** and vote!

Current relevant legislation

- Freedom of Information Act – 2000
- Privacy, Electronic & Communications Regulation (PECR) – 2003 *
- General Data Protection Regulation (passed in 2016 but enforceable from May 25th 2018)
- UK Data Protection Bill (came into act in May 2018 too)

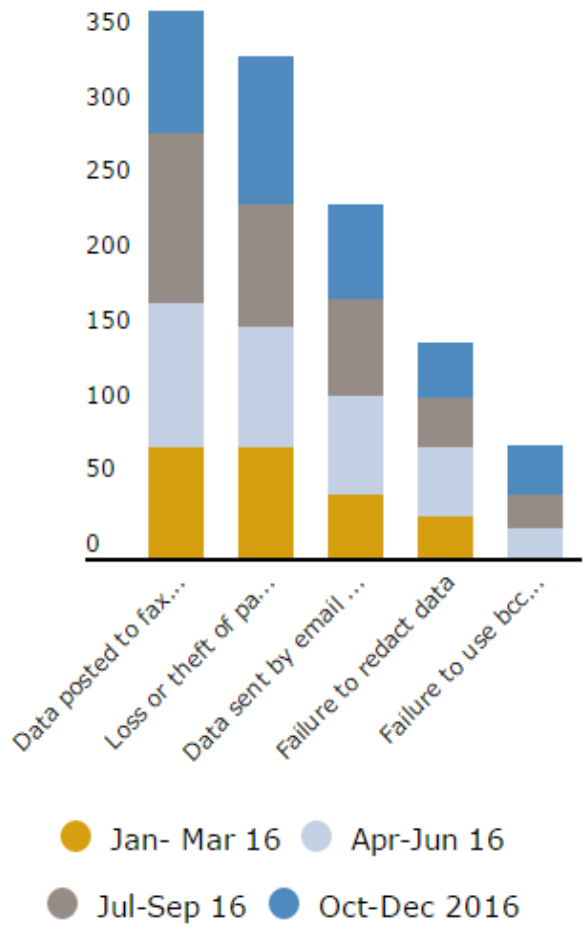
** E-privacy Regulation (coming soon - was due to launch with GDPR)*

Why should we comply?!

- Prevent harm to the individuals whose data you hold
- Reassure people that you use their information responsibly
- Comply with specific legal requirements
- Information Commissioner's Charity Guidance
- ICO's Data Protection Self Assessment – Controllers Checklist

The total number of reported incidents decreased by 3.5% in Q3

Data security incidents by type



43% increase in failure to use bcc when sending an email

22% increase in loss or theft of paperwork

This was partly due to a 41% increase in the health sector.

12% increase in failure to redact data

Data breach by historical society

Date **11 November 2016**

Type **Monetary penalties**

The ICO has fined a historical society after a laptop containing sensitive personal data was stolen whilst a member of staff was working away from the office. The laptop, which wasn't encrypted, contained the details of people who had donated artefacts to the society. An ICO investigation found the organisation had no policies or procedures around homeworking, encryption and mobile devices which resulted in a breach of data protection law.

British Heart Foundation

Date **09 December 2016**

Type **Monetary penalties**

Sector **Charitable and voluntary**

British Heart Foundation secretly screened millions of their donors so they could target them for more money, a comprehensive ICO investigation has found.

British Heart Foundation monetary penalty notice

Action we've taken

PDF (3.22MB)

The Alzheimer's Society

Date **07 January 2016**
Type **Enforcement notices**
Sector **Charitable and voluntary**

The ICO has found serious failings in the way volunteers at a national dementia support charity handled sensitive personal data.

It has ordered The Alzheimer's Society to take action after discovering that volunteers were using personal email addresses to receive and share information about people who use the charity, storing unencrypted data on their home computers and failing to keep paper records locked away.

Furthermore, volunteers were not trained in data protection, the charity's policies and procedures were not explained to them and they had little supervision from staff.

The Alzheimer's Society enforcement notice
Action we've taken
PDF (106.78K)

Warning for workers after charity employee is prosecuted for data protection offences

Date **08 November 2017**

Type **News**

People working with personal information have been warned they have to obey strict privacy laws after a charity worker was prosecuted for making his own copies of sensitive data.

Robert Morrisey, 63, sent spreadsheets containing the information of vulnerable clients to his personal email address without the knowledge of the data controller, his employer the Rochdale Connections Trust.

> "People have a right to expect that when they share their personal information with an organisation, it will be handled properly and legally. That is especially so when it is sensitive personal data.
>
> "People whose jobs give them access to this type of information need to realise that just because they can access it, that doesn't mean they should. They need to have a valid legal reason for doing so. Copying sensitive personal information without the necessary permission isn't a valid reason."

ICO action taken:

- Audits, advisory visits & overview reports listings
- Findings from ICO information risk reviews at 8 charities – April 2018

What is 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"*

The GDPR covers the processing of personal data in two ways:

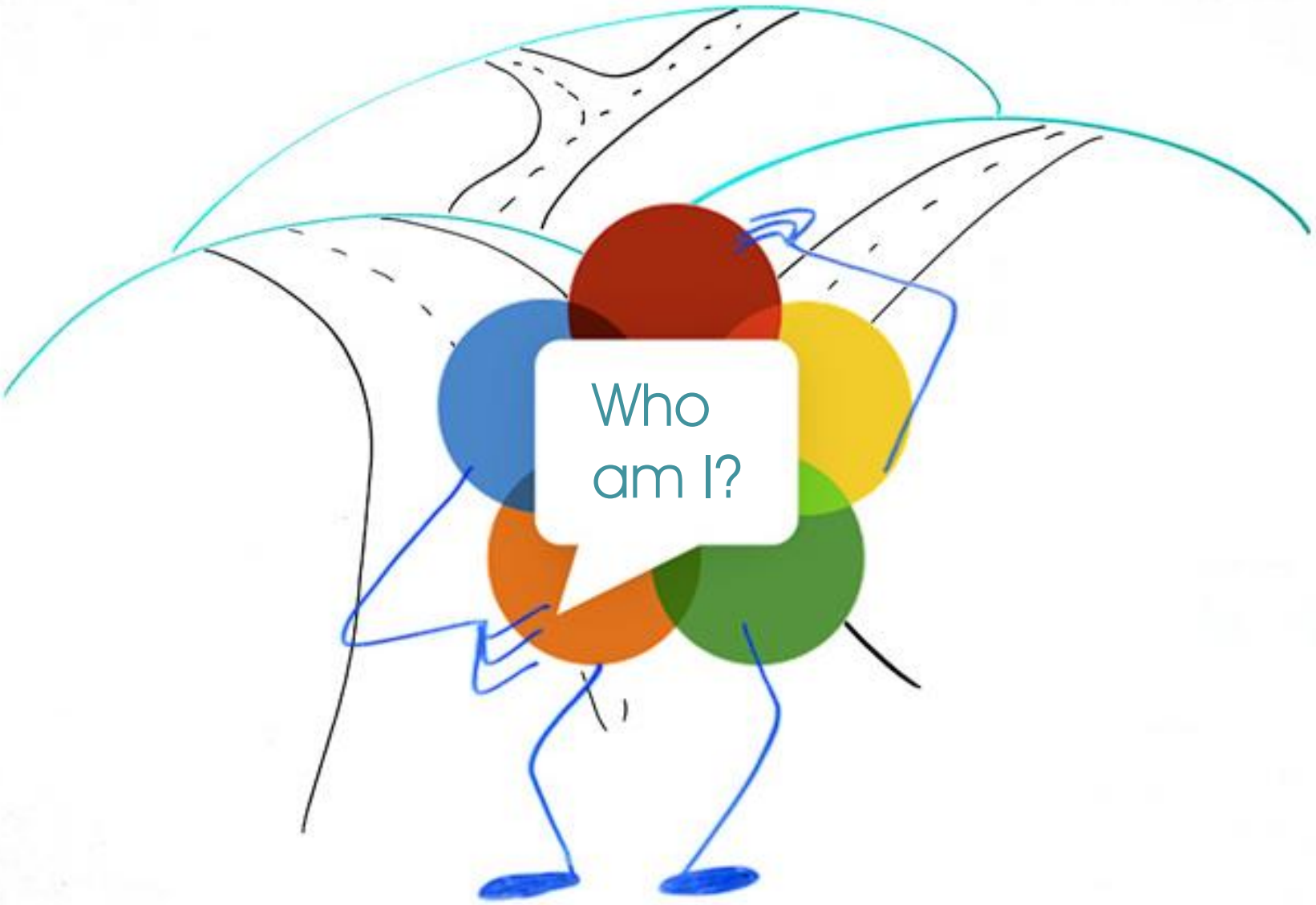
- personal data processed wholly or partly by automated means (that is, information in electronic form)

- personal data processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is, manual information in a filing system)

Special categories

(previously Sensitive Personal Data)

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation


Who
am I?

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

Data processing…

- How are you processing personal data?

Also there's a [Data protection self assessment – getting ready for GDPR]

Getting ready for the new UK data protection law

Eight practical steps for micro business owners and sole traders

ico.
Information Commissioner's Office

1. **Know** the law is changing – which you now do, so that's one thing you've done already!
2. **Make sure you have a record** of the personal data you hold and why.
3. **Identify** why you have personal data and how you use it.
4. **Have a plan** in case people ask about their rights regarding the personal information you hold about them.
5. **Ask yourself: before I collect their data**, do I clearly tell people why I need it and how I will use it?
6. **Check your security.** This can include locking filing cabinets and password-protecting any of your devices and cloud storage that hold your staff or customers' personal data.
7. **Develop a process** to make sure you know what to do if you breach data protection rules.
8. **Don't panic: we're here to help.** For example, you can click here to see some frequently asked questions and their answers for several different business sectors.

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?

- If your data processing is based on legitimate interests – be careful about extending your use beyond the original purpose

Legal basis for processing personal data

- Review different types of data processing you carry out, identify legal basis & document this

- Need to explain legal basis in privacy notices & when answering subject access requests

Action *– be sure you know and can justify the basis of all your processing especially if relying on legitimate interests*

Consent

- Review how you are seeking, obtaining & recording consent
- GDPR references consent & explicit consent (especially re 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
- GDPR clear that Controllers must be able to demonstrate consent was given

Action *– identify whether any of your current processing is based on assumed consent and stop – unless you can get consent OR have another legal basis for the processing*

Action *– review all the statements where you ask people for consent, to ensure that they are clear and unambiguous*

Action *– make sure that record keeping systems you use have the capacity to record details that consent has been given*

Document..

- Who consented
- When they consented
- What they were told at the time
- How they consented
- Whether they have withdrawn consent (& if so, when)

See the ICO Consent Checklist for further info

Children & young people

- Start thinking about putting systems in place to verify individual's ages. UK Gov intends to set the age limit at 13 for online services
- Ensure you are gathering parental or guardian consent in order to process children's data lawfully if they are under 16
- Ensure your privacy notice is written in language that children can understand

Organisational Accountability

Raising awareness

- Update trustees, staff & volunteers
- 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 organistions you've shared data with about an inaccuracy which needs correcting

Action *– carry out an information audit*

Communicating privacy information

- Review current privacy notices *(what you tell people when you collect their personal data e.g. your identity + how you intend to use their data)*
- GDPR requires additional things to 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

Action *– document what you do with personal data and the draw up a full privacy statement*

Transparency & choice

Privacy options code of practice and checklist

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 Controller)
- A trading company, even wholly owned, would be a separate Controller
- Two or more organisations can be joint Controllers of the same data

Processor

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

Individuals rights

- Main rights: (similar to previously + enhancements)
  - Subject access
  - Have accuracies corrected
  - Have information erased 'right to be forgotten'
  - Prevent direct marketing
  - Prevent automated decision-making & profiling
  - Data portability

- Check procedures & how you would react if someone requested e.g. deletion

Subject access requests

- Timeframe has changed – from 40 days to a month
- Most cases – you won't be able to charge (unless unfounded and excessive)
- If you are going to refuse a request – you'll need policies & procedures to justify this
- One option – consider developing systems allowing people to access their information easily online?

Data breaches

- Develop procedures to detect, report and investigate a personal data breach
- GDPR brings in a breach notification duty across the board (i.e. all organisations) within 72 hours
- But 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 – see further information

Action *– ensure all staff (and volunteers) know that whilst mistakes can happen, failing to report a breach (or potential breach or near miss) immediately to the relevant person in your organisation will be treated as gross misconduct*

Data Protection by Design & Default

- ICO gives guidance on Privacy Impact Assessments e.g. linking to risk management & project management processes (compulsory if high risk to rights & freedoms)

- Privacy by design and data minimisation approach was always Data Protection best practice - GDPR makes this an express requirement

Action *– make sure DP incorporated as a matter of course e.g. a standard check point before any new project / system signed off*

Data Protection Officers

- Certain situations where organisations required to appoint a DPO e.g. public bodies or where large scale processing (most charities unlikely to meet this)
- Allocate someone to take responsibility for data protection compliance
- Where does this sit within your organisational structure & governance?

International

- Probably not applicable!

BUT

- You need to be aware of rules on transferring data abroad

Action *– note the new requirement for Data Subjects to be informed if their data is being transferred abroad. Make sure you know where all your data is being stored or processed.*

Cloud computing

- Due diligence with any 3rd party 'data hosting' service / application
- Is there an option for data to be stored in the EU?
- Check policies & compliance
  - Privacy policies
  - Security statements
  - EU US Privacy Shield?

Key security measures

- **Protect data in transit**
  - passwords, encryption on USB devices & laptops
  - extreme care when faxing and emailing
  - care of confidential documents
- **Network security** – anti-virus, firewall, log-ons etc
- **Website security** – particularly re online transactions
- **Access controls** - clear desks, locked filing cabinets
- **Secure destruction** – shredding & wiping discs
- **Staff reliability** - checks, supervision, monitoring
- **Third party contractors** – due diligence checks (Data Processors)

NCSC Small Charity Cyber Security Guide

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?

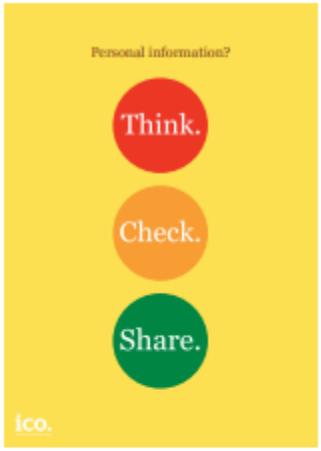
Using passwords to protect your data

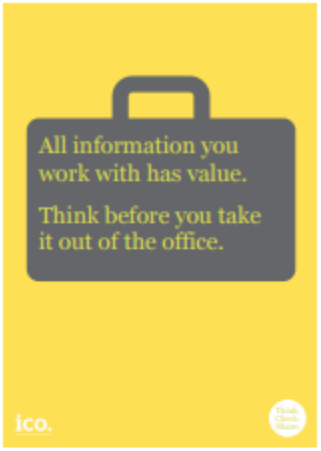
Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

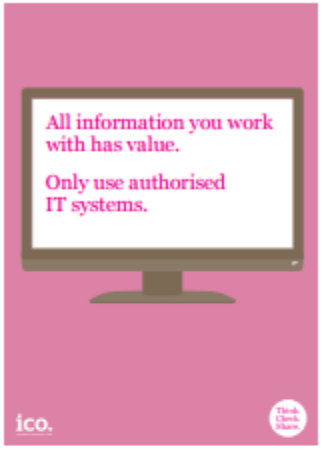
- Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **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.

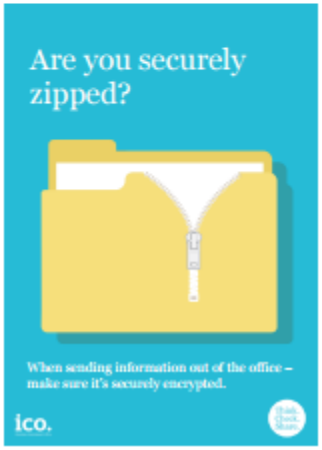
For more information go to www.ncsc.gov.uk @ncsc

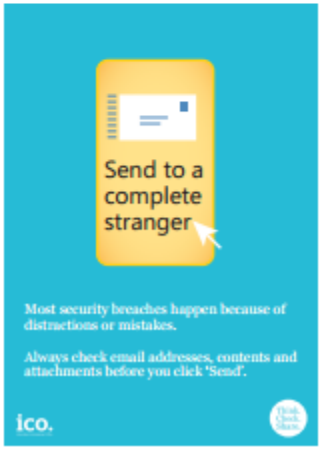
Think. Check. Share toolkit

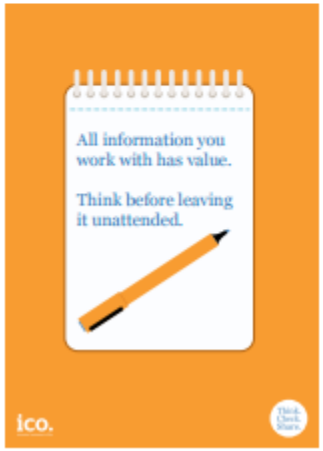


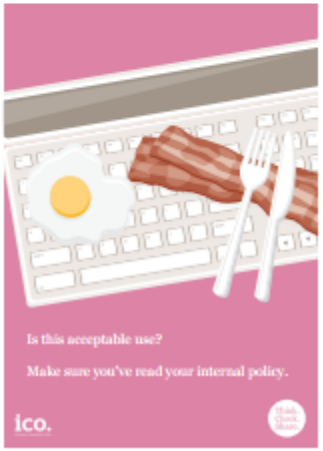


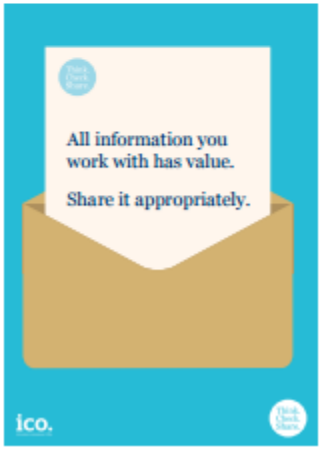












ICO's 5 top tips for small charities

- **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.

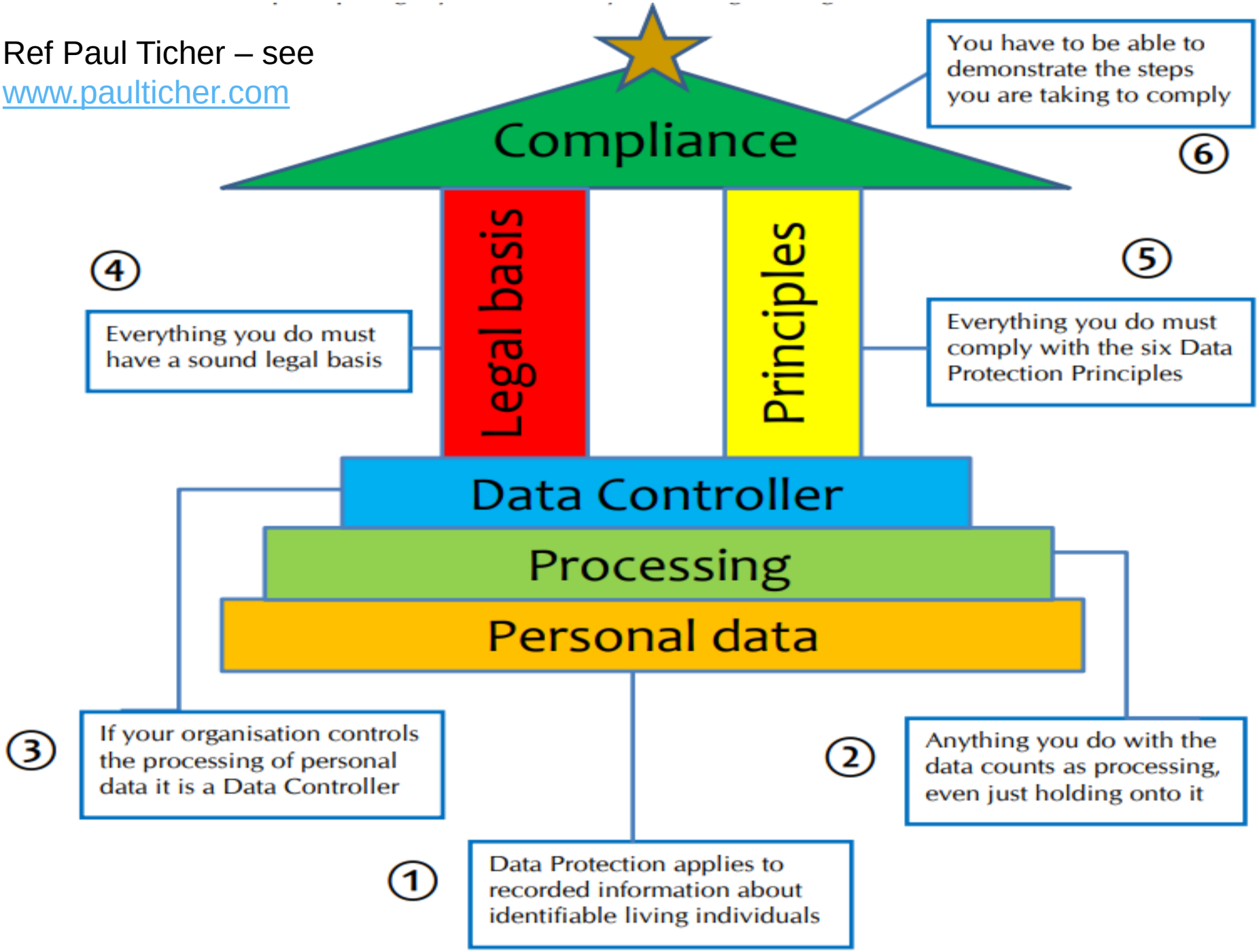
- **Make sure your staff are adequately trained**
  New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.

- **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.

Ref Paul Ticher – see
www.paulticher.com



superhighways

harnessing technology for community benefit

Useful GDPR links

impactaloud@superhighways.org.uk

Tel: 020 8255 8040

www.superhighways.org.uk

@SuperhighwaysUK