Bias Test Security Policy

1. Information Security Policy

1.1. A nominated person is responsible for preparing guidelines to ensure that all staff are aware of the key aspects of computer misuse legislation (or its equivalent), in so far as these requirements impact on their duties

1.2. It is the organisation's policy that the information it manages shall be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

1.3. This information security policy provides management direction and support for information security across the organisation. Specific, subsidiary information security policies shall be considered part of this information security policy and shall have equal standing.

1.4. This policy has been ratified by the organisation and forms part of its policies and procedures, including its Regulations for Conduct. It is applicable to and will be communicated to staff, partners and other relevant parties.

1.5. This policy shall be reviewed and updated regularly to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

1.6. To determine the appropriate levels of security measures applied to information systems, a process of risk assessment shall be carried out for each system to identify the probability and impact of security failures.

1.7. To manage information security within the organisation an information security oversight committee shall be established, chaired by a senior officer of the company and comprising appropriate senior organisational managers. The objective of this group shall be to ensure that there is clear direction and visible management support for security initiatives. This oversight group shall promote security through appropriate commitment and adequate resourcing.

1.8. An information security working party, comprising management representatives from all relevant parts of the organisation, shall devise and coordinate the implementation of information security controls.

1.9. The responsibility for ensuring the protection of information systems and ensuring that specific security processes are carried out shall lie with the head of the department managing that information system.

1.10. Specialist advice on information security shall be made available throughout the organisation.

1.11. The organisation will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.

1.12. The implementation of the information security policy shall be reviewed independently of those charged with its implementation.

Bias Test Compliance Policy

1. Compliance Policy

1.1. The Terms and Conditions of Employment and the organisation's Code of Conduct set out all employees' responsibilities with respect to their use of computer based information systems and data. Line managers must provide specific guidance on legal compliance to any member of staff whose duties require it.

1.2. All members of the organisation will comply with the Information Security Policy and, where appropriate, their compliance will be monitored.

1.3. Before any new systems are introduced, a risk assessment process will be carried out which will include an assessment of the legal obligations that may arise from the use of the system. These legal obligations will be documented and a named system controller, with responsibility for updating that information, will be identified.

1.4. Guidance documents will be made available to all computer users through the IT department's website covering the key aspects of the law of copyright, in so far as they relate to the use of information systems. Guidance is also available on the key aspects of computer misuse legislation.

1.5. The organisation's Code of Conduct forbids the use of information systems to send or publish derogatory remarks about people or organisations.

1.6. The organisation's data retention policy defines the appropriate length of time for different types of information to be held. Data will not be destroyed prior to the expiry of the relevant retention period and will not be retained beyond that period. During the retention period appropriate technical systems will be maintained to ensure that the data can be accessed.

1.7. The organisation will only process personal data in accordance with the requirements of the data protection legislation. Personal or confidential information will only be disclosed or shared where an employee has been authorised to do so.

1.8. Where it is necessary to collect evidence from the information systems, it shall be collected and presented to conform to the relevant rules of evidence. Expert guidance will normally be sought.

1.9. All of the organisation's systems will be operated and administered in accordance with the documented procedures. Regular compliance checks will be carried out to verify this compliance.

1. Legal Obligations

1.1. A nominated person is responsible for ensuring that all staff are fully aware of, and agree to comply with their legal responsibilities with respect to their use of computer based information systems and data. Such responsibilities are to be included within key staff documentation such as Terms and Conditions of Employment and the Organisation Code of Conduct.

1.2. System planning processes explicitly define and document the legal obligations arising from the operation of the proposed system. There is a named individual responsible for updating that information.

1.3. A nominated person is responsible for preparing guidelines to ensure that all staff are aware of the key aspects of the law of copyright, in so far as these requirements impact on their duties.

2. Safeguarding Organisational Records

2.1. The information created and stored by the organisation's information systems must be retained for a minimum period that meets both legal and business requirements. The organisation should maintain a suitable archiving and record retention procedure.

2.2. The archiving of documents must take place with due consideration for legal, regulatory and business issues with liaison between technical and business staff.

3. Retaining or deleting electronic mail

3.1. Data retention periods for email must be established to meet legal and business requirements and must be adhered to by all staff.

4. Complying with Data Protection Act

4.1. The organisation intends to comply fully with the requirements of data protection legislation in so far as it directly affects the organisation's activities

Personal privacy

4.2. Information regarding the organisation's applicants, clients, suppliers or other people dealing with the organisation is to be kept confidential and must be protected and safeguarded from unauthorised access and disclosure

5. Sharing information

5.1. Persons responsible for Human Resources management are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organisation and to external parties.

6. Safeguarding against libel and slander

6.1. Staff are prohibited from writing derogatory remarks about other persons or organisations.

7. Evidence

7.1. Where it is necessary to collect evidence against a person or organisation to meet regulatory or statutory requirements, it shall be collected and presented to conform to the relevant rules of evidence. Expert guidance will normally be sought

8. Computer misuse

8.1. A nominated person is responsible for preparing guidelines to ensure that all staff are aware of the key aspects of computer misuse legislation (or its equivalent), in so far as these requirements impact on their duties.

9. Ensuring compliance with organisational security policy

9.1. All staff are required to comply fully with the organisation's information security policies. The monitoring of such compliance is the responsibility of management.

10. Managing system operations and system administration

10.1. The organisation's systems must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the organisation's information security.

11. Technical compliance checking

11.1. All systems must be regularly checked to ensure that they comply with the organisational security policy