

**MINUTES OF A MEETING OF THE PARISH COUNCIL LIAISON MEETING
HELD AT 6.30PM ON WEDNESDAY 18 JULY 2018
COUNCIL CHAMBER - TOWN HALL**

MEMBERS PRESENT:

Councillor I Walsh (Chair)	Peterborough City Council
Councillor A Ellis	Peterborough City Council
Parish Councillor N. Boyce	Castor Parish Council
Parish Councillor I Allin	Orton Longueville Parish Council
Parish Councillor R Clarke	Wansford Parish Council
Parish Councillor K Lievesley	Ufford Parish Council
Parish Councillor S Lucas	Bainton and Ashton Parish Council
Parish Councillor H Clark,	Peakirk Parish Council, Chairman - CAPALC
Parish Councillor J Bartlett	Thorney Parish Council
Parish Councillor J Stannage	Wansford Parish Council
Parish Councillor D Magnus	Eye Parish Council
Parish Councillor H Brassey	Barnack Parish Council
Parish Councillor M Palmer,	Barnack Parish Council
Parish Councillor J Howard	Hampton Parish Council
Parish Councillor J Merrill	Bretton Parish Council
Parish Councillor V Moon	Werrington Neighbourhood Council
Parish Councillor M Samways	Ailsworth Parish Council
Parish Councillor J Hill	Deeping Gate Parish Council
Parish Councillor S Hudspeth	Deeping Gate Parish Council
Parish Clerk A Hankins	Peakirk Parish Council
Parish Clerk L George	Deeping Gate Parish Council
Parish Clerk J Haste	Glington Parish Council & Castor Parish Council
Parish Clerk A Hovell	Thorney Parish Council
Parish Clerk C Franks	Bainton and Ashton Parish Council

OFFICERS PRESENT:

Ben Stevenson	Data Protection Officer
Jawaid Khan	Head of Community Resilience and Integration
Sylvia Radouani	Community Capacity Officer & Parish Co-ordinator
David Beauchamp	Democratic Services Officer

ALSO PRESENT:

Ian Dewar	County Executive Officer - CAPALC
-----------	-----------------------------------

1. APOLOGIES FOR ABSENCE

Apologies for absence were received from J. Dobson (Helpston), J Hayes (Co-opted member on the Adults and Communities Scrutiny Committee, Bretton), P Thompson (Deeping Gate), G Smith, Werrington, S Carney (Barnack), D Batty (Glinton) and all of the Orton Waterville Parish Council.

2. MINUTES OF THE MEETING HELD ON 14 MARCH 2018

The minutes of meeting held on 14 March 2018 were agreed as a true and accurate record.

3. GDPR

The Data Protection Officer delivered his presentation which provided an overview of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 and how this would affect parish councils in particular. The full presentation may be found in Appendix 1. Areas discussed in the presentation included:

- Why has the law changed?
- A recap on the nature of personal data
- The 'Headline' changes of the new legislation
- Principles of Data Protection
- Rights
- What has happened to consent?
- When consent is inappropriate.
- Key things to consider for consent
- Recording and managing consent
- When may you need consent?
- Consent statements
- What if consent is not the right thing?
- Sensitive Information
- Keeping people informed about how their data is used.
- Rules for handling data breaches
- Incidents vs. Breaches
- Types of Incidents?
- First steps in dealing with incidents and breaches.
- What do we need to know about the incident or breach
- Rights of the data subject in the event of a breach
- Managing fault and blame
- Accountability
- Action Plan for Parish Councils to become compliant
- The Information Commissioner's Office (ICO)
- What data do you hold and why?
- Data Protection Policies
- What's in a Privacy Notice?
- I.T. Security
- Contracts
- Holding personal information securely

The Chairman thanked the Data Protection Officer for his presentation and asked the County Executive Officer of CAPALC to recommend what actions Parish Councils should take as next steps in light of the presentation.

- The County Executive Officer stated the Parish Councils are regarded by the Information Commissioner's Office as being relatively low risk in terms of the amount of data held.
- Parish councils could face considerable difficulties if an incident took place without being familiar with the legal background concerning the data protection legislation. CAPALC would employ a Data Protection Officer (DPO) as a shared resource for member councils at a low cost.
- A clear pathway must be followed after an incident to determine whether a breach had occurred and consult with a Data Protection Officer if necessary.
- Some mistakes were expected.

- An incident was not the fault of the parish clerk as they were an employee. It would be the responsibility of the Parish Council.

The Chairman asked for examples of what was classed as a data breach. The County Executive Officer of CAPALC invited the Data Protection Officer to respond:

- Care should be taken when calling something a 'breach'. Historically, Peterborough City Council had taken great care to record all incidents which resulted in Big Brother Watch listing Peterborough as the fourth-worst council in the country for data protection breaches. In reality, Peterborough was the fourth most honest authority with many authorities not recording any incidents.
- A Google Search for data breaches would reveal suitable examples.
- An example of a data breach from Peterborough City Council was as follows;
 - 10 documents relating to one child were sent out and the envelope also contained information about another child. This was reported to the ICO, procedures were followed correctly and the Council was not fined. This was classed as a breach because something was distributed to the public that should not have been seen and the Council was unable to contain it.
 - Other reported breaches largely involved sensitive social and health care records.
- An example of an incident that would not be classed as a breach.
 - On the same day as a presentation to school clerks, administrative staff failed to use the Blind Carbon Copy (BCC) function in an email allowing all recipients to see each other's email addresses. As they were all professional people involved in the same area of work, with 50% knowing each other's email addresses anyway, this was not classed as a breach due to the low risk.
- Councillors should have an instinctive feeling for the risk level of particular data. The data must have an impact on somebody to be a breach e.g. threaten their reputation, create financial issues, identity theft etc.
- The County Executive Officer of CAPALC stated that one of the simplest examples of a breach would be publishing a person's name in parish council minutes, in case they could be identified. Only a person's name, address and data of birth would be required to clone a person's identity.

The Chairman invited attendee's questions. The Parish Council Liaison Committee debated the presentation and in summary, key points raised and responses to questions included:

- Having listened to the presentation, Councillors stated that they were confident that very little of the data held by parish councils was of a personal nature.
- If collectively listed as the data controller, the Parish Council would have liability
- A deliberately committed breach would be a criminal offence and all liability would rest on the individual perpetrator. Many insurers would not cover the council in the event of a deliberate breach by an individual and Councillors were advised to check the wording of their policies. The key point was whether a person is acting on behalf of the council or not.
- The County Executive Officer stated that all Parish Councillors and Council Clerks had been given official email addresses and information sent out via this route was the responsibility of the corporate body of the council and it is this body that would be covered as long as the email address was being used correctly. This was not the case if personal email addresses were used.
- The Data Protection Officer stated that he had been unable to find a single example of an individual councillor being fined. The Information Commissioner's Office tended to target whole Councils. The only example of a Councillor being prosecuted by the

ICO that could be found occurred when information was intentionally deleted following a Freedom of Information request.

- There had been examples of whole councils being fined, e.g. when a councillor forwarded an email incorrectly and this was the responsibility of the council as a whole.
- If a Councillor needed to share information given to them by a resident, they must have been clear with the resident about who they were sharing it with or why. Residents should be explicitly asked if a councillor has their permission to share their information.
- It was highlighted that councillors may have several different roles and could be representing the Council, residents or their political party. It must therefore be made clear in what role the member was acting in as the information recipient and why the resident chose to share the information with them specifically. A resident might not want the information to be shared with anyone else.
- An example was given about an issue with a footpath. In this instance, there would be no need to share the resident's details. Other members would only be interested in the issues pertaining to the footpath itself or might have been approached by another resident about the same issue.
- There are some exceptions in the legislation when consent is not required but these were written in an ambiguous way.
- Councillors should think about what they are being asked and ask the provider of the data for permission if it needed to be shared
- Members expressed concern about the new regulations and suggested that templates were needed, e.g. for privacy notices. The County Executive Officer stated that the organisation used by CAPALC to provide the data protection officers would be providing them with documentation that Councils require to help them become compliant with the legislation. This would take place over the next three to six months.
- Parish Councils had been given some leeway by the Information Commissioner's Office to implement the new regulations. The ICO viewed the first year as being an opportunity to help organisations comply and they themselves were still working on interpreting the implications of the new legislation.
- There was no case law for the new act.
- Privacy notices tended to be similar across organisation and were fairly simple to write.
- If Councillors followed a framework for complying with the new legislation and use the support of other parish members or a Data Protection Officer, then compliance would be achieved.
- Contractors of public sector organisations should expect that the details of contracts, with the exception of some confidential information, were shared with the public as this was required by law. The consent of the contractors would not be relevant in this instance.
- The County Executive Officer of CAPALC stated that the release of the above information would be a part of the 2014 Transparency Code and the Tender Process. The release of this information was a requirement and not a breach.
- An individual had the right to make a complaint about data shared about themselves to a parish councillor, the data protection officer or direct to the Information Commissioner's Office. Typically, a notification would be received from the ICO that a complaint had been made and the council asked to respond.
- Decisions made by a council would not be overturned in the event that there had been a data breach as part of the process. However, it would be undesirable to have a controversy surrounding a data breach at the same time that an important decision was being made
- Councillors asked for extra information about what needed to be done regarding setting up and managing email distribution lists, which are often used by parish

councillors to distribute information to residents. The Data Protection Officer stated that it must be clear where a person's email address was obtained from and a record of them signing up must be kept. It must also have been made clear to the data subject how their data would be used. Emails should make it clear that a recipient could unsubscribe at any time, either via an automatic link or by inviting them to send an email to say they no longer wished to be on the list.

- Mailing lists should be refreshed at regular intervals. There was no fixed interval although the Data Protection Officer advised schools to do so every school year.
- Some organisations were not clear how to respond to the new legislation, hence the large number emails asking for people's consent to remain on their mailing list before the 25th May.
- If an organisation's mailing list had been built carefully, there should be no concerns. Recipients should know what they had signed up for it, e.g. a person's email address should not be taken from another list used for another purpose for use on a mailing list. It should also be clear to the recipient how to stop receiving the emails.

4. CAPALC SERVICES

The Chairman of the Board of the Cambridgeshire and Peterborough Association of Local Councils (CAPALC) presented this item alongside the County Executive Officer of CAPALC.

- The Chairman of the Board stated that he had attended three GDPR meetings and had developed some suggestions:
 - Parish councils must take action and be seen to be doing something.
 - Parish councils should register with the Information Commissioner's Office. It would cost £40 and showed positive intent.
 - A resolution should be passed at the next meeting of a parish council stating that the Council would take steps to become compliant with GDPR.
 - A plan should be developed over the next 12 months taking into account the data held, the reason for the data being held, how long it was held for etc.

If progress is seen to be made towards becoming compliant, a parish council should be 'safe'. The Information Commissioner's Office would not target a council for enforcement in this circumstance and if they did, only a warning would be issued on the first occasion. Wilfully ignoring this warning would result in heavier punishment and after this, potentially a fine. This would be unlikely to happen to a Parish Council.

- CAPALC were negotiating with a data protection company to provide support to parish councils who wished to sign up. The Chairman of the Board invited the County Executive Officer to discuss this in more detail:
- A minimum cost would be set to provide support to a Parish Council when they suspected an incident had occurred. Support would be provided to help a council through the process and identify the severity of the incident.
- If this incident became a breach, a Data Protection Officer would negotiate with the Information Commissioner's Office on the council's behalf if required to reduce the severity of the impact of their decision.
- Parish Councils would be looked on fairly and reasonably by the ICO because, despite being elected officials, parish councillors undertake this work voluntarily. A parish council could still encounter trouble if it continues to make the same mistakes however.
- CAPALC's task over the 6-12 months following the meeting was to get councils to follow the route towards compliance, work with those councils who were struggling to help them through to ensure a breach does not occur and if it does, to support them through the process of dealing with it.
- There would be a considerable amount of work for the Clerk or a council member to go through information held to determine its validity to either keep and record or

shred and destroy as appropriate. Having produced a summary of the information held, a council could begin to identify risk going forward.

- Some documentation was already available from the Society of Local Council Clerks (SLCC) although the company that CAPALC intended to use would provide their own documents. If a council filled in these documents and encountered a problem, the company would have a solutions package ready to implement which would save time.
- CAPALC could provide two locum clerks if a council needed extra support for as long as required although the existing clerk might need to do the work relating to data. Locum clerks would be covered by CAPALC's insurance. CAPALC are also aiming to provide auditing services. It was important to go through data in more detail at the internal audit stage to ensure that councils are compliant with government requirements. CAPALC are trying to tie these services up and provide a better package for councils.
- The Chairman stated that the information presented should be made available to those parish councils that did not have representatives at the meeting.

ACTIONS AGREED:

The Community Capacity Officer and Parish Coordinator would distribute the presentation slides to all parish councils.

5. CO-OPTED MEMBERS NOMINATIONS

The Chairman introduced the item and it was noted that members of Parish councils were entitled to be co-opted onto Peterborough City Council's Scrutiny Committees to participate in discussions. The Chairman noted the positive contributions made by these members and read out a list of members. The feedback session was abandoned due to lack of time and feedback would be sent to attendees via email. The members were as follows:

Health Scrutiny Committee: Henry Clark - Peakirk. Barry Warne (substitute) - Orton Waterville

Growth, Environment and Resources Scrutiny Committee: Keith Lievesley - Ufford, Richard Clarke - Wansford

Adults and Communities Scrutiny Committee: Neil Boyce - Castor, James Hayes - Bretton

Children and Education Scrutiny Committee: Susie Lucas - Bainton & Ashton, Junaid Bhatti - Bretton

The Chairman thanked the co-opted members for their work and contributions to the scrutiny committees. This was an excellent opportunity for parish councillors to ask, challenge and understand in more depth the business of Peterborough City Council and how this was related to parishes.

The Community Capacity Officer asked if the co-opted members could inform parish councillors how they could take forward their concerns. It was agreed that parish councillors should direct questions to the co-opted members once their feedback had been circulated via email. The Parish Council Liaison Committee would then see how that item was taken forward.

ACTIONS AGREED:

1. Parish council non-voting co-opted members of scrutiny committees would distribute their feedback to parish councils via email.
2. Parish councillors would direct any questions to the co-opted members once their feedback had been circulated. This committee could then assess how this points had been taken forward in the future.

ANY OTHER BUSINESS

The Chair invited the Community Capacity Officer to provide more details about the Parish Conference. It was to be held on the 15 November 2018 at the Allia Future Business Centre. The programme would be distributed in the week following this meeting. The conference was open to everybody. It would be held in one space, the conference room, and a working lunch would be held halfway through and not at the end. Key speakers would include Andy Gipp - Head of Policing for Peterborough, Rob Hill - Assistant Director of Community Safety (Peterborough and County), Parish Councillor Neil Boyce, and a representative of the fire brigade.


The Chairman stated that the conference would be focussed around community safety, police priorities, the expansion of city council's Prevention and Enforcement Service and grassroots community initiatives. Everyone was encouraged to attend.

- 6. DATE OF NEXT MEETING:**
19 September 2018

6.30pm to 8.07pm


CHAIRMAN

APPENDIX 1: PRESENTATION SLIDES FROM ITEM 3



Data Protection

Fun*



Why has it changed?

The world has changed a lot since the last data protection act in 1998.

The spread of the internet has meant more personal data is collected quicker and easier than ever before.

In May 2018, the General Data Protection Regulation has come into force alongside a new Data Protection act. These will bring changes to data protection.

Quick Recap...

Using personal data has an impact on privacy through how we use it, store it, collect it and destroy it.

There is always a controller who determines how and why data is processed. Processor is responsible for that processing. In some cases, you will be both.

Personal Information means any information which identifies a person such as name, address, email address, IP address, identification numbers.

Special Categories of Information used to be called sensitive personal data and includes ethnicity, politics, trade union, health, genetics

The Headlines

- a. Increased focus on compliance
- b. More visibility of processors
- c. Increased transparency
- d. Updates personal data for a digital world
- e. Increased focus on the right of privacy
- f. Greater rights for subjects
- g. Increased enforcement powers
- h. Addressing globalisation



Principles of Data Protection

1

You collect and use information lawfully and fairly

2

You collect and use information for specific purpose

3

You only collect and use the information you need

4

You keep information accurate and up to date

5

You only keep information for as long as is necessary

6

You keep information secure and prevent loss or damage

RIGHTS

The Right to be Informed

Explain to people what we are doing with their data in a clear and concise way.

The Right of Access

Provide a person's own data for free and ask them to specify what they want

The Right to Rectification

A person can ask us to amend data if it is inaccurate or incomplete

The Right to Erasure

A person can ask for information to be deleted in certain cases, for example consent withdrawn or no longer needed

The Right to Restrict

We can be asked to block processing, in certain situations, for example the accuracy is contested or no longer needed

The Right to Data Portability

We should be able to provide data back to people in a way in which they can re-use it but only in certain cases

The Right to Object

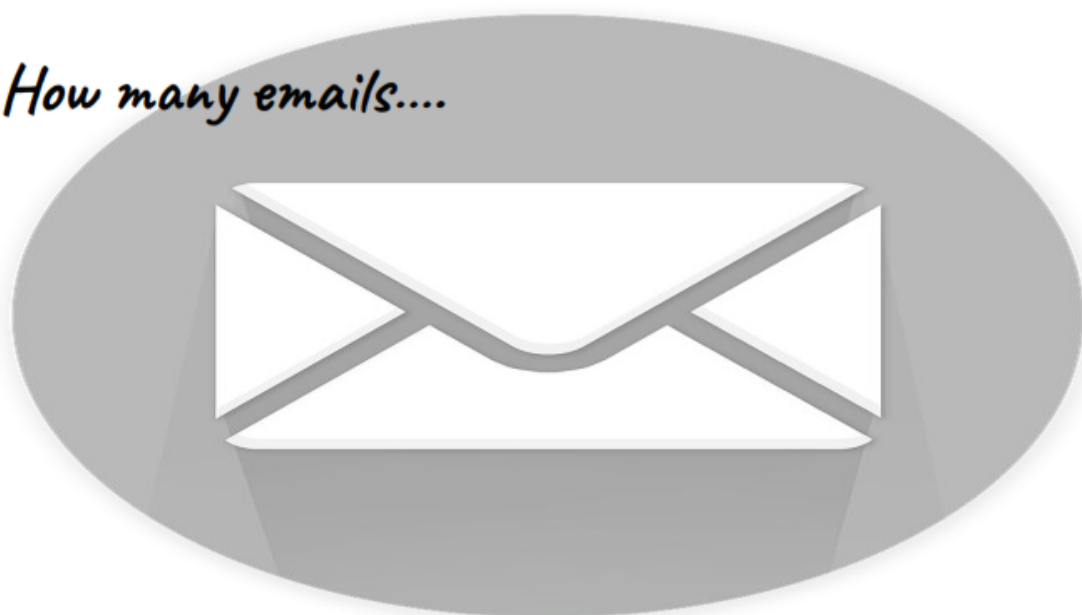
A person can object to processing activities for example those based on public interest or official authority

The Right on Automated Decision Making

We can be asked to make a "human decision" rather than by an automated process. This also applies to profiling.



How many emails....



What has happened to consent?

We are getting a higher standard for consent

It is an opt in. Not an opt out

Consent is not a precondition to a service

It offers a real choice and is freely given

I Agree

When it is not appropriate...

If you would process
the data anyway

You cannot imply
consent

You cannot
show that it is
freely given

Someone
suffers if they
do not give
consent



UNACCEPTABLE

Key things to consider for consent

- Is it the correct reason?
- Is it a free choice?
- Is it separate from terms and conditions?
- Is it clear what they are consenting to?
- Is it an affirmative action?
- Can they withdraw?

Recording and Managing

- You have a record that you have consent and when you got it and..
what that consent covers
- You review that consent remains valid and does not need amending
- You refresh consent by asking again at appropriate intervals
- You ensure that anyone can withdraw and there is no impact on them

When may you need consent?



Marketing?

Media?

Photographs?

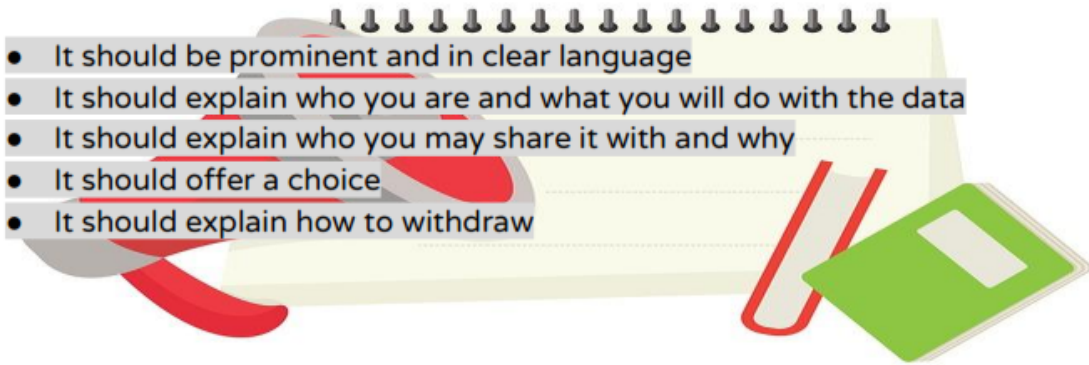
Secondary use?

Research?



A consent statement...

- It should be prominent and in clear language
- It should explain who you are and what you will do with the data
- It should explain who you may share it with and why
- It should offer a choice
- It should explain how to withdraw



What if consent is not the right thing?

Contract

Vital interest

Statutory duties/Public Task

Legal

Legitimate Interests?

Sensitive information

Consent

Vital interest

Social care

Public task

Legal

Occupational Health

What do they sign then?

Whatever you decide then you need to inform people.

When they fill a form in, explain what you are doing and why with a statement.

Link it to and share your online privacy notice.

You are informing, being transparent and engaging with people

Data Breaches



Some rules...

Don't ignore a report

Don't think it is someone else's problem

Don't pretend you don't know

Don't be distracted by it being someone's fault

and...

Don't call it a breach until you have assessed it!

rules



Incident or Breach? Is it obvious?

Incident is something that may have happened

You need to take action but you need to assess it before you call it a breach

Breaches will need to be reported to the ICO within 72 hours.

We'll start by understanding about the kinds of breaches



What types of incidents are there?



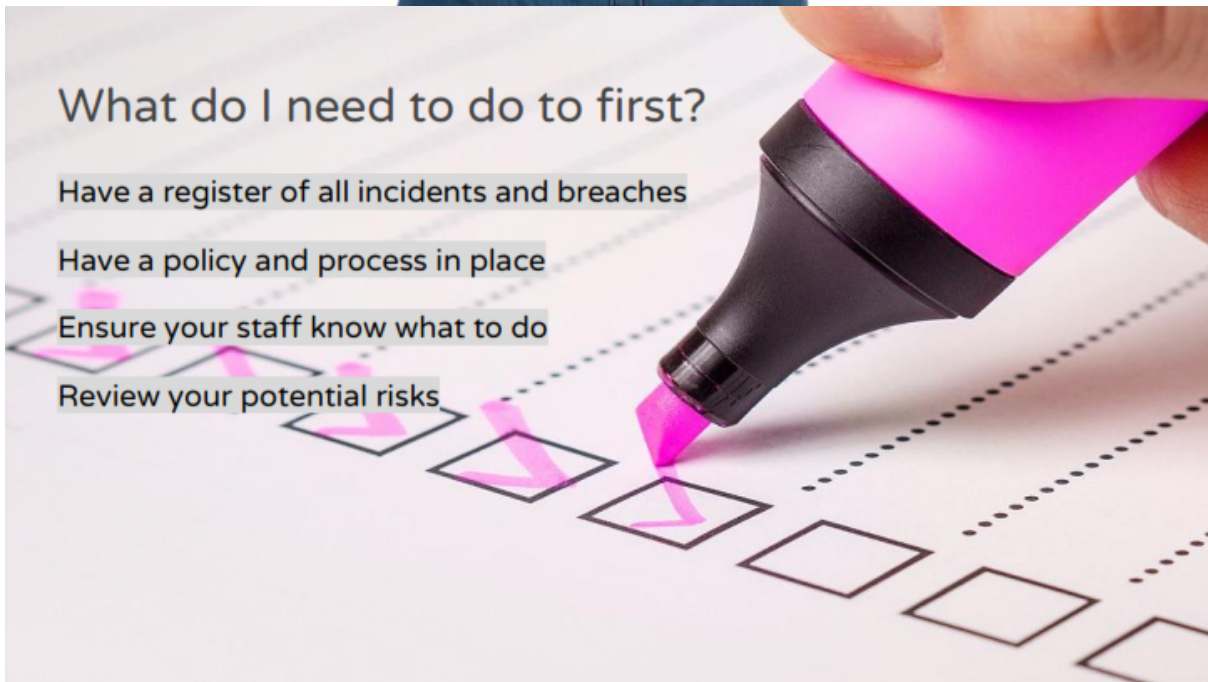
What do I need to do to first?

Have a register of all incidents and breaches

Have a policy and process in place

Ensure your staff know what to do

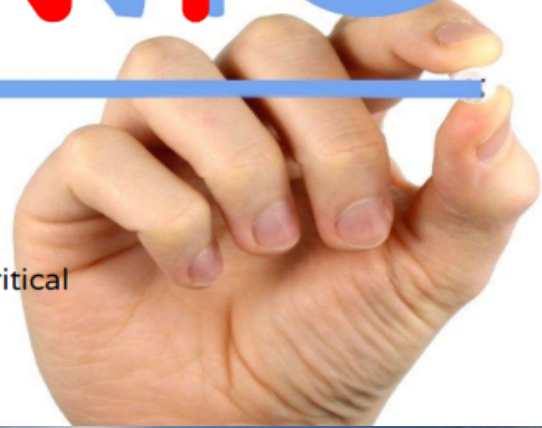
Review your potential risks



PANIC

DON'T

It's not a fun job but your response is critical



First, what do we need to know?

What kind of incident it is?

What kind of data is it?

How sensitive is the data?

How much is there?

What is the impact for individuals?

What kind of individuals are we talking about?

The number affected

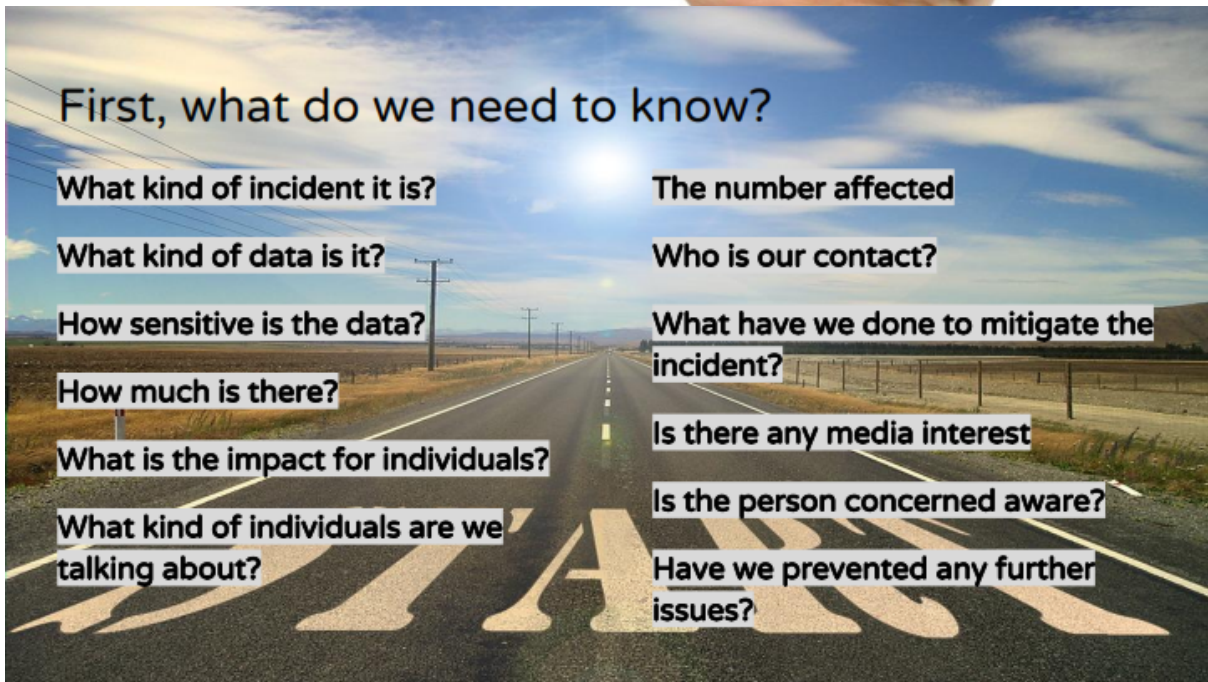
Who is our contact?

What have we done to mitigate the incident?

Is there any media interest

Is the person concerned aware?

Have we prevented any further issues?



What about the data subjects?



If there is a high risk to then we have to inform them

There is specific information we have to tell them

They can take legal action if they suffer

Whose fault was it?

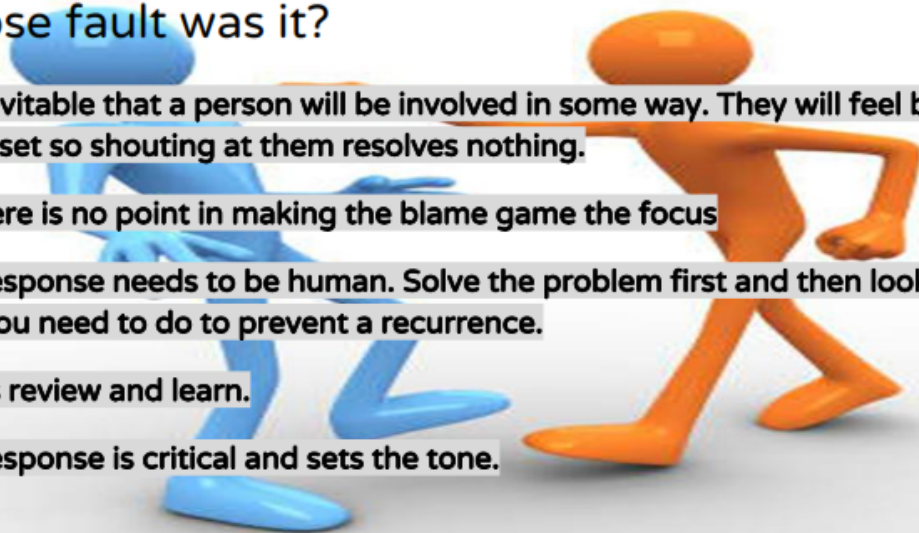
It is inevitable that a person will be involved in some way. They will feel bad and upset so shouting at them resolves nothing.

But there is no point in making the blame game the focus

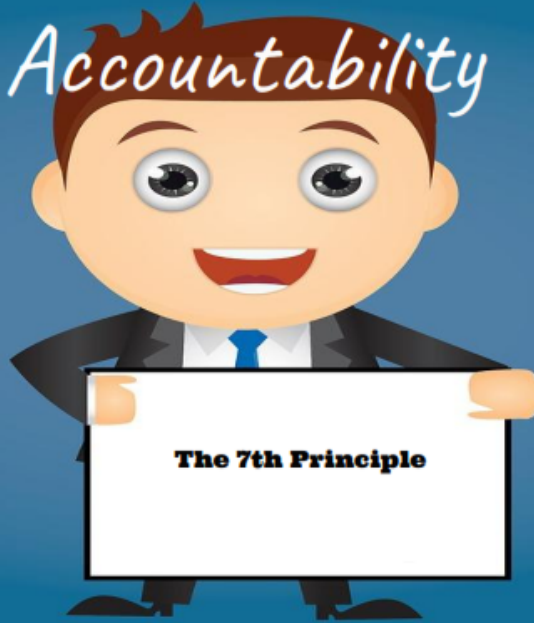
Your response needs to be human. Solve the problem first and then look at what you need to do to prevent a recurrence.

Always review and learn.

Your response is critical and sets the tone.



Accountability



Action Plan



The Information Commissioner

ico.

Information Commissioner's Office

The Information Commissioner's Office (ICO) oversees the UK's data protection regime. They are also the regulatory body for Freedom of Information and Privacy & Electronic Communication Regulations.

You need to be registered with the ICO.

What do you hold? and why?

You need to create a list of what information you hold and it can be a spreadsheet but it should list at a general level:

- Who you hold information about?
- What kinds of information you hold?
- Why you have the information?
- Who do you receive it from?
- Who you may share it with?
- Where you store it?
- How long you keep it for?
- Your reason for having that information



POLICY

Data Protection policy including Special Categories/Criminal Data

Data incident policy

Privacy by Design

Information/ICT Security

Information Sharing

Retention Schedule



What's in a Privacy Notice?

The identity of the controller i.e. yourself

What you are collecting, why, who you will share with and who may provide you with data

What is the basis for the processing, e.g. consent, statutory duty

How long you will keep information for

How to access their rights

It is kept securely and if any information is transferred outside of the UK or EU

The right to complain to the ICO

IT Security

Are your systems/networks protected and tested?

Do you have protocols to ensure access is restricted?

Do you have auditable systems for access/download?

Do you have secure means of sharing?

Do you have starter and leaver processes?

Contracts

If you contract out work which involves personal data then you need to review those contracts

They need very clear instructions on the use of personal data

You need to make sure that contractor understands and complies with data protection

This is your protection

Personal information is held and handled securely

Make sure you use your encrypted devices, tablets and phones if possible

Make sure you use the correct email addresses

Make sure you password protect files and PCs at home or work. Don't use easy to guess passwords like your name!

Make sure you know who you are talking to and whether you should share information with them

Make sure you think about the information as though it is about you and your family

