Country Trust
Where children learn and grow

Data Breach Procedure (read in conjunction with CT detailed Guidelines Data Breach)

Below is the guidance from the ICO with regard to the actions that an organisation should take following a Data Breach/or suspected Data Breach.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within **72 hours** of becoming aware of the breach, where feasible.

Don't Panic, you know it has happened so you are already taking control of the situation.

There are 4 things you need to have in mind when starting to deal with a breach situation:

1. **Containing the breach and recovering from the impact**
2. **Assessing the risk**
3. **Deciding who you need to inform**
4. **Learning from the incident**

The lead for a Data Breach situation with be Country Trust's Data Officer in conjunction with the CEO and our expert IT volunteer. It is important that there is a point of contact for staff, any data subject and the ICO if necessary**.**

Containing the breach

The Data Officer can advise on steps to take to contain the breach, for example, changing passwords, shutting down computers or halting network traffic.

They can also put safeguarding in place and for example provide instruction and authorisation to restore data from backups if that's possible.

They should also be thinking about who will need to be informed, including ICO, the data subjects, industry regulators or the police.

Risk assessment

A breach can impact business transactions and your staff's ability to work, it can also harm your reputation, but remember the risk in a personal data breach is to data subjects.

Think about how this breach could cause these people harm.

How sensitive is the data?

Could this breach lead to distress, financial or even physical harm?

Are there any safeguards in place that could lower the risk? For example, is the data encrypted? Has it gone to a trusted body?

Are there more safeguards you can put in place now?

The GDPR brings in a requirement to report a personal data breach to the ICO unless you can demonstrate it's unlikely to result in a risk to individual rights and freedoms.

If there is a high risk to individuals' rights and freedoms you will need to notify them. In fact, the ICO may require you to.

Notification – informing the ICO

During office hours you can call their specialist team on :

0303 123 1113

This is the best way to record the breach as the ICO can work with you to understand what's happened, get all of the information they need and help you with the next steps.

You will be able to explain the breach more clearly, they can ask any questions straight away and discuss how serious the breach is, and then can give advice on measures to take to contain the breach and whether you need to tell data subjects about what's happened. They will send you a copy of their record.

If you need to report and you can't reach the ICCO on the phone, if you already have a written report ready, or you have relevant documentation to send, you can report via ICO's website.

https://ico.org.uk/for-organisations/report-a-breach/

Informing the ICO: what they need from you

The ICO's breach reporting team will be able to discuss the details we require, and don't forget; the GPDR allows you to report in stages.

But the ICO will need a clear summary of what happened and when, and the steps that led to the breach.

- How many people could be affected and how many records? Remember, one person might have multiple records and one record might mention multiple people.
- What type of data has been breached? Is there any sensitive information?
- What did you have in place that could have stopped it?
- Are your staff trained?
- What steps have you taken so far to safeguard the data subjects?
- Are there any more steps you will take?
- They will ask about the policies and procedures you have in place. Are they written down?
- They will also ask whether staff are trained in the processes your organisation uses and if you provide guidance for them that they can use as a reference.
- The ICO will need to know about the security measures you have in place. This might be about password protection or network security, but might also be about locks on doors and cabinets.
- What have you learned from this breach?
- How can you improve your practices?
- What have you done or will you do to stop a similar incident from happening again?

Informing the ICO: what happens next?

In most cases our reporting team will give you recommendations to help you put better measures in place to help prevent similar breaches in the future.

If a breach is serious, complex or involves a cyber incident The ICO may need to carry out an in-depth investigation. They will contact you for more information.

DataBr Procedure
V1.0 May 2018