Purpose & Scope

This policy covers all Gardner & Co activities and processes in which personal data is used, whether in electronic or hard copy form.

This policy applies to all members of the company including staff, site personnel and others acting for, or on behalf of, the company or who are otherwise given access to the company's information infrastructure.

This policy takes precedence over any other company policy on matters relating to data protection.

Definitions

The following terms are defined in data protection legislation:

- Personal data – any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier (e.g. name, identification number, location data or online identifier).
- Special category personal data – the following types of personal data (specified in data protection legislation) which are particularly sensitive and private in nature, and therefore more likely to cause distress and damage if compromised:
    - Racial or ethnic origin
    - Political opinions
    - Religious or philosophical beliefs
    - Trade union membership
    - Health related conditions (physical or mental health)
    - Sex life and sexual orientation
    - Commission or alleged commission of any criminal offence
    - Genetic data
    - Biometric data, where processed to uniquely identify an individual
- Data subject – the individual to whom the personal data relates
- Data controller – determines the purposes and means of processing personal data
- Data processor – responsible for processing personal data on behalf of a controller
- Data breach – a security incident that affects the confidentiality, integrity or availability of personal data. A data breach occurs whenever any personal data is:
    - lost;
    - corrupted;
    - unintentionally destroyed or disclosed;
    - accessed or passed on without proper authorisation; or
    - made unavailable and this unavailability has a significant negative effect on the data subjects.

Policy

Gardner & Co (Kent)Ltd ("the company") is committed to complying with the General Data Protection Regulation (GDPR) and any legislation enacted in the UK in respect of the protection of personal data (together "data protection legislation"). To do this, the company will:

1. Only use personal data where strictly necessary and will rely on an appropriate lawful basis for processing personal data.
2. Inform data subjects of the lawful basis and explain the purpose and manner of the processing in the form of protection notices and other similar methods.
3. Keep personal data secure and manage incidents effectively when things go wrong.
4. Observe the rights of individuals under data protection legislation.
5. Ensure staff are trained appropriately in managing personal data.
6. Ensure that records containing personal data are managed effectively.
7. Only share personal data with third parties where adequate standards of data protection can be guaranteed and, where necessary, contractual arrangements are put in place.
8. Implement comprehensive and proportionate governance measures to demonstrate compliance with data protection legislation principles.

Roles and responsibilities

Every individual who works for, or on behalf of, the company must ensure that any personal data they handle is processed in accordance with this policy and the data protection legislation principles (see Data Protection Procedure).

The Senior Management Team is responsible for approving this policy and assuring that the company meets its data protection legislation obligations.

The Data Protection Officer is responsible for:

- Informing and advising the company of its data protection obligations
- Monitoring compliance
- Awareness-raising and training of staff involved with processing operations
- Undertaking internal audits of data protection
- Providing advice on data protection impact assessments
- Cooperating with the Information Commissioner and acting as the contact point for any issues relating to processing

Heads of Services and Senior Managers are responsible for ensuring awareness of, and compliance with, this policy in their respective areas.

The Senior management board is responsible for:

- Maintaining this policy
- Providing guidance, support, training and advice on data protection compliance
- Processing all subject access requests for the company
- Supporting the responsibilities of the Data Protection Officer

The Security Operations Group is responsible for managing information security across the company. The purpose of the group is to review the information security landscape (both digital and physical), assess the company's performance and readiness, and ensure risk reduction, remediation and response.