This document is purely for guidance and does not constitute legal advice or legal analysis. It is intended as a starting point only, and organisations may need to seek independent legal advice when renewing, enhancing or developing their own processes and procedures or for specific legal issues and/or questions.
Checklist - Preparing for a Personal Data Breach

☐ We know how to recognise a personal data breach;

☐ We understand that a personal data breach isn’t only about loss or theft of personal data;

☐ We have prepared a response plan for addressing any personal data breached that occur;

☐ We have allocated responsibility for managing breaches to a dedicated person or team;

☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

☐ We have in place a process to assess the likely risk to individuals as a result of a breach;

☐ We have a process to notify Jersey Office of the Information Commissioner (the JOIC) of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet;

☐ We know what information we must give the JOIC about a breach;

☐ We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms;

☐ We know where appropriate, we must inform affected individuals without undue delay;

☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects;

☐ We document all breaches, even if they don’t all need to be reported.