

evince documentation
Technical Infrastructure



Trust Court, The Vision Park, Histon, Cambridge CB24 9PW

01223 566522

<http://www.evince-online.com/>

evince@opp-links.org.uk



Document control

Authors: Giles Thurston
Owner: Giles Thurston
Date: April 2008
Version: 1.0
Sensitivity: Unrestricted

Date	Who	Detail	Version
07/04/2008	Giles Thurston	Public version	1.0

1 The Hosting Environment

Opportunity Links provides professional hosting services to a number of clients via an environment located in a secure, purpose built, state-of-the-art data centre in London Docklands. It is in this environment that the evince application will be hosted.

As an organisation, we mitigate any risks to the delivery of our hosting service by working in partnership with recognised world class providers of third-party services, using best-of-breed technologies and applying industry best practices throughout.

Opportunity Links has selected Claranet for the provision of its data centre facilities and high capacity bandwidth.

The London data centre is equipped with the latest fire control and suppression technology, redundant water-cooled Heating, Ventilating and Air Conditioning (HVAC) and humidity control systems as well as power surge protection, with onsite Uninterruptible Power Supply (UPS) and generators to ensure the continuous operation of our hosting architecture.

Physical access to the data centre is controlled by 24-hour manned security, restricted access lists and swipe cards. Unified video surveillance with an access-control system, security breach alarms with access monitoring, and heat sensors further bolster the building's extraordinary safety. In addition, each of the server racks has its own combination lock.

The high-speed, low latency, resilient network infrastructure ensures bandwidth capacity, reliability and optimal service levels. Using a robust architecture based on proven, best-of-breed hardware with multiple metropolitan fibre rings, Claranet provides mission critical levels of connectivity nationally.

Hardware

Opportunity Links standardise on a single, best-of-breed hardware vendor for each class of hardware to maximize efficiency, support knowledge and vendor response.

All server hardware used is HP with most deployments based on the latest Blade technology ensuring operational efficiency.

All networking devices are Cisco (the worldwide leader in networking for the Internet) ensuring both leading-class performance and compatibility.

Hardware is supported under a CalyX (formally ServiceTec) hardware agreement based on varying levels of response up to 4 hour *fix* 24 x 7 x 365 and is actively monitored by a dedicated

hardware management platform to proactively tackle issues before they become critical.

Software tools

The core hosting environment is built on Microsoft software. Microsoft's ubiquitous nature maximises its interoperability with other architecture components and assures its continued upgrading in line with current industry best practice.

Additional best-of-breed software, tools and solutions have been chosen to enhance the core software platform where needed. These are backed by vendor support agreements which provide comprehensive backup when needed.

Software is implemented to the latest versions to ensure reliability and to guard against vulnerabilities; it is actively monitored by a dedicated software management platform to proactively tackle issues before they become critical.

Availability Management

Opportunity Links' leading-edge server farm incorporates multiple levels of resilience which has been engineered to reduce the impact of single points of failure.

Each server has many resilient components (such as redundant hard drives, network interfaces, fans, power supplies, etc.) to protect against a complete server failure. However, all services have been designed to withstand such an event through the implementation of failover clusters and n+1 load balanced clusters to ensure high availability and scalability.

Capacity Management

Opportunity Links aims to run all its systems at around 85% capacity, to allow contingency for demand spikes, while providing value for money, and wherever possible the capacity of the infrastructure will have built-in allowances for unanticipated variances in demand, such as the burstable bandwidth agreement with our network provider.

Examples of systems currently hosted by Opportunity Links include:

- Website: ChildcareLink – a central government website drawing over 15 million hits and 3 million page views per month.
- Web Service: Parent Centre – a central government web service answering over 300 thousand transactions and transferring over 400MB of data per month

- **Application:** a line-of-business application delivered over the Internet to over 150 local authorities with around 500 concurrent users.

2 Quality Processes

Opportunity Links has implemented the OGC's ITIL best practice throughout our core IT processes and is also ISO27001 compliant, ensuring our security procedures and processes are regularly audited by an external auditor.

Opportunity Links technical staff are fully trained on the technologies deployed and hold professional qualifications, including MCSE (Microsoft Certified Systems Engineer), MCSA (Microsoft Certified Systems Administrator) and CCNA (Cisco Certified Network Associate).

ISO27001

Opportunity Links' is aware that public facing information is comprised of valuable assets that need to be continually and appropriately protected. One of the key objectives of information security is to protect these assets from threats which may endanger them. Information security can be characterised as the preservation of:

- **Confidentiality** - ensuring that access to information is appropriately authorized
- **Integrity** - safeguarding the accuracy and completeness of information and processing methods
- **Availability** - ensuring that authorised users have access to information when they need it

Opportunity Links hold the ISO27001 accreditation, an internationally recognised standard for IT systems security. To support this, Opportunity Links has a variety of internal security procedures and policies covering both the data centre and our internal infrastructure, to ensure information security is maintained at all times. There is a permanent security manager role within the organisation, a regular security forum and processes in place to rapidly escalate any issues to senior management if required.

All these procedures are independently audited twice a year to ensure that they are correctly implemented and that amendments to business processes or activities are reflected within the security infrastructure of the organisation.

Data Protection

All Opportunity Links staff are Criminal Records Bureau (CRB) checked upon joining the company, and access to the data and IT systems is given strictly on a need only basis via industry standard secure technologies such as Virtual Private Networks (VPNs), Intrusion Detection Systems (IDS), Firewalls and enterprise-wide

anti-virus software. Live systems are physically segregated from development and office environments to enhance security. All changes to the live environment are tightly controlled through a change and release management process.

All hosted databases have a backup and recovery strategy designed to suit the use of the database. If databases are updated on a frequent or constant basis then this would usually extend to a backup strategy that would allow rollbacks to a particular point in time. For example, if an incorrect update was made and it was found to have been made at 3:07pm the previous day, the database could be rolled back to 3:06pm to minimise the amount of data lost.

All databases are regularly maintained. Tasks performed include

- the re-building of table indexes;
- the updating of database statistics; and
- the running of database integrity checks.

These tasks are run automatically to ensure the databases continue to store and process data efficiently.

To ensure that databases continue to function efficiently as the quantity of data grows, and potentially as their usage changes, database performance is checked periodically to ensure indexes are optimised and queries are running efficiently. To this end we also have automatic processes which monitor the size of the database and the free space remaining within them.

Backups are performed daily using the latest software and automated hardware technology, stored on high-capacity tape.

Tapes are kept secure at all times and rotated on a regular basis. Offsite backups are held securely at our main office and all employees are trained on the relevant aspects of data protection legislation.