Use of Voyager
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-and-regulations/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

This code of practice is intended to ensure the security of the University's Library Management system¹ by providing users and systems managers with an overview of their responsibilities in managing and using Voyager.

1 Code of Practice Version

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>CoP Version</th>
<th>Template Version</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>18/09/2011</td>
<td>Version 1.0</td>
<td>1.4te here</td>
<td>C Watt</td>
<td>Update to new template at request of internal audit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QA Date</th>
<th>QA Process</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>19/09/2011</td>
<td>Security Committee</td>
<td>This document has already been signed off by the Security Committee but is being represented in the new template format.</td>
</tr>
</tbody>
</table>

Suggested date for Revision of the CoP | Author
18/09/2014 | C Watt

2 System Description

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>System Version</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>18/09/2011</td>
<td>7.1</td>
<td>C Watt</td>
<td>Update to new template at request of internal audit</td>
</tr>
</tbody>
</table>

2.1 System Name | Library Management System (Voyager)

2.2 Description of System

The Voyager Integrated Library System is used to manage the workflow of library materials purchase, cataloguing and circulation of items from UoE’s collections.

The core workflow system (for staff use) comprises acquisitions, cataloguing, and circulation modules.

¹ Voyager is the library management system which covers acquisitions, cataloguing, circulation, and online public access catalogue modules.
Catalogued items can be browsed & searched by staff and public via the web-based Online Public Access Catalogue (OPAC). Self Check functionality allows users (Patrons) to check-in and check-out their own items via the 3M devices in the various library sites.

<table>
<thead>
<tr>
<th>2.3 Data</th>
<th>Voyager contains personal details of staff, student and members of other patron groups, including contact details, and their borrower records including incurred fees.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4 Components</td>
<td>Voyager is a package provided by Ex Libris Group and is based on an Oracle DBMS; Modules include Acquisitions, Cataloguing, Circulation, OPAC (Online Public Access Catalogue), Self Check, SysAdmin.</td>
</tr>
<tr>
<td>2.5 System Owner</td>
<td>Information Systems Manager, L&amp;C Digital Library Section.</td>
</tr>
<tr>
<td>2.6 User base</td>
<td>Workflow staff (UoE staff who use the client applications to add and update records to manage acquisitions, cataloguing, and circulation activities); UoE reference staff (UoE staff who use the client applications on a readonly basis for reference or to deal with patron enquiries); Patrons (staff and students who borrow items from UoE’s libraries); General Public (world wide use of OPAC).</td>
</tr>
<tr>
<td>2.7 Criticality</td>
<td>High.</td>
</tr>
<tr>
<td>2.8 Disaster Recovery Status</td>
<td>A disaster recovery plan is in place and has been tested. The plan is reviewed on an annual basis.</td>
</tr>
</tbody>
</table>

### 3 User Responsibilities

| 3.1 Data | Users have a duty to safeguard their password.  
Patron records contain personal information including one or more addresses and phone numbers. Staff who access personal data need to be aware of their responsibilities handling such data.  
Staff changing job must email information.systems@ed.ac.uk so that access to data may be amended or terminated. |
|----------|-------------------------------------------------------------------------------------------------------------------------------------|
| 3.2 Usernames and passwords | Passwords should be set, used and maintained in accordance with the University Computing Regulations and Voyager security.  
Users must only log into Voyager suing their own username and password.  
Passwords should not be written down.  
Passwords should never be divulged to anyone and never given in response to an email message. |
| 3.3 Physical Security | Users must ensure they log out from Voyager client applications or lock computer when away from desk.  
Last person out of the office should lock door. |
| 3.4 Remote/Mobile working | Access beyond the firewall must only be done in a secure manner approved by the University.  
Users must ensure they log out correctly when ending an Voyager session.  
Staff using the voyager client applications on a mobile device (eg cataloguing, using a laptop) must take measures to ensure that applications are not left running if the device is left unattended, to prevent |
| 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 is maintained in a secure environment.  
• Advice about the secure transfer of Voyager data is available from information.systems@ed.ac.uk |
| 3.6 Authorisation | • Levels of access for end users is usually determined by job function.  
• Each operator who uses a Voyager staff module must have an Operator Profile containing a name, operator ID, and password. The system requires operators to log in to Voyager staff modules by entering their operator ID and password (both case-sensitive).  
• Access to authorised areas requires approval from the user’s module head; Any concerns about unauthorised use should be reported to information.systems@ed.ac.uk |
| 3.7 Competencies | • It is the responsibility of all users to ensure they have sufficient knowledge and understanding of Voyager procedures and processes prior to using the system.  
• Detailed user guides are available via the L&C Information Systems Team wiki; specific training can be requested from information.systems@ed.ac.uk |

4 System Owner Responsibilities

IS (Library & Collections) is the owner of the Library Management System (Voyager) and as such has a duty to ensure the following guidance is followed in respect of its responsibilities as the system owner, system manager and owner of the relationship with Ex Libris Group, the third party provider of the application software. Several areas of responsibility for support have been assumed by the L&C Digital Library Section.

| 4.1 Competencies | Ex Libris has a specialist support team, however it is normally only necessary to escalate the most serious (system down type) incidents to them; 1st and 2nd line support has been handled by the Digital Library since 1999; as part of the IS help and support review responsibility for some aspects of 1st line support are in the process of being transferred to IS Helpline. The Information Systems Team focus is on 2nd line incident and problem management. The Information Systems Team assist the production of 1st and 2nd line troubleshooting procedures. |
| 4.2 Operations | The physical security of the Voyager infrastructure is a responsibility of the IS ITI-Unix section. |
| 4.3 System Documentation | It is the responsibility of the L&C Information Systems team to ensure all system documentation is prepared and kept up to date. |
| 4.4 Segregation of Duties | • ITI-Unix staff (Hardware and OS platform configuration)  
• DLS Information Systems Team (Application config and management)  
• Ex Libris (Incidental Troubleshooting, also some DBMS work due to maintenance & support agreement). |
4.5 Security incidents
All security incidents should be reported to the information.systems@ed.ac.uk who will investigate by liaison with the ITI-Unix team.

4.6 Fault/problem reporting
All incidents should be reported to the IS helpline in the first instance and escalated via UniDesk to the Digital Library Information Systems Team as appropriate if 1st line resolution is not possible.

4.7 Systems Development
All upgrades and change requests are prioritised and scheduled via L&C’s annual workplanning process. Core systems development is carried out by Ex Libris in Des Plaines, Illinois, USA; local development of add-ons to improve functionality is carried out using appropriate frameworks including Java, RAILS, Perl, html, CSS, or web-based reporting using JasperReports; end-user data reporting is currently done with MS Access.

5 System Management

5.1 User Account Management
Access to authorised areas requires approval from the user’s module head and a request to information.systems@ed.ac.uk

A permanent Operator Profile, named System Administrator, acts as control profile for access to the System Administration module. This Operator ID and Password are known to Ex Libris customer support staff as operational backup to the DLS Information Systems Team.

5.2 Access Control
Appropriate access to system-level users is agreed between the Information Systems Manager and the ITI-Unix section. Passwords for service accounts (used by UoE staff and Ex Libris support and upgrades staff) are managed by the Information Systems Manager; access to service account passwords is on a need to know basis, and is regularly reviewed; passwords are frequently changed.

5.3 Access Monitoring
User logs are monitored and unusual events are escalated for action.

5.4 Change control
Application level configuration changes or patches are carried out either by the Information Systems Team or Ex Libris; System level configuration changes are normally carried out by ITI-Unix section or IST, as appropriate; IST changes are documented in UniDesk and signed off by the team manager; ITI-Unix changes are agreed and approved within CMS; all changes made by Ex Libris are to be agreed in advance with the Information Systems Manager and also documented on Ex Libris’s call management system.

5.5 Systems Clock Synchronisation
ntpd is run via root’s crontab at least daily.

5.6 Network Management
n/a

5.7 Business Continuity
In the case of total failure of both DBMS and Application servers, or destruction of the physical environment, business continuity can be maintained via a pre-configured DR environment; depending on the impact of a given incident, it may be necessary to agree a level of reduced availability, depending on platform capacity, and each
customer’s circumstances and priorities at the time.

Business continuity procedures are documented on the ITI-Unix wiki and the L&C Information Systems Team wiki.

### 6 Third Party

<table>
<thead>
<tr>
<th>6.1 Outsourcing</th>
<th>n/a</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2 Contracts and Agreements</td>
<td>Voyager is provided by Ex Libris; UoE is licensed for use and for annual maintenance (original agreements were signed with Endeavor, subsequently bought by Ex Libris).</td>
</tr>
<tr>
<td>6.3 Compliance with the University security policy</td>
<td>A contract with the supplier has been in place for 12 years and was based on standard university terms and conditions at the time. At no point has compliance been an issue and the supplier is not considered a risk. Ex Libris agree to comply with IS L&amp;C’s established change control procedures; it is intended that the university security policy is regularly reviewed and the supplier is expected to agree to comply with it and this CoP.</td>
</tr>
<tr>
<td>6.4 Personal Data</td>
<td>Ex Libris is registered as a “safe harbour” for circumstances where data might ever be required to be stored outside UoE’s infrastructure (for example, troubleshooting data integrity).</td>
</tr>
</tbody>
</table>