Checklist for dealing with data security breaches

A data breach is defined as more than just losing data. It could be a breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. If a breach does occur:

Step	Action/Task	Completed
1	Make an assessment of whether a personal data breach has occurred and how serous it is. Consider the likelihood and severity of the resulting risk to people's rights and freedoms.	
2	If you decide that the breach is not serious enough to report, then make a record of the breach and the rationale for not reporting it.	
3	Decide whether a reportable breach has occurred. Consider whether it is likely that the breach will result in a risk to employees' rights and freedoms (having a negative impact on the employee). If it is then the ICO should be notified. Reportable data breaches might include, when data has been sent to the wrong person, the loss or theft of technology devices, a hack, when data is not retrievable, or has been altered in some way or erased.	
4	Contact the Information Commissioner's Office (ICO) without delay if there is a high risk of employees' rights and freedoms being breached, and within 72 hours of becoming aware of the breach in all other reportable cases. If you don't have all the details within the 72-hour timescale, contact them anyway – you can always update them later.	
5	Provide the following details to the ICO: • A description of the nature of the personal data breach including, where possible: o The categories and approximate number of individuals concerned; and o The categories and approximate number of personal data records concerned • The name and contact details of your Data Protection Office (if there is 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, including, where appropriate, the measures taken to mitigate any possible adverse effects.	
6	If the breach is likely to result in high risk to the rights and freedoms of individuals, inform those concerned as soon as possible, clearly explain: o The nature of the personal data breach o The name and contact details of your Data Protection Officer or other contact point o An explanation of the likely consequences of the breach, and o A description of the measures taken, or proposed, to deal with the breach including, where appropriate, any measures taken to mitigate the possible adverse effects, and	

	○ Any steps recommended to those individuals to protect themselves from the effects of the breach.	
7	Following any personal data breach, review how the breach occurred and whether any steps need to be taken to prevent a recurrence. Document any remedial action taken.	