Whyte&Co.
Enforcement Services
7, White Oak Square, London Road, Swanley, Kent BR8 7AG
TEL: 0345 458 9429 ● **FAX:** 0345 458 9439 ● **EMAIL:** info@whyte.co.uk ● **WEB:** www.whyte.co.uk

DATA PROTECTION POLICY

Policy Statement

Whyte & Co. is committed to ensuring that it fully complies with all its legal obligations under the Data Protection Acts of 1998 and 2003. The company processes a considerable amount of personal data and as such it has a number of legal responsibilities, failure to comply with which could result in legal action and substantial financial penalties not to mention the loss of clients. The purpose of this document is to detail our approach to Data Protection so that both we and others can see that it is adequate and appropriate.

Whyte & Co. is registered with the Information Commissioners Office under the Data Protection Act 1998.

Management Commitment and Resources

This policy has the full support of senior management who are committed to providing the necessary resources to ensure that its objectives are achieved.

Responsibility

The partners have ultimate responsibility for this policy but day-to-day responsibility is delegated to the IT Manager who is also the Data Protection Manager.

This policy is applicable to all staff and failure to comply is a disciplinary offence that could in some instances constitute gross misconduct.

Communication and Training

The policy will be made available to all staff. All who handle personal data will receive data protection awareness training and this will commence during induction. Particular emphasis will be placed on the eight data protection principles with specific examples provided of how these relate to the company's activities.

Audit and Review

Compliance with this policy will be audited annually using the pro-forma checklist provided by the Information Commissioners Office and the results documented and reviewed by Senior Management.

The policy will be reviewed annually or at such more frequent interval as may be considered necessary due to changes in legislation, changes in the manner in which the company processes data or apparent deficiencies in the policy.

Relationship to Other Procedures

Whyte & Co operates an integrated management system (IMS) comprising a quality, environmental and information security management system accredited to ISO 9001. ISO 14001 and ISO 27001 respectively. This policy will be audited in accordance with our IMS audit procedure, documented and controlled under our document control procedure and training in the policy will be provided in accordance with our training procedure.

Data Protection will be taken into consideration in the design of all new business processes.

Use of Data

All data held by Whyte & Co. is held under a duty of confidentiality. It is held and processed for lawful purposes only and is not used in any way that is incompatible with the purposes for which it was obtained. No sensitive personal data is held.

Client Requests for Data

Clients have a right to be provided with any data pertaining to the service which we provide them and any requests for the provision of data should be complied with as fully and promptly as possible. However, care must be taken to ensure that the request does in fact emanate from a client and that the particular member of staff requesting the information is properly authorised to make such a request.

Complaints

Nearly all data held by Whyte & Co. has been supplied by our clients or government agencies e.g. DVLA and we are not therefore responsible for its accuracy in the first instance. Complainants should be referred to the appropriate client / agency. However, if the complaint relates to the inaccuracy of data that has been obtained by Whyte & Co. the complaint should be referred to the Director of Operations.

7, White Oak Square, London Road, Swanley, Kent BR8 7AG
TEL: 0345 458 9429 ● **FAX:** 0345 458 9439 ● **EMAIL:** info@whyte.co.uk ● **WEB:** www.whyte.co.uk

Data Security

Access to personal data is on a need to know basis.

Access to data is controlled by restricting physical access to our premises which are alarmed and through the use of locked filing cabinets.

Access to databases is controlled through the use of encrypted passwords that are regularly changed and the use of firewalls with an integrated Intruder Detection System.

Hard copy data is removed for shredding and recycling by a contractor who issues a certificate of secure destruction.

Before discussing a case staff are required to ask appropriate questions in order to satisfy themselves as to the identity of the person to whom they talking. As a general rule staff are under instruction not to discuss cases with third parties unless and until we have received written authorisation from the data subject, so to do.

All PC's that are disposed of have their hard drives erased prior to disposal.

Data Backup

Backups are handled by two distinct mechanisms which complement each other.

1. Tape backups of the servers occur nightly in a "grandfather, father, son" (GFS) configuration.

- Daily (son) backups are run nightly Monday to Friday each week. The tapes used for these are cycled on a four-week basis.
- On the first day of each month, a separate monthly (father) backup is run and the resulting tape is held for a full year until the corresponding month.
- At the end of the year, a separate yearly (grandfather) backup is run and the resulting tape is held indefinitely.
- All tapes are stored off-site until required for their allocated day or month's backup.
- All backups are Full backups of the entire server systems ensuring each tape contains all company data and server configuration data.
- Systems that change infrequently (e.g. web-server, firewall and other network infrastructure configuration) are backed up as and when changes are made. These backups are held as online images which are backed up as part of the normal tape backup cycle.

2. The core business system (Enforcer) database is further protected by a mechanism known as "log shipping". This entails periodically (once per hour in our case) sending a log of all database transactions to a separate location where they can be rebuilt onto a different system thereby creating an exact mirror of the database.

7, White Oak Square, London Road, Swanley, Kent BR8 7AG
TEL: 0345 458 9429 ● **FAX:** 0345 458 9439 ● **EMAIL:** info@whyte.co.uk ● **WEB:** www.whyte.co.uk

- Each hour, a backup is made of the preceding hour's transactions. This is encrypted and securely transferred off-site to a business partner. The log is then decrypted and "played" onto the mirror copy of the database stored at our business partner's premises.

- At the beginning of each day a "start of day" (SOD) backup is taken. This is a full backup of the database retained on the database server and plays no direct role in the log shipping system except to provide a potentially faster route to a restore.

- In the event of a disaster with the database at Whyte & Co., the full database can be restored on-site in the event that the company's database server remains viable. If the server is not repairable or destroyed, the database can be rebuilt to a new server at a new site if necessary. In either case, the maximum data loss would be one hour's worth of transactions.

The effectiveness of our backup system is routinely tested as part of our disaster recovery/business continuity planning. To date, we have demonstrated several times that we are able to recover our systems to a new server at a different site within 4 hours. A separate "disaster recovery" server is maintained off-site and is periodically refreshed with an up-to-date copy of the company's working systems.

Disaster Recovery

This is covered by our Business Continuity Plan.

Viruses, Trojans, Spyware etc.

All of the company's systems are protected against malicious software by appropriate applications that are automatically updated on a daily basis.

In addition staff have no access rights to non-business related internet sites or personal e-mail systems.

Retention of Data

Data is retained for a maximum period of six years (Limitations Act) or such longer period as may be specified by our client local authority. Procedures are in place for the automatic erasure of data once the expiry date is reached.

Subject Access Requests

All subject access requests (Section 7, DPA) are immediately referred to the Director of Operations who will ensure that a response is provided as promptly as possible but in any event within the statutory time period. They will also ensure that the information is provided in a format that is intelligible.

7, White Oak Square, London Road, Swanley, Kent BR8 7AG
TEL: 0345 458 9429 ● **FAX:** 0345 458 9439 ● **EMAIL:** info@whyte.co.uk ● **WEB:** www.whyte.co.uk

DVLA

Whyte & Co. has a file transfer link with the DVLA that enables us to obtain registered keeper information electronically. It is critical that this facility is not abused and that it is not used for any purpose other than that for which it was established e.g. to confirm whether or a not a vehicle in respect of which a PCN has been issued is still registered to the same keeper and address.

Under no circumstances may it be used in relation to any other type of debt than Road Traffic Debt. It may only be used to obtain confirmation in respect of vehicles for which we already hold a warrant and not to obtain keeper details for vehicles which may or may not be registered to the debtor.

Enforcement Agents must not request a DVLA check for purposes other than outlined above and office based staff responsible for processing requests must ensure that the vehicle is one for which we hold a warrant.

Failure to comply will constitute gross misconduct

Review

This policy will be reviewed biennially or whenever there is a change in relevant legislation, case law or accepted best practice or any matter which calls the efficacy of the policy into question.

Paul Whyte

Partner

7, White Oak Square, London Road, Swanley, Kent BR8 7AG
TEL: 0345 458 9429 ● **FAX:** 0345 458 9439 ● **EMAIL:** info@whyte.co.uk ● **WEB:** www.whyte.co.uk