Platinum
MOTOR GROUP

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your Director or manager in charge immediately, complete Section 1 of this form and email it to the Data Protection Officer (mark.greenfield@platinummg.co.uk) and IT Helpdesk (it@platinummg.co.uk) where appropriate.

Section 1: Notification of Data Security Breach	To be completed by Department Manager/ Director of person reporting incident
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If so, please provide details:	
Brief description of any action taken at time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Fowarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by the Lead Investigation Officer in consultation with the Head of area affected by the breach and if appropriate IT where applicable
Details of IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial, legal liability or reputational consequences for the company or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories	
HIGH RISK personal data • **Special Categories personal data** (as defined in the Data Protection Legislation) relating to a living, identifiable individual's: a) Racial or ethnic origin; b) Health	
• Information that could be used to commit identity fraud such as personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
• Spreadsheets containing sensitive information such as address, telephone numbers, etc;	
• Security information that would compromise the safety of individuals if disclosed.	
Data Protection Officer and/or Lead investigation Officer to consider whether it should be escalated to the ICO.	

Section 3: Action taken	To be completed by the Data Protection Officer and/or Lead investigation Office
Incident number	E.g. year/001
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	Yes/No If YES, notified on (date):
Follow up action required/recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other Internal Stakeholders (details, dates):	
For use of Data Protection Officer and/or Lead Officer:	
Notification to ICO	Yes/No If YES, notified on: Details:
Notification to data subjects	Yes/No If YES, notified on: Details:
Notification to other external, regulator/stakeholder	Yes/No If YES, notified on: Details: