Veritau Group

Information Governance Policy

Contents

Information Governance Policy

POLICY STATEMENT

1 This policy sets out the Group's objectives in respect of information governance. It provides a framework for the Boards and management team, and is intended to help inform future action plans. It also recognises the importance of maintaining effective information assurance and risk management mechanisms to help deliver those objectives.

PURPOSE AND OBJECTIVES

2 The Group holds information and data in its own right (including financial, performance and staff related information). It also holds information and data on behalf of its client organisations to support the delivery of its services.

3 An objective of this policy is to ensure the confidentiality, integrity and availability of information held by the Group by reducing the risk of:

- unauthorised access to information;
- incomplete or inaccurate information, and
- unnecessary collection or use of information (particularly personal data).

4 An objective of this policy is to ensure that the information the Group uses is:

- sufficient, complete and relevant;
- accurate, reliable and subject to periodic verification;
- up to date and used in a timely way.

5 Relevant definitions are contained in the glossary.

SCOPE

6 This policy applies to all employees, contractors and agents of the Group with any form of access to the Group's data and information systems.

7 This policy exists to safeguard the Group's information systems and all its information assets. Its purpose is to protect the Group's information assets from all threats, whether internal or external, deliberate or accidental, and to ensure service continuity, minimise damage or loss, and maximise opportunities.

8 This policy applies to information in all forms including, but not limited to:

- hard copy or documents printed or written on paper;
- information or data stored electronically, including scanned images;
- communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- recordings of verbal communications, such as voicemail;

- published web content, for example on the Group's website;
- photographs, video and other digital images.

RISKS

9 Reliable and accurate information is critical to proper decision making and for the effective delivery of services to the Group's clients. This makes information a vital business asset that to be utilises and protected. Information risk management aims to maintain the confidentiality, integrity and availability (CIA) of the Group's information.

10 This policy reduces the risks associated with personal data including the harm that might occur to data subjects – including citizens, customers and clients, and the Group's employees; and the consequent financial and reputational risks to the Group.

11 The management of information risks should be incorporated into all day-to-day operations. It is a tool for managing information proactively rather than reactively. It will help the Group to provide the right information to the right people at the right time, and help avoid incidents where data is lost or improperly disclosed.

CORPORATE GOVERNANCE

12 This policy is part of the framework governing information management within the Group.

13 The Chief Executive is the Senior Information Risk Owner (SIRO) for the Group with responsibility for overseeing the development and implementation of the policy framework and ongoing compliance. The SIRO reports on the application of the policy framework to the Boards.

14 The SIRO will appoint an "owner" for each of the Group's information assets. Assistant Directors and Managers may expect to be appointed as Information Asset Owners (IAOs) for assets in their area. Each IAO should:

- record each asset accurately in the Group's Information Asset Register;
- identify any personal data within each asset and ensure compliance with UK GDPR and the Data Protection Act 2018 (DPA).

15 The Veritau Management Team (VMT) works to ensure the policy framework is up to date and reflects new or emerging information risks. Each VMT member is responsible for monitoring compliance with the policy framework in their area and for escalating issues to the SIRO for further consideration.

POLICY IMPLEMENTATION

16 An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

17 Each VMT member will act as the owner of any Information Asset in their management area. Where responsibility is unclear VMT will appoint a single member to this role. The role of Information Asset Owner (IAO) includes:

- recording each information asset accurately in the Group's Information Asset Register(s);
- applying risk management to identify risks to each asset (including risks associated with its storage and transmission, as well as access to it);
- devising working practices that fulfil this policy by applying controls over access and use of information, appropriate to the risks identified above
- identifying any personal data and ensuring compliance with the Data Protection Act 2018 (DPA) through the application of the Group's Data Protection Policy

18 An understanding of this policy and its related guidance is regarded as a basic competence for all managers.

INFORMATION RISK MANAGEMENT

19 Information risk management is the process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's information and information systems.

20 Risks can never be eliminated fully. A structured, systematic and focused approach to managing risk is therefore required. However risk management is not about being 'risk averse', it is about being 'risk aware'. Some degree of risk taking is inevitable and necessary if the Group is to achieve its objectives. By being 'risk aware', the Group is in a better position to avoid threats, take advantage of opportunities and ensure its objectives and goals are realised.

21 Information risks will be managed by assigning roles and responsibilities and co-ordinating the implementation of this policy and all supporting documentation, as follows:

- The **Senior Information Risk Owner** (SIRO) is responsible for maintaining the Group's information governance policy framework, and for ensuring its ongoing effectiveness. The SIRO will be supported by the Group's AD Information Governance.
- Individual **ADs and managers** must be familiar with the information assets in their particular area. They are required to report on what information their team holds and how it is being managed. They are also responsible for identifying and recording information risks and for helping to develop appropriate mitigation strategies.
- **Users** are employees, temporary staff, contractors and agents who access and process data on the Group's information systems. As part of a positive risk culture, users must be 'risk aware'; discussing information risks and potential threats to data with their managers. They must also be aware of the Group's information policies and fully comply with them.

COMPILING AND MAINTAINING THE INFORMATION ASSET REGISTER

22 Each VMT member is responsible for ensuring the Group's Information Asset Register is kept up to date. The entries in the Register will be used by the Boards and SIRO to help identify the areas of highest risk to the Group. The register needs to include sufficient information to help identify and explain the risk management decisions within each area.

23 The Information Asset Register can be used to help to identify the different types of information assets held and provide direction on the risk to the Group that any loss, compromise or lack of availability might have. Appendix 1 provides further guidance on compiling the Register and for assessing information risks.

INFORMATION SECURITY

24 The aim of information security is to protect the Group's information assets from a wide range of threats whether internal or external, deliberate or accidental, in order to ensure service continuity and minimise the impact of adverse events on clients and staff.

25 Ultimate responsibility for information security rests with the SIRO, but on a day-to-day basis ADs and managers will be responsible for implementing this policy and related procedures in their teams. They will be able to seek advice and guidance from the SIRO or Information Governance Manager to support them in this task.

26 When processing information on behalf of a client organisation, ADs and managers must make sure that their staff are aware of the information security policies and procedures applicable to that client.

SECURITY CLASSIFICATIONS

27 The Group will have regard to the policies and practices applicable to each client in respect of security classifications. The Group will not routinely mark information relating to a client unless a security classification scheme is in place. Similarly, the Group will not mark its own documents.

ANTI VIRUS

28 Computer virus and malicious software can present serious risks to the security of information held by the Group. The Group uses computer networks and systems provided by City of York Council, which may be accessed remotely using facilities offered by its various host councils, or by devices provided by CYC, or by other devices using software authorised by CYC.

29 All users of the Group's IT systems are responsible for ensuring they comply with the requirements of the anti-virus policies of City of York and host councils

E-MAIL

30 The Group recognises the potential financial, legal and reputational risks that may be caused by the misuse of e-mail. Detailed rules associated with e-mail

usage are included in the Group's Electronic Communications policy but in addition to this:

- non-work email accounts must not be used to conduct Group business;
- secure e-mail facilities or other secure data transfer arrangements (eg secure FTP server) must be used for communicating personal data;
- automatic forwarding of email must be considered carefully to prevent personal data being forwarded inappropriately.

COMPLAINTS

31 The Group's Complaints Policy will apply to any complaint made about matters within the scope of this policy.

COMPLIANCE

32 Employees are required to comply with this policy. Failure to do so could result in disciplinary action being taken against the member of staff concerned

REVIEW AND REVISION

33 This policy will be reviewed annually.

REFERENCES

34 This policy should be read in the context of the Group's other information governance policies and guidelines, national legislation and codes of practice, and accepted best practice.

35 The following policy documents are directly relevant to this policy:

- Data Breach Procedure
- Data Protection Policy
- Document and Records Management Policy
- Information Access Policy
- Information Security Policy

KEY MESSAGES

36 Information is a key asset for the Group (like money, property, or the skills of its staff) and must be protected accordingly.

37 The Chief Executive is the Senior Information Risk Owner (SIRO) for the Group, with responsibility for overseeing the development and implementation of the policy framework and ongoing compliance.

38 Risk management provides the framework for devising and applying security measures to protect the Group's information assets. Individual managers are responsible for the information assets in their area. Information assets should be recorded in the Group's information asset register and any associated risks

should be identified and mitigating action taken. Managers will be supported in this by the SIRO and Information Governance Manager.

39 A range of specific security policies governs the use of the Group's IT infrastructure to ensure that it and the information on it are protected from unauthorised disclosure, loss or corruption, and improper use.

40 Breaches of these policies, and other incidents which threaten disclosure, or loss or corruption of an information asset or part of one, must be reported using the Group's reporting system.