Data Breaches: Are You Ready?

This checklist is designed for all business groups to test their readiness. It's the responsibility of the Data Protection Champions (DPCs) to periodically test their teams' preparedness and, if any weaknesses are identified, timely discuss and address them with their Executive management.

Preparing for a personal data breach

- Our colleagues know how to recognise a personal data breach. ☐
- Our colleagues understand that a personal data breach isn't just about loss or theft of personal data. ☐
- Our business group has robust data breach detection, investigation and internal reporting procedures in place to ensure that we can quickly detect a data breach on time and notify it accordingly to the Society's Data Protection Manager (DPM)[1]. ☐
- Our business group has allocated responsibility for managing data breaches to a dedicated colleague or team. ☐
- Our colleagues are aware of the process to report a data breach internally (ie. to the DPCs or the Society's DPM) and have read all the relevant policies to ensure compliance with the Society's guidelines. ☐

Responding to a personal data breach

- Our colleagues understand that, when a data breach occurs, all relevant information regarding the data breach must be communicated to the DPCs, so that a Data Security Incident Reporting Form can be completed and sent to the Society's DPM. ☐
- On becoming aware of a data breach, our business group can quickly establish the root causes and promptly take steps to try and contain its impact on the affected individuals (where possible), and timely notify the Society's DPM, so that they can assess the incident and decide the next steps. ☐
- We understand that, if a personal data breach occurs, we should not contact the affected individuals in the first instance, but let our DPCs, or the Society's DPM know about the data breach, so that the necessary assessment can be made, and further steps taken as deemed appropriate. ☐
- Our business group know that, when a data breach occurs, accurate information must be given to the DPCs so that the Data Protection Incident Reporting Form can be completely adequately, eg. whether or not the data breach was a result of human error or a systemic issue, how a recurrence can be prevented through better processes, further training or other corrective steps. ☐

[1] The GDPR introduced the obligation for certain organisations to formally appoint a Data Protection Officer (DPO). Within the Society, this requirement applies to our Healthcare business. The Society's DPM also covers the DPO role.