



CH & Co – Managing Personal Data Breaches

Personal data breaches are one of the key risks for our organisation. They can lead to large fines, costly complaints and claims from individuals and reputational damage. We also need to tell the data protection regulator (the ICO) about some personal data breaches, which we have to do very quickly after the breach happens. If the breach relates to client data, we might also need to tell clients within a certain period of time to avoid breaching our contracts with clients. We're reliant on our employees to tell us when breaches happen so that we can meet these obligations.

So, it's vital that everyone at CH&CO knows what to do if they become aware of a personal data breach. This document gives you the information you need to make sure you can respond and react to a personal data breach in the right way, so that CH&CO can comply with its obligations and reduce the risk of damage to the business and to individuals.

So, what is a personal data breach?

A personal data breach is any **security breach** which leads to **personal data** being **destroyed, lost, changed, disclosed** or **accessed** when it shouldn't have been. "Personal data" means any information we hold about an individual and includes business contact information, e.g. joe.bloggs@chandcogroup.com.

Examples of actual or possible personal data breaches include:

- a hacker getting access to personal data held on our technology system
- sending an email containing information about an individual to the wrong person
- sending a spreadsheet of salary information to the wrong person (including someone else at CH&CO who is not authorised to see that information)
- accidentally including email addresses in the "CC" instead of "BCC" field, if other recipients would not be authorised to see all those email addresses
- a laptop containing personal data being stolen or being left on a train
- our technology systems failing and losing or corrupting personal data
- scams like "phishing" where a fraudster tricks someone into clicking a link that looks legitimate and sharing login details

You can see that this is very wide and includes things that you might not think would be a breach. If you are not sure whether something that has happened is a personal data breach, **it is always best to be cautious and treat it as a personal data breach.**

Version	1	Date	12.10.2023	Issued by	Legal Department
Version	1.1	Date	19.02.2024	Issued by	Legal / IT Department



What should I do about it?

If you think that a personal data breach has happened, or even if you think that one might happen (for example, if you've accidentally clicked on a link that you think might be suspicious but you are not sure), you **must**:

1. **report it immediately to the Service Desk** by:
 - a. firstly, calling 02034113852
 - b. secondly, sending an email to IT@pabulum-catering.co.uk with details of the breach, subject line as : Pabulum Data Breach Incident
2. tell your line manager.

You should tell the Service Desk **everything that you know** about the breach, including:

- what happened, how it happened, when did it happen and when did you become aware? dates and times
- how much personal data is involved and how many individuals could be affected
- what type of personal data is involved and which individuals this affects
- what you've done so far about the breach (see below)
- who else is aware of the breach
- anything else that is relevant.

Even if the breach has happened because of a mistake that you've made, you must still report it. You will not get into trouble because of a simple error, but if you don't report a breach then we risk being fined for not reporting the breach to the regulator, as well as for the breach itself.

Should I do anything else?

If there are things that you can do straight away to reduce the effects of the breach then you should do these. For example:

- if you've sent an email or document to the wrong person, you should try to recall the email, or if that's not possible, ask the person who's received the email to delete all copies of it and confirm that they've deleted it and not sent it on to anyone else.
- if you've left a laptop on a train, you should call the train company to see if it's been handed in and can be collected.

If you are not sure what to do, ask the Service Desk when you report the breach.

What should I do if I have questions?

If you have any questions about personal data breaches or about this document, you should contact the Legal Team at: legal@chandcogroup.com.

Version	1	Date	12.10.2023	Issued by	Legal Department
Version	1.1	Date	19.02.2024	Issued by	Legal / IT Department