DATA AND INFORMATION POLICY

POLICY:	**DATA AND INFORMATION**
Owner:	CIO
Author:	Greg Dwyer
Service Area:	ICT
Date:	September 2022
Review Date:	March 2023

Contents

1.0 Purpose

The purpose of this policy is to define the standards to adopt when handling business data and information. This includes both paper and electronic records and provides direction on information handling guidelines to be followed.

2.0 Scope

The policy applies to all users who have access to the Council's data, information or information systems.

3.0 Policy

3.1 Principles

Rushcliffe Borough Council commits to ensuring all data and information is held securely at all times. It will ensure every user is aware of, and understands, the basic level of protection to be afforded when handling data including specific information handling guidelines to be followed.

3.2 Risks

Rushcliffe Borough Council recognises the risks associated with users accessing and handling information in order to conduct official Council business.

The Council also handles sensitive information. The security of this information is of paramount importance. Failure to manage sensitive information in accordance with this policy or the Information Classification & Handling Policy may result in a breach of legislation which can be a criminal offence and may lead to prosecution.

Non-compliance with this policy may result in financial loss, an inability to provide services to our customers, and adversely impact the Council's reputation.

3.3 Assertions

Generic
All data and information, in any form, is for the use of the Council or its registered agents only.

Users must not (without due authority):

- access, change or disclose data held on computer systems. Data includes but is not limited to text, images, video and music.
- access, change or disclose information held in documents (electronic or paper)
- move sensitive electronic data or information off Council property unless encrypted as detailed in the Information Classification & Handling Policy.
- move sensitive paper documents off Council property unless this is carried out in accordance with the Information Classification & Handling Policy.

Users of computer equipment should safeguard data by ensuring that equipment is not left logged-on when unattended.

Users must report at once to their line manager any incident involving loss of electronic data and information which breaches statutory legislation or which poses a threat to the reputation of the Council. This will apply especially to records classified as sensitive.

Sensitive information must be stored securely. A risk assessment should be undertaken to identify the appropriate level of protection to secure the information being stored.

Paper documents in an open office should be protected by the controls for the building as detailed in the Physical Access Policy. To increase protection for sensitive documents the following should be considered:

- Lockable filing cabinets.
- Locked safes.
- Separate secure rooms protected by access controls.

Users must report at once to their line manager any incident involving the loss of sensitive data and information held on paper or other non-electronic formats.

Data and Information Handling Guidelines

Sensitive information should not be left on desks unattended or in a position where it may be overlooked by unauthorised personnel. Similarly computer screens should not be situated or positioned so that sensitive information can be overlooked.

If the work area is left unattended for any length of time sensitive documents or storage media containing sensitive data or information should be put away to prevent others from reading, copying or removing it.

At the end of each day, desks must be cleared of all documents that contain any sensitive information. Sensitive information should be stored in a locked cabinet or drawers overnight.

Users should not leave material lying on printers, photocopiers or fax machines at the end of the day.

Waste paper, including computer printouts, must be disposed of with due regard to its sensitivity. Sensitive documents must be shredded and individual Service Areas must be responsible to ensure appropriate facilities are provided.

Computer screens should be locked to prevent unauthorised access when unattended. A screen saver with password protection must be used on all computer equipment and will lock automatically after a period of inactivity to protect information. Users must not tamper with this security feature.

Regular reviews of all data and information records to determine disposal or archiving should be undertaken. Failure to perform this activity regularly will lead to a build up of unwanted records and waste valuable storage resource.

3.4 Responsibilities

The Chief Information Officer has overall accountability and authority for this policy.

Managers have overall responsibility for the care and security of data and information under their control. This includes the authorisation of access to data and information by Council employees and third parties.

All employees of the Council also have responsibility for the care and security of data and information under their control in the performance of their day to day duties and must familiarise themselves with this policy.

4.0 Related Policies, Standards and Guidelines

This policy should be read in conjunction with the:

- Information Security Policy
- Physical Access Policy
- Information Classification & Handling Policy
- Data Protection Policy
- Data Retention Policy

5.0 Terms and Definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in Appendix B of the Information Security Policy.

Sensitive.
Sensitive means all data, records or documents classified as 'OFFICIAL (SENSITIVE)' as defined within the Information Classification & Handling Policy.

Due authority
Due authority or authorised means being given explicit permission to undertake a specified activity or series of activities by a person (such as a Manager) who is held accountable for the outcomes of the activity / activities.

6.0 Enforcement

Any employee found deliberately contravening this policy may be subject to disciplinary action and, where appropriate, legal action.

7.0 Review

This document will be reviewed annually as a minimum or wherever there may be a change of influencing circumstances.

Policy review will be undertaken by the Chief Information Officer.

8.0 Document Attributes

Document Information

Title	Data and Information Policy
Identifier	Data and Information Policy
File Location	http://intranet/documents/information,management/information, security,policy,centre/
Description	Policy determining standards to manage data and information assets in the Council
Keywords	Policy; Data; Information; Asset; Paper; Records; Storage; Clear Desk
Format	MS Word
Author	Greg Dwyer
Owner	CIO
Classification	OFFICIAL
Date Created	17 August 2010
Last Review Date	September 2022
Next Review Date	March 2023
Date to Dispose	12 months after later version of policy released

Document History

Date	Summary of Changes	Version
29/03/2010	First draft	0.1
27/04/2010	Second draft following review of first draft by IS Policy Review Group on 19/04/2010	0.2
17/08/2010	Third draft following review of second draft by Deputy Chief Executive, Head of Corporate Services and ICT Manager on 26/07/2010	0.3
15/09/2014	Reflect changes to job titles & organisation structure	0.4
17/03/2016	Reflect changes to job titles & organisation structure	0.5
15/03/2017	Reflect changes to job titles	1.0
02/03/2018	Reflect changes to job titles and the introduction of GDPR	1.1
19/03/2018	Final review and update by CIO	1.2
21/03/2019	Reviewed, no changes.	1.3
07/04/2020	Reviewed, no changes.	1.4
09/03/2021	Reviewed, no changes (CF)	1.5
26/09/2022	Reviewed, no changes (GD)	1.6

Document Approval

Date	Name & Job Title of Approver(s)	Version
19/03/2018	Ken Thompson (CIO)	1.2

Distribution

Name / Group	Title
Executive Managers	

Coverage

Group
All Employees

End of Document