MANAGING DATA PROTECTION BREACHES

There are four key steps to the Chambers data protection breach management plan:

1. Containment and recovery
2. Assessment and ongoing risk
3. Notification of breach
4. Evaluation and response

1. Containment and recovery
[INSERT ROLE TITLE] and reporting person must:

   1. Identify what systems have been affected (eg servers, email, broadband, local network, remote access, telephones, practice management system, word-processing and barristers' files, payroll, marketing, mobile devices, backups, remote storage).
   2. Identify the means used to enable the attack to take place.
   3. Take steps to recover any lost data and limit the damage that the breach can cause where possible.
   4. Prioritise the sequence of restoring systems (consider local network, practice management, barristers' files, broadband, email, telephones, remote access, remote backup, mobile devices).
   5. Decide who will lead the investigation into the breach.
   6. Find out who needs to be aware of the breach and tell those persons what they are expected to do (if anything) to assist in the containment and recovery of the breach. Inform Chair of Management Committee and consider informing the Senior Clerk and Head of Chambers.
   7. Consider whether data relating to the intrusion needs to be preserved in a forensically sound manner. If yes, obtain advice from a specialist security consultant on how this should be done (e.g.......... insert).

2. Assess the risks
The person leading the investigation must assess the potential adverse consequences of the breach for the individual concerned (the individuals to whom the personal data in question pertain), the potential severity or scale of the breach and the likelihood of adverse consequences occurring.

3. Notification of breaches
Chambers has a duty to report all data protection breaches that are likely to result in a risk to the rights and freedoms of individuals to the Information Commissioner's Office (ICO).
The [DPO/DPM/HEAD OF CHAMBERS/ SENIOR CLERK], [INSERT NAME], or a suitable deputy in [HIS/HER] absence, is responsible for ensuring that all relevant data protection breaches are reported to the ICO without delay and no later than 72 hours after having become aware of it.
The [DPO/DPM/HEAD OF CHAMBERS/ SENIOR CLERK], [INSERT NAME] will report the breach to the ICO in accordance with the reporting methods set by the ICO.
When the personal data breach is likely to result in a high risk to data subjects, the individuals affected by the data protection breach, must also be informed without undue delay. The investigating person must provide individuals with specific and clear information about what has happened and what is being done to address the breach. Advice should also be offered on any steps that the affected individuals can take to protect themselves. The individuals must be given contact details should they require further information or help.
Consideration must also be made as to whether any other third parties should be notified, including for example the Police, insurers, BSB, CJSM, the bank etc. Consider also informing solicitors, lay clients, factual and expert witnesses, and opposing parties in litigation.

4. Evaluation and response
The final step is to evaluate the Chambers' response to the data protection breach.
It is important to establish whether the breach was caused by an isolated incident or is part of a wider systematic issue, and to identify the steps needed to prevent repetition (including configuration of IT facilities and amendments to policies and procedures).
Any lessons learned should be shared across Chambers as appropriate by communicating the details to the relevant members and staff of Chambers.

The [DPO/DPM/HEAD OF CHAMBERS/ SENIOR CLERK], [INSERT NAME] will review all any records of data breaches periodically to establish any trends requiring further attention.

RECORDING A DATA PROTECTION BREACH

There must be a central record of all data protection breaches that occur. [INSERT NAME & ROLE TITLE] is responsible for maintaining a data protection breach register.