KENSINGTON & CHELSEA AND WESTMINSTER LIBRARIES & ARCHIVES

INFORMATION SHARING AGREEMENT

1.1 General

Kensington & Chelsea and Westminster Libraries & Archives is a grouping of public library authorities who cooperate together to provide enhanced library services for members of the public. This shared service is primarily achieved by each member using the same Library Management System to store membership data, the library stock holdings and the transactional data when a library member borrows an item.

The Information Sharing Agreement of Kensington & Chelsea and Westminster Libraries & Archives (ISA) has been drawn up to ensure that all constituent members are aware of the basis on which the personal data of public library members is both stored and shared.

The ISA has been drawn up to demonstrate to users that their personal data is correctly managed and that the constituent members are confident that appropriate steps have been taken to seek to protect them from legal challenge. The ISA is on the website and the home page of the Enterprise online library catalogue of each constituent member. This is so it can be viewed by members of the public who are members of a library service of the constituent members. It should also give reassurance to customers that we manage their personal data, only as described.

Kensington & Chelsea and Westminster Libraries & Archives work together to provide a shared service by the loaning of library items to its members in partnership with SirsiDynix, who provide the Library Management System software, known as Symphony.

1.2. Objectives

- To ensure that Kensington & Chelsea and Westminster Libraries & Archives adopt a consistent approach
- To ensure that library members can have confidence in how the constituent members manages personal data
- To ensure that the Information Sharing Agreement conforms to current best practice in information management between partners
- To ensure that the processing of personal information is carried out in compliance with the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR)
- To ensure that adequate security arrangements are in place relating to user information

Obligations and duties of Kensington & Chelsea and Westminster Libraries & Archives

- It is incumbent on all constituent members to ensure that all authorised personnel* manage the personal data to which they have access
- In accordance with the DPA, unauthorised personnel are unable to access customer membership records via the Library Management System
- All constituent members must ensure that the personal data held is managed in such a way as to meet current good practice and legal obligations
- All constituent members will ensure that partner organisations delivering services and managing information on their behalf comply with the required legislation and sign information sharing agreements with the responsible library authority

- All members must notify the other constituent members, at the earliest possible opportunity, if any issues arise which impact on the operation of the Information Sharing Agreement

Benefits to the constituent members

- By adherence to the Information Sharing Agreement, each constituent member knows the basis on which the other constituent members manage the personal data which is shared across Kensington & Chelsea and Westminster Libraries & Archives
- All constituent members know that the assessment of risk of sharing personal data is reflected in the operation of the Library Management System within the Information Sharing Agreement

Benefits to the Public

- Library members know on what basis personal data is managed within Kensington & Chelsea and Westminster Libraries & Archives and that it will not be shared with any 3rd party outside the constituent members. This does not preclude individual each authority sharing the data within their authority, so long as library members are made aware of this and give their formal consent
- Library members know what safeguards are in place to protect personal data within Kensington & Chelsea and Westminster Libraries & Archives

1.3. Operation of the ISA

An agreed basis on which the constituent members manage and share membership data will provide a robust and reliable system and process by which data is stored and managed and shared across Kensington & Chelsea and Westminster Libraries & Archives.

Kensington & Chelsea and Westminster Libraries & Archives operate on the basis of any person joining any one of the constituent library services being able to use their “home” membership card to access the joint resources of all Libraries & Archives and all stock – books, eBooks, talking books, DVDs and CDs and online resources.

Legally, library members can join library services if they live, work or study in a locality so there is the potential for people to access services from three different points.

At any library within Kensington & Chelsea and Westminster, employed staff need to be able to check member details to confirm membership and to identify any previous matters affecting current usage.

1.4. Information to be shared

Member information – name, address, contact details, date of birth, faith, sexuality, disability, language and ethnic origin (if recorded) plus details of items borrowed and any outstanding debts to any constituent member. It is recognised that Kensington & Chelsea and Westminster Libraries & Archives operate differing membership arrangements.

Information is obtained from the library member at the point of joining for the purpose of recording membership details. Consent for information processing is required as part of the membership application.

The information is not made available to any Third Party except the other constituent members (and within that authority) and their contracted partners, except where the Police or Security Services have lodged a formal request or functionality has been selected by the Libraries & Archives such as payment card processing.

Information would primarily be used either to support the library members use of the service, e.g. the library member does not have their membership card and wishes to borrow an item OR a library member has run up debts to one of the constituent members which the other constituent members need to be aware of. It data is used in any other way it should only be within the same authority and for activities for which the member has given explicit consent.

1.5. Data Protection Act and General Data Protection Regulations

Each constituent member will operate under the terms of the DPA 2018 and the GDPR ensuring that only designated staff release any data covered by the Act.

The release of data will be governed by constituent member authority rules on releasing data.

1.6. Process

The data is held on a database as part of the Library Management System which is a shared system across all constituent members.

As the data is held on a shared management system to which authorised staff have access, the access is immediate. Data on a library member does not require extraction or transfer in the normal sense.

Authorised personnel will only use library member information to assist in provision of the service and to be aware of any issues that many exist in delivering that service. It is recognised that such information may also be used to market the service, but only within the authority to which the library member belongs and where explicit consent has been given.

Authorised personnel will be able to access the information, all of whom are aware of safeguarding issues and any release of data will be within the terms of the DPA 2018 and GDPR.

Authorised personnel will also have access to data to enable them to deliver the library service as contracted by the relevant library authority.

Information is retained for the period that an individual is a library member. Expired membership data is retained for 18 months to enable reactivation of expired user accounts.

If any member information was unlawfully disclosed, then the employing authority would be expected to institute disciplinary proceedings against the employee.

1.7. Data Security - technical

Security of the IT system to avoid exploitation and records copying

SirsiDynix Symphony is based on an n-tier Service Oriented Architecture, consisting of separate presentation, business logic and data access layers. The business layer contains all of the functional services (components) required for the LMS. Services are accessed using standard web service or API calls, across encrypted connections.

All sensitive data held in the Library Management System can only be accessed by authorised users, or in the case of public users, via unique number and PIN, or encrypted PIN/password, or via a single sign on option if a third party IdP is in use by the member library. Authenticated public users can only access their own sensitive data.

All user logins and passwords are created via the administration functions.

Permissions and access rights are allocated from within the application setup/configuration function.

Normal SirsiDynix Symphony users will not have access to the prompts required for administrative access.

Sensitive data from the public views is protected by a unique borrower number and PIN; system data is protected by secure logon and password. Data validation prevents data corruption.

SirsiDynix Symphony provides audit trails for cash management and ordering functions; further transaction audit facilities are available via borrower and item logs. An audit is maintained of user logins and unsuccessful attempts.

SirsiDynix develops its public access applications to W3C standards to ensure that maximum protection is provided to the backend services. Any information contained within comments does not present any details of how the system connects to the backend or the environment within which it operates.

In terms of protection from forceful browsing attacks, SirsiDynix Symphony staff interfaces are not publicly accessible and all web applications are deployed into the web server which has directory browsing disabled as default.

Symphony does not provide a WSDL, but it can be disabled at the constituent members request. SirsiDynix's code development includes data verification routines which ensure that if data is tampered with it is rejected.

SirsiDynix does not openly publish any schemas to prevent them from being compromised.

Although SirsiDynix does not use WSDAL, if information is needed to be transmitted between services, trusts are set up between the services.

The adoption of standard HTTP modules which implements canonicalization best practise into the web server enables the server to map the request to a file system path. The routines used must correctly parse the URL to avoid serving or processing unexpected content.

From a web application security perspective, SirsiDynix validate input and encode output, standard techniques include escaping 'dangerous' characters to protect general inputs and SQL injection.

Extensive use of parameterised SQL queries, i.e. prepared statements, is used throughout the applications to eliminate possible SQL injection.

Contextual output encoding/escaping as part of the above also helps prevent cross-site scripting together with tying any session cookies to an IP address.

1.8. Public notification

The library membership form used in all Libraries & Archives of the constituent members specifies that personal data is held on a common database and that it may be accessed by authorised personnel in any authority.

Notices are also displayed in Libraries & Archives, on the constituent member websites, membership forms, joining packs and other locations and means as deemed appropriate by each authority, reminding members of this.

1.9. Definition of terms

*Authorised Personnel

Authorised staff, volunteers and contracted partner organisations who deliver library services on behalf of a designated library authority. These may be commercial, voluntary or community organisations who have properly designated contracts, terms and conditions, Service Level Agreements and Information Sharing Agreements in place. All authorised personnel are responsible for ensuring that Kensington & Chelsea and Westminster Libraries & Archives data is managed appropriately.

GDPR and DPA 2018

General Data Protection Regulations and Data Protection Act 2018. The GDPR forms part of the data protection regime in the UK, together with the Data Protection Act 2018 (DPA 2018). The main provisions of these apply from 25 May 2018.