USER ACCESS POLICY

POLICY:	**USER ACCESS**
Owner:	CIO
Author:	Greg Dwyer
Service Area:	ICT Services
Date:	Sept 2022
Review Date:	March 2023

Contents

1.0 Purpose

Rushcliffe Borough Council holds large amounts of sensitive data whether personal or business related. Information security is very important to help protect the interests and confidentiality of the Council and its customers. Information security cannot be achieved by technical means alone. Information security must be enforced and applied by people, and this policy addresses security issues related to people.

2.0 Scope

The policy applies to all Rushcliffe Borough Council Councillors and Employees, who require access to Council information systems or information of any type or format (paper or electronic).

Where access is to be granted to a third party (e.g. contractors, service providers, voluntary agencies and partners) compliance with the Third Party Access policy must be agreed and documented.

3.0 Policy

3.1 Principles

Rushcliffe Borough Council commits to effectively manage the use of its information and information systems, and therefore anyone given access to Council information systems must:

- Be suitable for their roles.
- Fully understand their responsibilities to assure the security of information.
- Request that access to information and associated systems be removed as soon as it is no longer required.

3.2 Risk

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

Non-compliance with this policy may affect the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

3.3 Assertions

Rushcliffe Borough Council will ensure that individuals are checked to ensure that they are authorised to access Council information systems, as detailed at Appendix A

Rushcliffe Borough Council will ensure that users are trained to use information systems securely, as detailed at Appendix B

Rushcliffe Borough Council will ensure that user access to information systems is removed promptly when the requirement for access ends, as detailed at Appendix C

Access to Council information systems will not be permitted until the requirements of this policy have been met.

3.4 Responsibilities

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

The Chief Information Officer, ICT and HR Managers are responsible for the implementation of this policy.

All users of Council information and associated systems will familiarise themselves with this policy.

4.0 Related Policies, Standards and Guidelines

This policy should be read in conjunction with the:

- Information Security Policy
- Information Classification Policy
- Computer Usage Policy and Guide
- Data Protection Policy
- Network Access Policy
- Remote Access Policy
- Remote Working 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 A of the Information Security Policy.

6.0 Enforcement

Any user or administrator found deliberately contravening this policy or caught jeopardising the security of information that is the property of Rushcliffe Borough Council 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 Appendices

8.1 Appendix A: Providing initial access to Information / Information Systems

8.1.1 Prior to Employment

The Council must ensure that potential users are recruited in line with the Council's Recruitment and Selection Procedures for the roles they are considered for and to reduce the risk of theft, fraud or misuse of information or information systems by those users.

8.1.2 Roles and Responsibilities

Decisions on the appropriate level of access to information or information systems for a particular user are the responsibility of the Information or Systems Owner.

Departmental Heads and Managers are responsible for ensuring that creation of new users, changes in role, and termination of users are notified to the ICT Service Desk in a timely manner.

The information security responsibilities of users are defined and documented in the Computer Usage Policy and Guide and are incorporated into the induction process and contracts of employment. As a minimum this should include a statement that every user is aware of, and understands, the following Council policies:

- Information Security Policy
- Information Classification Policy
- Computer Usage Policy and Guide

8.1.3 User Screening

Background verification checks must be carried out on all employees who are information users, in accordance with all relevant laws, regulations and ethics. The level of such checks must be appropriate to the business requirements, the classification of the information to be accessed, and the risks involved.

The basic requirements for Council employment will be:

- Minimum of two satisfactory references.
- Completeness and accuracy check of employee's application form.
- Confirmation of claimed academic and professional qualifications.
- Identity check against a passport or equivalent document that contains a photograph.

Where a user must be cleared to "Baseline Personnel Security Standard". The following requirements must be met:

- Minimum of 2 satisfactory references.
- Completeness and accuracy check of employee's application form.
- Confirmation of claimed academic and professional qualifications.

- Identity check against a passport or equivalent document that contains a photograph. Identity must be proven through visibility of:
  - A full 10 year passport.
- Or two from the following list:
  - British driving licence.
  - P45 form.
  - Birth certificate.
  - Proof of residence – i.e. council tax or utility bill.
- Verification of full employment history for the past 3 years.
- Verification of nationality and immigration status.
- Verification of criminal record (unspent convictions only). Criminal Records Bureau checks on the user must be carried out to an appropriate level as demanded by law.

All the above requirements for verification checks must be applied to technical support and temporary staff that have access to those systems or any copies of the contents of those systems (e.g. backup tapes, printouts, test data-sets).

8.1.4 Terms and Conditions of Employment

As part of their contractual obligation users must agree and sign the terms of their employment contract, which states their and the Council's responsibilities for information security.

8.2 Appendix B: Ongoing access to Information / Information Systems

8.2.1 During Employment

The Council must ensure that all users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support the Information Security Policy in the course of their work, and to reduce the risk of human error. It is also necessary that user changes in role or business environment are carried out in an orderly manner that ensures the continuing security of the information systems to which they have access.

8.2.2 Management Responsibilities

Line managers must notify the appropriate function, including ICT Services, in a timely manner of any changes in a user's role or business environment, to ensure that the user's access can be changed as appropriate.

Processes must ensure that access to information systems is extended to include new user requirements and also that any access that is no longer needed is removed.

Any changes to user access must be made in a timely manner and be clearly communicated to the user.

Line managers must ensure users understand and are aware of information security threats and their responsibilities in applying appropriate Council policies. The overarching policy is the Information Security Policy and within that document are details of related policies and guidelines

8.2.3 User Screening

Where a user must be cleared to "Baseline Personnel Security Standard", the following checks must be undertaken for existing employees prior to access being provided:

- Identity check against a passport or equivalent documents. Identity must be proven through visibility of:
    - A full 10 year passport.
    - Or two from the following list:
        - British driving licence.
        - P45 form.
        - Birth certificate.
        - Proof of residence – i.e. council tax or utility bill.
- Verification of criminal record (unspent convictions only). Criminal Records Bureau checks on the user must be carried out to an appropriate level as demanded by law.

8.2.4 Information Security Awareness, Education and Training

All users must receive appropriate information security awareness training and regular updates in related statute and organisational policies and procedures as relevant for their role.

It is the role of line managers to ensure that their staff are adequately trained and equipped to carry out their role efficiently and securely.

8.3 Appendix C: Termination of access to Information / Information Systems

8.3.1 Secure Termination of Employment

Termination of employment may be due to resignation, change of role, suspension or the end of a contract or project. The key requirement is that access to Rushcliffe Borough Council information assets is removed in a timely manner when no longer required by the user.

8.3.2 Termination Responsibilities

Line managers must notify the ICT Service Desk in a timely manner of the impending termination or suspension of employment so that their access can be suspended.

ICT Service Desk must notify the appropriate system owners who must suspend access for that user at an appropriate time, taking into account the nature of the termination.

Responsibilities for notifying changes, performing employment termination or change of employment must be clearly defined and assigned.

8.3.3 Return of Assets

Users must return all of the organisation's assets in their possession upon termination of their employment, contract or agreement. This must include any copies of information in any format.

It is the role of line managers to ensure their staff return these assets on or prior to the last day of employment

8.3.4 Removal of Access Rights

All access rights of users of Council information systems will be removed in a timely manner upon termination or suspension of their employment, contract or agreement.

Emergency suspension of a user's access will be implemented when that access is considered a risk to the Council or its systems.

9.0 Document Attributes

Document Information

Title	User Access Policy
Identifier	User Access Policy
File Location	
Description	Policy determining the user access rights to Council information and information systems
Keywords	Policy; User Access Rights; Information; Information Systems
Format	MS Word
Author	Greg Dwyer
Owner	Chief Information Officer
Classification	OFFICIAL
Date Created	27th August 2010
Last Review Date	Sept 2022
Next Review Date	March 2023
Date to Dispose	12 months after later version of policy released

Document History

Date	Summary of Changes	Version
26/03/10	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
27/08/2010	Third draft following review of second draft by Deputy Chief Executive, Head of Corporate Services and ICT Manager on 26/07/2010	0.3
23/09/2014	Updated to reflect changes to organisation	0.4
17/03/2016	Updated to reflect changes to organisation	0.5
16/03/2017	Amended appendices naming to conform with corporate std	1.0
02/03/2018	Amended job titles and ensure GDPR compliant	1.1
20/03/2018	Final review and update by CIO	1.2
21/03/2019	Removed references to Third Party Access. Third Party Access covered by Third Party Access Policy	1.3
07/04/2020	Reviewed, no changes	1.4
16/03/2021	Removed redundant references to GCSx	1.5
27/09/2022	Reviewed, no changes	1.6

Document Approval

Date	Name & Job Title of Approver(s)	Version
20/03/2018	Ken Thompson CIO	1.2

Distribution

Name / Group	Title
Executive Managers	

Coverage

Group
All Employees

All Members
All Contractors & third party Agency staff

End of Document