CAMBRIDGESHIRE
& PETERBOROUGH
COMBINED AUTHORITY

Data Incident Reporting Policy

Type of document:	Guidance
Document produced by:	Cambridgeshire & Peterborough CA Data Protection Officer
Document approved by:	Cambridgeshire & Peterborough Combined Authority Board
Version :	Version 2
Issue date:	
How is this shared?	Electronically
Date due for review:	Annually April
Reviewer:	

Data Protection Contact		
Contact Details	**Email**	**Phone**
Sue Hall	dpo@cambridgeshirepeterborough-ca.gov.uk	07706 341719

Table of Contents

Introduction

We have to protect the data that we have. We have a lot of data on different customers and staff. This can include personal and sensitive information but also, for example, commercially sensitive information or simply data. We have to have processes in place to do this but sometimes things do go wrong.

When information is lost or shared inappropriately, it is vital that appropriate action is taken to minimise the impact and risk as soon as possible.

"If you only read this…"

Do make sure that you know who you are talking to

Do make sure you only share information with the right person

Do make sure you check envelopes or emails to make sure they have the right information

Do check postal and email addresses before you send

Do know what to do if something goes wrong

Do report any concerns

Don't ignore a breach

Don't ignore a customer complaining about a breach

The important bits

If we get it wrong, then our customers and residents could be at risk

If we get it wrong, then we could be fined the equivalent of £17.5 million or 4% of total worldwide income by the Information Commissioner

If we get it wrong, then people can sue us if they suffer detriment

If we get it wrong, then we have to spend more time fixing the problem then it would have taken to make sure we were not getting it wrong

What is a data breach?

A data breach is something which affects people's rights and freedoms.

When something is reported then we will call it a data incident until we have assessed it as a breach. If we say it is a breach, then it must be reported to the Information Commissioner within 72 hours and if it's a high risk then people whose data it is.

All reports will be considered as a data incident until we can determine the risk to the data subjects.

Near misses should also be reported and recorded in the same way as an actual data breach.

What kind of incidents do you mean?

A data incident is more than if we just lose some information. It can be where:

- personal information is disclosed to someone who does not have the right to see it. It could be documents, a spreadsheet or just an email.
- The loss of information
- The corruption of information
- The unavailability of information
- The data being incorrect

It can be caused by

- Loss or theft of data or equipment on which data is stored
- Deliberate or accidental action by someone
- Not having the right access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood or power cut
- Hacking
- 'Blagging' offences where information is obtained by deception
- Alteration of personal data without permission
- Virus attacks

If there is personal information and/or sensitive personal information as defined in this policy contained within the document, email etc. then this must be reported.

Data could also be disclosed which is not personal but reveals information of a commercially sensitive nature or is confidential. This can also have an impact on us but would not need to be reported to the ICO.

When does it become a breach?

We will consider that all incidents have an element of risk to someone and take the same actions in all cases.

Once we have the facts then we will determine what that level of risk is.

The Data Protection Officer (DPO) along with the SIRO (Senior Information Risk Owner) will determine this. This will include a risk assessment which will cover the following:

- **Whether any personal data has been lost or whether it is a loss of data**
- **The potential harm or risks to the data subject as a result of the incident**, including any distress the data subject may suffer as a result of the incident
- **The volume of the data involved** – this must be determined by the facts and extent of the breach
- **The sensitivity of the data involved** – where the data is classed as sensitive personal data and the release of that data can lead to the data subject suffering substantial harm.

- **Assess the impact of the breach such as:**
  - How could the loss of control over the personal data affect someone?
  - Could it cause discrimination?
  - Could it cause identity theft or fraud
  - Could it cause financial loss?
  - Could it cause embarrassment and upset?
  - Could it cause damage to reputation?
  - Could it cause loss of confidentiality?

The DPO along with the SIRO and Chief Executive will decide if we need to inform the Information Commissioner's Office (ICO) and/or the people concerned. The Data Protection Officer will contact the ICO with all relevant information on the breach as per the section entitled 'Contacting the ICO'.

How do I report something?

Use Appendix A and send this to dpo@cambridgeshirepeterborough-ca.gov.uk.

If it is urgent then phone to speak to the Data Protection Officer on 07706 341719.

If the incident occurs or is discovered outside normal working hours, the investigation and notification of relevant officers should begin as soon as is practicable either by text or email.

What happens after I report something?

The DPO will make an initial assessment based on what they have been told. They, in conjunction with the affecteddepartment, will determine what steps are taken.

Contacting those affected

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must be informed without undue delay (as soon as possible). The Responsible officer should do this when it is decided that people are at sufficient risk.

Roles and Responsibilities

All staff

All of us have responsibility to report a concern. The manager/lead will have responsibility for reporting an incident/breach directly to the DPO and establishing what has happened/informing the DPO of the incident details.

The manager/lead, or someone in their absence, should take immediate action to recover any documents, whether electronic or hard copy, and put measures in place to prevent future breaches.

The Data Protection Officer

They will maintain a central log of all breaches and near misses as reported and provide advice on actions to be taken.

An investigation will only be undertaken by the DPO when requested to do so by the director or Chief Executive and only in specific circumstances.

In the event of a complaint being made to the ICO, the DPO will act as the collator of information to provide the response

The Affected Department

When an incident occurs then the department affected will undertake an investigation or review. They will nominate an individual to lead on investigating and gathering information which should be at the level of manager or above. We can call them the **Department Lead.** Their role helps to add background and context to an incident that only someone from the department can give. They will need to gather information on what has happened and liaise with the DPO to determine what actions should be taken.

The Department Lead

The Department Lead will be responsible for any communication with data subjects who have been affected by the data breach. Any response must be checked by the DPO, responses should be as quickly as possible and no later than 10 working days. The department will initiate disciplinary action / provide supervision or training if required (as appropriate)

Contacting the ICO

Once we decide this then the DPO or deputy will complete the referral.

A notifiable breach must be reported by the DPO or the deputy to the ICO without undue delay, but not later than 72 hours after becoming aware of it. The 72 hour clock starts from the moment that a breach has been determined. If 72 hours lapses, reasons for the delay must be given.

When reporting a breach, the following must be provided:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

It may not always be possible to investigate a breach fully within 72 hours, The ICO must be informed within the 72 hours but the required information can be given in phases, as long as this is done without undue further delay.

Breaches we need to notify the ICO about

When a personal data breach has occurred, the likelihood of the risk to people's rights and freedoms needs to be established. If a risk is likely, you must notify the ICO; if a risk is unlikely, you don't have to report it.

Complaints about breaches

Sometimes customers make complaints about data breaches to a central complaints team or as part of a wider complaint about a department. The DPO should be made aware of such complaints however the department should take the responsibility for investigation and review as they would in any event,and liaise with the DPO on the response to this aspect of the complaint.

Complaints officers must ensure that they inform the DPO of any suspected incident as soon as they become aware of it to ensure that we can still meet our timescales.

Information to be provided to individuals when telling them about a breach

You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of any data protection officer you have, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

If possible, you should give specific and clear advice to individuals on the steps they can take to protect themselves, and what you are willing to do to help them. Depending on the circumstances, this may include such things as:

- forcing a password reset;
- advising individuals to use strong, unique passwords; and
- telling them to look out for phishing emails or fraudulent activity on their accounts.

Putting it right for good

Regardless of whether there was a risk or not, we have to make sure that we do not repeat mistakes.

We need to look at the processes and systems which may have caused the incident and work out what we can do to stop it repeating.

This may mean:

- Reviewing how information is held and shared
- Looking at what extra security checks we can put in place
- Introducing peer checks of envelopes
- Providing extra training on systems
- Raising awareness through meetings
- Restricting access and auditing systems, implementing technical and organisational measures, e.g. disabling autofill.

The DPO will assess the risks, impact, changes needed and discuss the implementation of changes with the Department Lead. The DPO and the Department Lead will ensure that change is implemented to prevent repeats.

How does the DPO assess impact and risk?

The impact of the breach will be assessed by the DPO using the Impact assessment. We will look at the following kinds of questions:

Was any data lost or compromised in the incident? For example, if paperwork was in the wrong envelope or the email went to the wrong person. However, if you lost an encrypted laptop or phone then there may not be an issue unless you were logged in when you lost it.
Was personal data lost or compromised? This means is the data about living individuals such as customers or employees. This makes a data protection incident.
If yes, was sensitive personal data compromised? This is the really sensitive stuff like health, sexual life, political or religious beliefs, potential or actual criminal offences. If this happens then it is more serious.
What is the number of people whose data was affected by the incident? Large numbers of people affected can be more serious but equally a very sensitive piece of information about one person can also be serious.
Is the data breach unlikely to result in a risk to the individual/individuals? This means is anyone unlikely to be affected; this means that although data has been lost, it is unlikely to have an affect if we can recover the information or contain the issue.
Did people affected by the incident give the information to the authority in confidence? People often do expect it to be confidential even if it is not particularly sensitive
Does this incident put anyone at risk of physical harm? If it does then this makes it a more serious matter because we have to make sure customers and employees are kept safe
Is there a risk that the incident could lead to damage to individuals e.g. via identity theft/ fraud? If we lose bank accounts details or ID documents, then these could be used by to commit crimes.
Could the incident damage an individual's reputation, or cause hurt, distress or humiliation e.g. loss of medical records, disciplinary records etc.? Even if the loss does not put them at risk of physical harm or fraud, it can still cause distress if information about a person is made public. It can cause upset and hurt which we need to consider properly
Can the incident have a serious impact on the authority's reputation? The authority has to keep the trust of its customers. If we don't then they may stop working with us. Media stories can also cause this as can referrals to the ICO.
Has any similar incident happened before in the section? A one-off error may be unavoidable but repeated incidents of the same kind in a department can show that we have to change processes to stop repeats.
Do HR need to be involved or referred to? This is maybe because the issue is one of capability, or because of deliberate and malicious actions to cause the breach.
If this incident involves the loss or theft of IT Equipment has an urgent call been logged with ICT? The sooner we can block or wipe the device, the better.

Monitoring and Review

Post-breach review

A review of the breach should take place to discuss the details of the breach: why it happened, what impact it had, what actions were taken to resolve it, how the team can prevent it from happening again and any lessons learnt. The review should take place about 2-3 weeks after the breach.

There will be a quarterly report to the Data Protection Officer and an annual report to the CA Board.

This will inform training and risk assessments.

This policy shall be reviewed annually after implementation.

Appendix A – Data Incident Reporting Form

Once completed, please send a copy to dpo@cambridgeshirepeterborough-ca.gov.uk and retain a copy for your records.

	To be completed
Reported by	
Responsible officer	
Department	
Date and time of when the incident occurred	
Date and time reported to DPO	
Date and time you become aware of the incident	
Reason for delay if any	
Does this incident affect any other parties?	
How did you become aware of the incident?	
What kind of incident is this?	

How many individuals could this incident affect?	
Subject names and details	
What kind of people are affected?	
Are these people aware?	
Ease of identification of individuals	
Type of data lost	
Summarise the incident and the information that has been lost	
Actions Taken by department to mitigate, recover etc.	
What impact does this have on the individuals involved? What is the risk to them?	
Risk to subjects	
What is the impact on the authority and its business?	
Temporary or Permanent Loss	

Please complete the following checklist to confirm what actions you have taken:

Have you informed your director? (include name of director)	
Has an extensive search for any physical loss been undertaken?	
Have you been able to retrieve the lost data?	
Has the lost data been destroyed?	
Have you reviewed procedures to prevent recurrences?	
Is there likely to be media interest as a result?	