Information Security Policy

Document Overview	
A new policy covering Information Security and outlining the expectations for achieving a secure information environment. Guidance and Standards documents support this document to provide officers with support to achieve the policy requirements.	
Intended Audience	All Kirklees employees, Councillors, volunteers and organisations working on behalf of Kirklees
Linked Policy	Information Governance Policy Records Management Policy Data Protection Policy Information Sharing Policy

Revision History			
Version	Author	Reason for issue	Date
3.0	Katy Deacon	Annual Review	10/01/2020
Date of next revision		January 2021	

Policy Scope

- This overarching policy document provides:
  - The requirements that must be met for the information assets of Kirklees Council to be created, stored and destroyed securely and responsibly
  - The requirements of the systems and processes that maintain information security
  - An outline of the expectations of individuals who hold responsibility for maintaining information security
  - An understanding of how the quality of implementation will be checked and reviewed

Policy Statement

- Information is a corporate asset and the purpose of the Information Security Policy is to define and regulate the management of information systems and information assets. This is necessary to ensure information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance.
- The Information Security Policy and associated guidance documents apply to all information assets, irrespective of form, which are owned, processed or used by the Council or which are connected to any networks managed by the Council
- The Information Security Policy documents apply to all persons employed by Kirklees Council as a volunteer, temporary, contracting, Councillor or permanent member of staff and as such all are required to comply with the policy
- Information will be protected in line with all Council Policies and Legislation, notably those relating to Data Protection, Human Rights and Freedom of Information.

- Each information asset will have a nominated Information Asset Owner who is responsible for defining the appropriate users of the asset and ensuring that appropriate security measures are in place to protect the asset
- It is the responsibility of all Kirklees employees, Councillors, volunteers and organisations working on behalf of Kirklees to maintain the integrity of Kirklees information
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification
- Responsibility for the security of information, systems, equipment and premises as far as these are within individuals' control
- All employees and those working on behalf of the council should avoid unauthorised or unintended disclosure, loss or damage to the council's information; unofficial access to any council system; loss or damage to any council equipment and unofficial access to council premises
- Information will be protected against unauthorised access
- Compliance with the Information Security Policy will be enforced.
- The Information Security Policy is a specific part of Kirklees Council's overall Information Governance Framework and relates to the other policies, including:
  - Information Management Strategy
  - Information Governance Policy
  - Information Sharing and Processing Policy
  - Data Protection policy
  - Records Management policy
  - IT strategy

Accountability

The appendix to IG Policies contains details of the accountable roles for Information Governance. In addition to these roles:

- *Managers* are responsible for ensuring that records and information systems in work areas conform to this policy and to the requirements of legislation.
- *All members of staff* are responsible for complying with the policy and legislation and ensuring good Information Security practices are followed

Legal compliance, Monitoring compliance and Information Quality Assurance notes for IG Policies can be found in the Appendix to IG Policies.

Guidance and Support

- Detailed guidance is available on the intranet to provide support to staff in the following areas:
  a. Information Sharing Guidance
  b. Information Processing Guidance
  c. Privacy Notice Guidance
  d. Using encrypted memory sticks
  e. Clear Desk, Clear Screen Guidance