CHECKLIST BREACH RESPONSE PLAN

Once a Data Breach has been identified, you need to take steps to address what has happened.

		YES	NO
1.	Have we got a plan for data breaches?	☐	☐
2.	Does everyone know about the plan and what their role is/what they can/cannot do?	☐	☐
3.	Do we need to involve any external experts such as cyber security experts, legal counsel, or the police?	☐	☐
4.	Have we secured our systems?	☐	☐
5.	Have we fixed any vulnerabilities e.g. Changing usernames/passwords or access credentials, or updating systems by way of application of necessary patches or new software?	☐	☐
6.	Do we know how the Data Breach occurred? (What happened and who was involved)	☐	☐
7.	Do we know if there's likely to be a risk to the individual(s)' rights and freedoms? (Have you assessed the severity of the impact or the potential impact on the individual(s) as a result of the breach?)	☐	☐
8.	Do we need to notify the JOIC (or any other supervisory authority)	☐	☐
9.	Do we need to notify the Jersey Cyber Security Centre (JCSC)	☐	☐
10.	Do we need to notify the States of Jersey Police (SOJP)/any other law enforcement agency?	☐	☐
11.	Do we need to notify affected data subjects?	☐	☐
12.	Is there anyone else we need to notify such as insurers/third parties subject to a contractual requirement?	☐	☐
13.	Have we filled in our breach log?	☐	☐