Appendix 12b

Risk Assessment Process for Data Breaches

SMA UK treats Data Breaches very seriously.

- If a Data Breach has occurred a risk assessment should be made immediately and recorded on the Security Breach Notification form. List the threats and calculate the risk associated. This will help advise senior staff on the next steps to take.

The risk assessment approach

1. Firstly, think about the threat events which could impact the confidentiality, accuracy, or availability of the data you are collecting, processing or storing.

2. Next assign a numerical value as listed below.

Highly Probable	5	The event will certainly occur
Probable	4	The event is likely to occur
Possible	3	The event could occur
Unlikely	2	Little chance of the event happening
Highly unlikely	1	Almost no chance of it occurring

3. Then consider the impact of the event

Disclosure of personal details, such as name, address, telephone number, emails, date of birth, gender, medical data, bank details, conversations and any additional data, which could result in a large number data subjects suffering harm, anxiety or identity theft as a direct result of disclosure.	5
Disclosure of personal details, such as name, address, telephone number, emails, date of birth, gender, medical data, bank details, conversations and any additional data, which could result in small number data subjects suffering harm, anxiety or identity theft as a direct result of disclosure.	4
Disclosure of some personal details, such as name, address, emails, telephone number, date of birth, undefined medical data or personal contact of some data subjects	3
Disclosure of name, address, emails, telephone number, date of birth, of some data subjects	2
Disclosure of no more than two personal details, from name, address, emails, telephone number or date of birth of data subjects	1

4. Multiply the Likelihood value by the Impact value to determine a risk score

5. Data Breach – If there is a Data Breach then this figure for each event will help decide further action by senior staff, for instance if the breach needs reporting to the ICO.

Example

A. A laptop has been left on unattended in a public place. A member of the public has witness a stranger placing a data stick into the computer and thought it likely that data was removed. There was spreadsheet on the desktop containing names, address, email address, telephone number and some comments of over 50 data subjects but no medical information or bank details

Event	Likelihood	Impact	Result	Comment
Data has been removed from the computer	5	3	5X3=15	Medium / High risk - This is serious enough to be reported to the ICO. This is as much a precaution due to the number of pieces of data stolen rather than the nature of the data. Although the nature of the comments need to be considered. It is also a breach of policy and data subjects, if known should be contacted. Otherwise a public statement needs to be made.