**Use of *Freedom of Information Database***
**Code of Practice**

## Introduction

This code of practice is intended to support the Information Security Policy of the University and should be read in conjunction with this document.

http://www.ed.ac.uk/schools-departments/information-services/about/policies-andregulations/security-policies/security-policy

This code of practice is also qualified by The University of Edinburgh computing regulations, found at:

http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations

## 1. Code of Practice Version

| Revision Date | CoP Version | Template Version | Author | Notes |
|---|---|---|---|---|
| 26/09/2011 | Version 1.1 | Version 1.3 | M Gallagher | First submitted to IT Security Working Group |
| 18/11/2011 | Version 1.2 | Version 1.4 | M. Gallagher | Minor changes requested by ITSWG |
| 10/2/2015 | Version 1.3 | Version 1.5 | S Cranston | Updated to reflect current practice and changes to RMS |
| 6/05/2015 | Version 1.4 | Version 1.6 | S Cranston | Updated to incorporate comments from IS Applications |

| QA Date | QA Process | Notes |
|---|---|---|
| **14 Jul 2015** | **ITC Security Working Gp** | |

| Suggested date for Revision of the CoP | Author |
|---|---|
| 01/06/2017 | S Cranston |

## 2. System description

| | | |
|---|---|---|
| 2.1 | System name | *Freedom of Information Database* |

| | | |
|---|---|---|
| 2.2 | Description of system | *The Freedom of Information Database is divided into two sections: the publication scheme database (which allows the information published by the University as a matter of routine to be maintained), and the information request monitoring database (which allows requests for University information to be logged and tracked).*<br><br>*It enables the University to fulfill its requirements under the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004 and the Data Protection Act 1998.* |
| 2.3 | Data | *The publication scheme database contains URL links to data which the University routinely makes available. It also contains data about members of staff that are responsible for updating this information. The request monitoring database contains data which the University uses to track and respond to information requests. This includes each request itself, contact details of applicants, the members of staff that deal with each request, and information about the steps involved in the handling of each request The database therefore contains some medium risk information.* |
| 2.4 | Components | *Publication scheme database and information request monitoring database. Uses Oracle Corporate Database.* |
| 2.5 | System owner | *Records Management Section (RMS). Operational responsibility exercised locally by Assistant Records Manager.* |
| 2.6 | User base | *RMS (7 members of staff), Freedom of Information Promoters and Freedom of Information Practitioners. As of February 2015 there were 6 Promoters and 152 Practitioners.* |
| 2.7 | Criticality | *Low* |
| 2.8 | Disaster recovery status | *System designated Priority 3 status in IS Applications Disaster Recovery Plan.*<br>*Business Continuity Plan outlined in relevant section below.* |

## 3. User responsibilities

| | | |
|---|---|---|
| 3.1 | Data | *Users have a duty to enter relevant and not excessive data into the database and ensure that any data gleaned from it are appropriately secured.*<br>*Publication scheme information is intended for public exposure. Unauthorised alteration of publication scheme data is therefore the primary security concern, although this is not considered high risk. Measures to mitigate this risk are in place. User authorisation is conducted by the Records Management Section, access to the database is EASE authenticated and any changes are subject to a double approval process.*<br>*Personal data are held in the request monitoring database, including details of applicants (name, contact details and address) and practitioners. Staff need to be aware of their responsibilities for handling personal data.*<br>*Care should be taken to ensure personal data or sensitive business information that is printed out is not left lying in public areas.*<br>*Staff changing job must email recordsmanagement@ed.ac.uk so that access to data may be amended or terminated. Any concerns regarding the use of data should be reported directly to recordsmanagement@ed.ac.uk* |
| 3.2 | Usernames and passwords | *Access is EASE authenticated.* |
| 3.3 | Physical security | *Users must ensure they log out when finished using the database or lock computer when away from desk. Last person out of the office should lock door.* |
| 3.4 | Remote/mobile working | *Both sections of the database are accessed via a web interface - access beyond the firewall must only be done in a secure manner approved by the University.*<br>*Users must ensure they log out correctly when ending a session.*<br>*Users must adhere to the University policy on the storage, transmission and use of personal data and sensitive business information outwith the University computing environment, and take security precautions when using mobile devices or otherwise accessing the database in public.* |
| 3.5 | Downloads and removal of data from premises | *Care must be taken to ensure that data taken off site, downloaded or provided to third parties are maintained in a secure environment.*<br>*Data is extracted from the request monitoring database for reporting purposes by the Records Management Section, using BI SUITE* |

| | | |
|---|---|---|
| 3.6 | Authorisation and access control | *Records Management Section authorise new users and assign access levels. Access levels are determined by job function.*<br>*Records Management Section maintain list of relevant staff to determine whether access should be granted and what level of access should be allocated.*<br>*There are two levels of access:*<br>*Admin: allocated to RMS. Enables users to create, view and edit all entries in the publication scheme and request monitoring databases.*<br>*Practitioner: allocated to Freedom of Information Promoters and Practitioners. Enables users to create, view and edit only the entries of their unit in the publication scheme and request monitoring databases.* |
| 3.7 | Competencies | *It is the responsibility of all users to ensure they have sufficient knowledge and understanding of database procedures and processes prior to using the system.*<br>*A detailed user guide is available at: http://www.ed.ac.uk/schools-departments/records-management-section/freedom-of-information/publication-scheme/manual/overview and http://www.ed.ac.uk/schools-departments/records-management-section/freedom-of-information/request-handling-procedures/request-monitoring-manual*<br>*A 'Help' function is accessible on all screens of the database.*<br>*Specific training can be requested from recordsmanagement@ed.ac.uk* |

## 4. System Owner Responsibilities

| | | |
|---|---|---|
| 4.1 | Competencies | *RMS must maintain an accurate record of Freedom of Information Promoters and Practitioners to regulate access appropriately. Assistant Records Manager responsible for database maintenance locally and escalating issues where appropriate.* |
| 4.2 | Operations | *The physical and operational security of the database is a delegated responsibility of IS Applications.* |
| 4.3 | System documentation | *System documentation is held by IS Applications. It is the responsibility of the Records Management Section to ensure all user documentation is prepared and kept up to date.* |
| 4.4 | Segregation of Duties | *RMS (authorising and administering user access, deciding upon content, suggesting updates, reporting faults).*<br>*IS Applications (maintaining and securing technical infrastructure).* |
| 4.5 | Security incidents | *All security incidents should be reported to IS Applications, who will decide on the most appropriate course of action.* |
| 4.6 | Fault/problem reporting | *All incidents reported via UniDesk in the first instance and escalated as appropriate if first line resolution is not possible.* |
| 4.7 | Systems development | *IS Applications is responsible for system development.* |

## 5. System Management

| | | |
|---|---|---|
| 5.1 | User account management | *After the authorisation process has been completed, user accounts are created by the Records Management Section through the database interface. Accounts are disposed of by the allocation of an 'Active to' date, after which it will become inactive. Account details are not deleted from the system altogether as individual practitioners are linked to the requests they deal with. Removing user details altogether will result in an incomplete audit trail and the possible loss of requests associated with a non-current practitioner.* |
| 5.2 | Access control | *Access is controlled by EASE authentication and linking appropriate access privileges to users' accounts.* |
| 5.3 | Access monitoring | *Access is not monitored.* |
| 5.4 | Change control | *Changes proposed by RMS, agreed with IS Applications and carried out via UniDesk.*<br>*Changes applied on three levels:*<br>*Development (by IS Applications for initial development work); Test (by RMS via the internet to test and comment on changes); and the Live site.* |
| 5.5 | Systems clock synchronisation | *Delegated to IS - Network Time Protocol daemon and highly accurate clocks used to keep servers synchronised.* |
| 5.6 | Network management | *n/a* |
| 5.7 | Business continuity | *Back up copy of publication scheme database held by RMS and updated on an annual basis.*<br>*Process in place for dealing with information requests if database is not functional. In addition to the database we have information about requests on our shared drive. Requests could be monitored using a spreadsheet as a short term measure if the database wasn't available. If no computing facilities were available, we could monitor requests, to some extent, on paper.*<br>*Backup of database held at King's Buildings. Oracle database backed up daily, to server and tape, as well as offsite.* |
| 5.8 | Security Control | *Security is a delegated responsibility of IS Applications. Strict security is in place – this is based on distinction of database and application tiers, firewalls, encryption and a variety of security standards adhered to by IS. IS security and access arrangements are regularly reviewed externally.* |

## 6. Third Party

| | | |
|---|---|---|
| 6.1 | Outsourcing | *Database is not outsourced - responsibility for the security of the database is not shared with any third parties.* |
| 6.2 | Contracts and Agreements | *n/a* |
| 6.3 | Compliance with the university security policy | *n/a* |
| 6.4 | Personal data | *n/a* |