Policy Document

Human Resources Information Security Standards

[23/08/2011]

Document Control

Organisation	Redditch Borough Council
Title	Human Resources Information Security Policy
Author	Mark Hanwell
Filename	Human Resources Information Security.doc
Owner	Mark Hanwell – ICT Transformation Manager
Subject	Human Resources Information Security Policy
Protective Marking	Unclassified
Review date	23/08/2011

Revision History

Revision Date	Revisor	Previous Version	Description of Revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Head of Business Transformation	Deborah Poole	23rd August 2011

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contents

1 Policy Statement

Redditch Borough Council will ensure that individuals are checked to ensure that they are authorised to access Council information systems.

Redditch Borough Council will ensure that users are trained to use information systems securely.

Redditch Borough Council will ensure that user access to information systems is removed promptly when the requirement for access ends.

2 Purpose

Redditch Borough Council holds large amounts of personal and RESTRICTED information. 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 also be enforced and applied by people, and this policy addresses security issues related to people.

The procedures accompanying this policy are split into 3 key stages of a user's access to information or information systems used to deliver Council business:

1. Prior to granting access to information or information systems - checks must be made to ensure that the individual is suitable for access to Council information systems.
2. The period during access to information or information systems - users must be trained and equipped to use systems securely and their access must be regularly reviewed to ensure it remains appropriate.
3. When a user's requirement for access to information or information systems ends (i.e. when a user terminates their employment with the Council, or changes their role so that access is no longer required) - access needs to be removed in a controlled manner.

This policy also addresses third party access to Council information systems (e.g. contractors, service providers, voluntary agencies and partners).

3 Scope

This policy applies to any person that requires access to Council information systems or information of any type or format (paper or electronic).

The policy applies automatically to all Redditch Borough Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council.

Where access is to be granted to any third party (e.g. contractors, service providers, voluntary agencies, partners) compliance with this policy must be agreed and documented. Responsibility for ensuring this lies with the Council employee that initiates this third party access.

4 Definition

Redditch Borough Council understands that to reduce the risk of theft, fraud or inappropriate use of its information systems, anyone that is given access to Council information systems **must**:

- Be suitable for their roles.

- Fully understand their responsibilities for ensuring the security of the information.
- Only have access to the information they need.
- Request that this access be removed as soon as it is no longer required.

This policy must therefore be applied prior, during and after any user's access to information or information systems used to deliver Council business.

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

5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6 Applying the Policy

For information on how to apply this policy, readers are advised to refer to Appendix 1.

7 Policy Compliance

If any user is found to have breached this policy, they may be subject to Redditch Borough Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or ICT.

8 Policy Governance

The following table identifies who within Redditch Borough Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	ICT Transformation Manager
Accountable	Head of Business Transformation
Consulted	Corporate Management Team
Informed	All Council Employees, All Temporary Staff, All Contractors etc

9 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the ICT Transformation Manager

10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- Email Policy.
- Internet Acceptable Usage Policy.
- Software Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- IT Access Policy.
- Information Protection Policy.
- Information Security Incident Management Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy;

- Computer, Telephone and Desk Use Policy.
- Remote Working Policy.
- Removable Media Policy.
- Legal Responsibilities Policy.
- Communications and Operation Management Policy.
- IT Infrastructure Policy.

11 Key Messages

- Every user must be aware of, and understand, the following policies:
    - Information Protection Policy.
    - Email Policy.
    - Internet Acceptable Usage Policy.
    - Software Policy.
    - GCSx Acceptable Usage Policy and Personal Commitment Statement.
    - IT Access Policy.
    - Information Security Incident Management Policy.

- Background verification checks must be carried out on all users.
- Users who require access to PROTECT and RESTRICTED information and / or require use of the Government Connect Secure Extranet (GCSx) email facility **must** be cleared to "Baseline Personnel Security Standard".

- 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.
- Processes must be implemented to ensure that all access rights of users of Council information systems shall be removed in a timely manner upon termination or suspension of their employment, contract or agreement.

Appendix 1

A1 Applying the Policy – Prior to Access to Information or Information Systems

A1.1 Prior to Employment

The Council must ensure that potential users are recruited in line with the Council's Recruitment and Selection Policy 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. These requirements are corporate in nature

A1.2 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 Asset Owner – please refer to the Information Protection Policy.

Line managers are responsible for ensuring that creation of new users, changes in role, and termination of users are notified to the ICT. Helpdesk in a timely manner, using an agreed process.

The information security responsibilities of users must be defined and documented and incorporated into induction processes and contracts of employment. As a minimum this will include:

- A statement that every user is aware of, and understands, the following Council policies:
    - Information Protection Policy
    - Email Policy
    - Internet Acceptable Usage Policy.
    - Software Policy.
    - GCSx Acceptable Usage Policy and Personal Commitment Statement.
    - IT Access Policy.
    - Information Security Incident Management Policy.

A1.3 User Screening

Background verification checks must be carried out on all potential 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 must 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.

Users who require access to PROTECT and RESTRICTED information and / or require use of the Government Connect Secure Extranet (GCSx) and email facility **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.

Where access is to systems processing payment card data, credit checks on the user must be carried out to an appropriate level as required by the Payment Card Industry Data Security Standards (PCI-DSS).

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).

A1.4 Terms and Conditions of Employment

As part of their contractual obligation users must agree and sign the terms of their employment contract, which shall state their and the Council's responsibilities for information security. This must be drafted by the Council's lawyers and must form an integral part of the contract of employment.

Each user must sign a confidentiality statement that they understand the nature of the information they access, that they will not use the information for unauthorised purposes and that they will return or destroy any information or assets when their employment terminates.

A2 Applying the Policy – During Access to Information or Information Systems

A2.1 During Continued 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 organisational 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.

A2.2 Management Responsibilities

Line managers must notify the appropriate function 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.

Departmental managers must require users to understand and be aware of information security threats and their responsibilities in applying appropriate Council policies. These policies include:

- Information Protection Policy.
- Information Security Incident Management Policy.

This requirement must be documented.

A2.3 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 Departmental managers to ensure that their staff are adequately trained and equipped to carry out their role efficiently and securely.

A3 Applying the Policy – When Access to Information or Information Systems is No Longer Required

A3.1 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 Redditch Borough Council information assets is removed in a timely manner when no longer required by the user.

A3.2 Termination Responsibilities

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

ICT Helpdesk 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.

A3.3 Return of Assets

Processes must be implemented to ensure that users 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.

A3.4 Removal of Access Rights

Processes must be implemented to ensure that all access rights of users of Council information systems shall be removed in a timely manner upon termination or suspension of their employment, contract or agreement.

Processes and responsibilities must be agreed and implemented to enable emergency suspension of a user's access when that access is considered a risk to the Council or its systems as defined in the Information Security Incident Management Policy.