Information Governance Policy

Contents

OVERVIEW AND PURPOSE

1. This policy is part of the University's information governance framework. The governance of information is critical for the University to meet its legal, regulatory and internal policy responsibilities, as well as ensuring that the quality of information supporting strategic business decision making is of the highest order.

2. The information governance framework covers all information related policies, processes, committees, roles and responsibilities, controls, standards, training and online guidance for those handling data and information.

3. The purpose of this policy is to provide clarity for staff at all levels of the organisation regarding information governance arrangements and their responsibilities when processing data. Processing is defined as including the creation, storage, use, disclosure, archiving and destruction of data.

4. Effective information governance is critical to reducing compliance and quality risks arising from increasing volumes of data, along with associated costs.

5. To protect the University's information assets, the information governance framework will ensure:

    - information will be protected from unauthorised access
    - confidentiality of information will be assured
    - integrity of information will be maintained
    - information will be supported by the highest quality data
    - regulatory and legislative requirements are met
    - business continuity plans will be produced, maintained and tested
    - information security training will be made available to all staff, affiliates and students and
    - all potential or suspected data breaches and cyber-attacks will be reported to the University's Data Protection Officer.

6. Non-compliance with information governance policies and standards exposes the University to significant risks including, but not limited to:

    - reputational damage
    - financial penalties
    - unnecessary costs
    - legal action
    - service disruption
    - potentially serious negative impacts on individuals

SCOPE

7. The policy applies to all staff and affiliates, including contractors, temporary staff, student workers, collaborative partners and any third party in a contractual relationship with the University for the processing of information.

8. The policy applies to all information processed for any University purpose including, but not limited to information relating to:

    - teaching and learning
    - professional services and support functions
    - research and knowledge exchange
    - internal and external reporting, legal or regulatory.

POLICY

RELATED POLICIES

9. This policy provides the foundation that underpins policies for data protection, data quality, freedom of information, information security, records management, document management, retention and special category data.

PROCESSES

10. University departments are responsible for designing processes in accordance with information governance principles.

ROLES AND RESPONSIBILITIES

11. All staff and affiliates have an important role in the effective governance of information and data. The Data Quality Policy details data related roles and what they mean for everybody. The following list is provided for guidance in understanding key governance roles and structures.

    - **Senior Information Risk Owner (SIRO)**
      The SIRO is accountable at a senior leadership level for ensuring that the University has effective information governance arrangements in place. This role is carried out by the University Secretary.

    - **Information asset owners**
      Staff with responsibility for the quality and security of information assets related to specific University operations. An information asset can be a meaningful dataset, an IT system or other asset type with value to the University requiring specific arrangements to protect and exploit it. Typically, these individuals will

be senior staff in faculties and directorates.

- **Head of Compliance and Information Governance (and Data Protection Officer)**
  Responsible for ensuring that all elements of the University's information governance framework are in place, training and guidance are available to staff, affiliates and students, and that controls are effective. Additionally, owns the relationship between the University and the Information Commissioner's Office (ICO).

- **Cyber Security Manager**
  Responsible for ensuring the confidentiality, integrity and availability of the University's information assets through effective policies, processes, technologies and controls, including the availability of cyber-security awareness training for all staff, affiliates and students.

- **Line managers**
  responsible for ensuring that all staff and affiliates reporting to them carry out their duties in a manner compliant with information governance policies, including the requirement for all staff and affiliates to complete compliance training.

- **All staff and affiliates**
  Everybody is responsible for handling data in a manner compliant with the University's information governance framework and its policies.

- **Information Governance Committee (IGC)**
  IGC is the main forum for discussing information governance related matters. It also plays a role in the approval of new, and major revisions to, information framework policies.

- **Data Quality Assurance Group**
  Responsible for ensuring effective measures are in place to minimise risks arising from the quality of data in statutory returns.

CONTROLS

12. All University processes involving personal data must maintain a detailed Record of Processing Activity (RoPA) describing the process, its purpose and how it complies with UK GDPR and data protection law.

13. All University projects or new initiatives involving the processing of personal data must complete a Data Protection Impact Assessment (DPIA) to ensure they comply with UK GDPR and data protection law.

14. Information Asset Owners must ensure that data quality standards are met through the implementation and enforcement of effective controls, including training, reference documentation and consideration of techniques such as peer reviews.

Standards

15. The Head of Compliance and Information Governance may periodically monitor the University's compliance with information governance policies through sample data audits.

16. The effectiveness of the University's information governance framework will be periodically reviewed to ensure continued relevance.

Training

17. All staff and affiliates with a Kingston University network account are responsible for completing data protection and cyber security compliance training courses annually.

18. Teams with specific additional training needs will be offered tailored training recognising the raised risks from some University activities and roles.

Online Guidance

19. All staff and affiliates are responsible for following online guidance provided by the Compliance and Information Governance team.

RELATED LEGISLATION, REGULATIONS AND POLICIES

20. Related legislation

- UK Data Protection Act 2018
- UK General Data Protection Regulation
- The Freedom of Information (FOI) Act 2000

21. This policy should be read in conjunction with other relevant University policies and documents that form the overall information governance framework, which can be viewed in the Information regulations section of the University website.

BREACH OF POLICY

22. Anybody handling personal data agrees to abide by the terms of any applicable policies. Users who are found to have breached the terms of relevant policies may be

subject to warnings, verbal and written. In serious cases individuals will be subject to the University's disciplinary procedures, and possible legal action.