/* NO COMMENT */

EVERY POLICE STATION, EVERY DAY!

GOVERNANCE & ACCOUNTABILITY

POLICY STATEMENT

Our business has an appropriate data protection policy.

GDPR requires us to show how we comply with its principles. Our policy helps us address data protection in a consistent manner and demonstrate accountability under the GDPR.

This is a stand alone policy statement and part of a general staff policy. The policy clearly sets out our approach to data protection together with our responsibilities for implementing the policy and monitoring compliance.

The management have approved the policy and we have published and communicated it to all staff. We have reviewed and updated the policy and will update and review it again at planned intervals or when required to ensure it remains relevant.

Our business monitors our own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

TRAINNING

Our business provides data protection awareness training for all staff. We have brief all staff handling personal data on their data protection responsibilities. We provide awareness training on or shortly after appointment with updates at regular intervals or when required.

We have also considered specialist training for staff with specific duties, such as information security and database management and marketing. Regularly communicating key messages is equally important for us to reinforce training

and maintain awareness (for example intranet articles, circulars, team briefings and posters).

MONITORING

Our business monitors our own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

Documenting policies alone is often not enough to provide assurances that staff are adhering to the processes they outline so we have ensured that we have a process to monitor compliance to data protection and security policies.

We have regular test measures that are detailed within the policies to provide assurances about their continued effectiveness.

Responsibility for monitoring compliance with the policy are independent of the people implementing the policy, to allow the monitoring to be unbiased. Staff report the results of compliance testing on a regular basis to senior management.

PROCESSOR CONTRACTS

Our business will ensure that a written contract with the processors we use is in place. This is an ongoing process.

Whenever we use a processor we ensure we have a written contract in place, or another legal act must apply. The contract is important so both parties understand their responsibilities and liabilities.

GDPR sets out what we included in the contract.

We are directly liable for overall compliance with GDPR and for demonstrating that compliance. If we don't achieve this, then we may be liable to pay damages

in legal proceedings or be subject to fines or other penalties or corrective measures.

We must only appoint processors who can provide 'sufficient guarantees' that the requirements of GDPR will be met and the rights of data subjects protected.

Processors must only act on our documented instructions. They do however have some direct obligations and responsibilities under GDPR. If they fail to comply they may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

We may implement the use of adherence by a processor to an approved code of conduct or certification scheme to help demonstrate that us have chosen a suitable processor. However they are not yet available. In the future, standard contractual clauses may be provided by the European Commission or the ICO, and may form part of a code or certification scheme. However these are not yet available.