Impreglon UK Ltd.
Information and Data Protection Policy

The Data Protection Act 1998 requires every data controller who is processing personal data to notify the Information Commissioner's Office unless they are exempt. Failure to notify is a criminal offence. Impreglon UK has notified the Information Commissioner's Office for the following purposes:

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Information and databank administration
- CCTV for premises security

If Impreglon UK needs to collect data for any purpose not stated above we will notify the Information Commissioner's Office before collecting that data.

The Data Controller for Impreglon UK is Guy Williams, Director.

Eight Data Protection Principles

Whenever collecting information about people Impreglon UK agrees to apply the Eight Data Protection Principles:

1. Personal data should be processed fairly and lawfully
2. Personal data should be obtained only for the purpose specified
3. Data should be adequate, relevant and not excessive for the purposes required
4. Accurate and kept up-to-date
5. Data should not be kept for longer than is necessary for purpose
6. Data processed in accordance with the rights of data subjects under this act
7. Security: appropriate technical and organizational measures should be taken unauthorized or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
8. Personal data shall not be transferred outside the EU unless that country or territory ensures an adequate level of data protection.

Security Statement

Impreglon UK has taken measures to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage.

This includes:

- Adopting an information security policy (this document is our policy).
- Taking steps to control physical security (current files and staff records are all kept in a locked cabinet).
- Putting in place controls on access to information, for example password protection on files and server access.
- Establishing a business continuity/disaster recovery plan (Impreglon UK takes regular back-ups of its computer data files and this is stored away from the office at a safe location).
- Training all staff on security systems and procedures.
- Detecting and investigating breaches of security should they occur.
- Ensuring that individuals have a right to see what data is being kept on them, and for what purpose within 40 days of a request being made.
- Ensuring that staff agree to try to keep work taken home relatively secure, that they return all work related material and that Impreglon UK should be informed if any information or data is mislaid or stolen.