INFORMATION SECURITY POLICY

1. INTRODUCTION

a. Information and Information systems underpin the Company's activities and are essential to its operational and administrative functions. It is therefore essential that all employers, consultants and agents play their part in safeguarding the availability, integrity, confidentiality and authenticity of the information they hold or access. The misappropriation of information not only has the potential to cause reputational damage and disruption to its own business and that of its clients, but may also expose the organisation to the risk of legal sanctions.
b. The Company and all employees, contracts, associates and agents will comply with legal obligations and responsibilities at all times.
c. The Company and all employees, contracts, associates and agents will comply with legal obligations and responsibilities at all times.
d. Additionally, the loss or inadvertent disclosure of personal information can cause a significant amount of distress to the people whose information is affected.
e. This document constitutes the Company's Information Security Policy, including guidance for employees, consultants and agents. All members of the business have a responsibility to work within the guidelines of this Policy.
f. In order to carry out its duties effectively and efficiently, the Company has to collect and make use of personal information about individuals, such as employers, employees, and applicants for posts, suppliers and clients. The Company is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

2. SCOPE OF POLICY

a. This policy is applicable to all personal data/information processed by the Company in its lawful work. It will apply to all staff, partner organisations, contractors or agents performing work for or on behalf of the Company.
b. The Company affirms its commitment to the obligations of legal requirements.

3. SECURITY AND ACCESS TO INFORMATION

a. Access and usage of business information systems is covered by the Company's Internet and Email Use Policy and the Employee Handbook.
b. This Policy provides a framework for the management of information security for the whole of the Company operation and business, and applies to:
    i. All those with access to the Company's information systems, including staff, consultants, agents and visitors.
    ii. All data or information held in print or in electronic formats by the Company including documents, spreadsheets and other paper and electronic data, images and video.

iii. All systems attached to a Company computer or telephone networks and any cloud or other systems supplied by the Company.
iv. All information processed by the Company pursuant to its operational activities, regardless of whether the information is processed electronically or in paper form, including all communications sent to or from the Company and any information held on cloud or other authorised systems external to the Company's network.
v. All Company owned and personal Mobile Computing Devices being used to access the Company's Information systems as well as Company owned non-mobile computers. Non-mobile devices, such as personally owned desktop computers that are used outside the Company's premises to access Company information are also within the scope of this Policy.
vi. All external third parties that provide services to the Company in respect of information processing facilities and business activities.

4. MARKETING

a. This framework applies to all data utilised for marketing whether acquired from third parties, released to third parties or processed internally for marketing campaigns.
b. The business acknowledges the right of an individual to object to processing for the purposes of direct marketing, who must be allowed the opportunity to do so.

5. SUBJECT ACCESS REQUESTS

a. Individuals (e.g. staff, apprentices and any customers) have the right to access personal data held about them electronically or in paper files by making a "Subject Access Request".
b. The Company reserves the right to levy a charge of £10 for each request in line with the Data Protection (Subject Access Fees and Miscellaneous Provisions) Regulations 2000.
c. Staff should direct all Subject Access Requests to the Chief executive Officer who will manage requests inline with business subject access and disclosure procedures.

6. DISCLOSURE

a. If a member of staff is requested to disclose personal data to third parties, then this should only be done strictly in compliance with the first principle of data protection (see Appendix A). In the first instance the member of staff should obtain information from the person making the request as to the data being requested and the purpose(s) for which it is being requested.
b. Should any staff be unsure about whether or not to disclose personal data to a third party, they should contact the Chief executive Officer in the first instance for advice.

7. RESPONSIBILITIES

a. All staff have a responsibility to abide by this policy and associated procedures.
b. Disciplinary action may be taken against staff in breach of data protection policy in line with HR Policy.
c. If staff have queries on obligations under the Data Protection Act please direct them to the Chief executive Officer in the first instance for advice.

8. TRAINING

a. Training on data protection aspects will be provided as necessary and as appropriate either using internal or external facilitation.

9. RELATED INFORMATION

a. Within this policy statement there are references to other related policies and procedures which include:
   - Employee Handbook
   - Internet and Email Use Policy
   - The Information Commissioner's Website http://www.ico.gov.uk

10. INFORMATION SECURITY KEY PRINCIPLES

a. The Company recognises that information is a fundamental asset to a knowledge-driven organisation and it is the Company's policy that the information it manages is protected against the adverse effects of failures in confidentiality, integrity, availability and compliance with legal requirements, which may otherwise occur. Achieving this objective is dependent on all members of the Company complying with this policy.
b. The Company has adopted the following eight principles to underpin this Information Security Policy:
   i. Information will be protected in line with all relevant Company policies and legislation, notably those pertaining to Data Protection, Freedom of Information, and Human Rights.
   ii. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the information and ensuring that appropriate security measures are in place to protect the information asset.
   iii. Information will be made available solely to those who have a legitimate need for access.
   iv. Information will be classified according to the Company's data classification guidelines.
   v. The integrity of information will be maintained.
   vi. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
   vii. Information will be protected against unauthorised access.

viii. Action which breaches the terms of the Information Security Policy and its associated policies will be dealt with via the Company Disciplinary Procedures.

11. INFORMATION CLASSIFICATION AND HANDLING

a. Information is a fundamental Company asset, required for the effective operation of the Company and the services it offers, administrative, management and commercial activities. The correct classification of information is important to help ensure the prevention of information leaks and to minimise the impact of such leaks if they do occur. As well as being good practice, it helps to ensure that the Company remains compliant with Data Protection and Freedom of Information regulations.
b. To ensure that Company information can be both accessed, used and shared effectively, and also protected from inappropriate access, use or sharing, the following information management principles will apply:
    i. Information is an Asset: Information is an asset that has value to the Company and must be managed accordingly. ii) Information is Shared: Users have access to the information necessary to carry out their duties; therefore information is shared where permissible and appropriate.
    ii. Information is Secure: Information is protected from unauthorised use and disclosure. In addition to traditional aspects of information security, such as the Data Protection Act, this includes protection of sensitive and commercial information.
    iii. Information is Responsibly Managed: All employees of the Company community have responsibility for ensuring the secure and appropriate use of information assets.
    iv. To support the operation of the above principles this Policy has been developed to ensure that all employees of the Company understand the ways in which different kinds of information and data should be handled accordingly to their sensitivity.
c. Information classification is based on the level of sensitivity and the impact on the Company or an individual should that information be disclosed, altered, lost or destroyed without authorisation. The classification of all information into different categories ensures that individuals who have a legitimate reason to access a piece of information are able to do so, while at the same time ensuring that information is protected from those who have no right to access the information. The classification will guide the appropriate security and technical controls required.
d. All information owned, used, created or maintained within the Company should be categorised into one of the following three categories:
    i. Non-Sensitive/Open
    ii. Personal/Confidential
    iii. Highly Sensitive
e. The majority of information held by the Company will come under the 'Non-Sensitive/Open' category. A small amount of information, including personal data/information, will be categorised as 'Personal/Confidential'. The 'Highly Sensitive' classification should only be used where no lesser classification is appropriate.

f. Note that it is possible for one piece of information or document to have different classifications throughout its lifecycle; for instance, commercially sensitive information may become less sensitive over time. Where one set of information contains a range of information, such as a database, the highest classification must be applied to the whole set of information. The Data Protection Act defines 'Sensitive Personal Data' as information which relates to racial or ethnic origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences. The processing of 'Sensitive Personal Data' is subject to additional conditions that are more stringent.
g. Data encryption is required for 'Personal/Confidential' or 'Highly Sensitive' data. Encryption must always be used to protect 'Personal/Confidential' or 'Highly Sensitive' data transmitted over data networks to protect against the risk of interception. This includes when accessing network services which require authentication (i.e. username and password access) or when sending or receiving such data via email.
h. 'Personal/Confidential' or 'Highly Sensitive' information should only be taken for use away from Company premises in an encrypted form unless its confidentiality can otherwise be assured. Where 'Personal/Confidential' or 'Highly Sensitive' data is being stored or accessed from mobile computing devices the devices themselves must be encrypted; it is not permitted to store or access 'Personal/Confidential' or 'Highly Sensitive' data on personal non-Company owned devices, mobile or otherwise. However wherever possible, notwithstanding the data classification, it is preferable to access Company information using the Company's remote access facilities.

12. FAILURE TO COMPLY

Employees are reminded that non-adherence to this policy and all associated Company policies could result in disciplinary proceedings as outlined in the Company Handbook and the Disciplinary Policy.

13. POLICY REVIEW.

This policy does not form part of an individual's contract of employment and may be amended from time to time.

14. APPENDIX A: DATA PROTECTION PRINCIPLES

a. Anyone processing personal information must comply with these eight enforceable principles of good information handling practice which are as follows:
   I. Personal data shall be processed fairly and lawfully.
   II. Personal data shall be held only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.
   III. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
   IV. Personal data shall be accurate and where necessary kept up to date.

V. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

VI. Personal data shall be processed in accordance with the rights of data subject under the Data Protection Act 1998.

VII. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of the data.

VIII. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.