

Making the most of Koha features to protect citizens' privacy

Aude Charillon

PTFS Europe



That was a long title, but really, I want to cover:

- Laws and ethics (just a little bit)
- Koha features for...
 - Enhancing citizens' privacy
 - Data retention (or rather its opposite!)
 - Security options
- What else would be helpful?



A little bit on laws and ethics



The General Data Protection Regulation

*Principles relating to processing of **personal data** (article 5)*

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes
- limited to what is necessary
- accurate and kept up to date
- kept for no longer than is necessary for the purposes for which it was collected
- appropriate security



Professional ethical standards

“Freedom of access to information and freedom of expression [...] are essential concepts for the library and information profession.

Privacy is integral to ensuring these rights.”

[IFLA Statement on Privacy in the Library Environment](#) (2015)



“As an ethical Information Professional I make a commitment to uphold, promote and defend:

- [...] The confidentiality of information provided by clients or users and the right of all individuals to privacy”.

From: CILIP's Ethical Principles

<https://www.cilip.org.uk/page/ethics>



Enhancing citizens' privacy



Informing citizens

- Cookie consent ([Bug 27378](#), coming soon!)

Example: British Museum Library <https://library.britishmuseum.org>

Cookies on the British Museum Library Catalogue

We have placed some essential cookies on your device to make our site work. Select "Accept only essential cookies" to allow only these. Please note, we will use an essential cookie to save your choice.

We would like to set an additional cookie that provide personalisation and send anonymized information about how this site is used to our Google Analytics account. Select "Accept all cookies" to allow these.

For the Library's Cookie Policy, select *More Information*.

Accept all cookies

Accept only essential cookies

More information

Informing citizens

Cookie consent

CookieConsent set of system preferences.

- Allow an admin to define code that requires consent to run (e.g. code that results in a non-essential cookie being set), along with a name and description for that code.
- Allow a user to see exactly which cookies (essential and non-essential) may be set and which non-essential cookies they can consent to if they wish.
- Prevent the running of any code that causes a non-essential cookie to be set unless the user has explicitly consented to it.



Informing citizens

- Display or link to your Privacy policy on your OPAC

Example: Cheshire Libraries (footer link) <https://cheslive.koha-ptfs.co.uk>

Help

- If you have any queries or need any assistance with our digital services, please [contact us via e-mail](#).
- Please remember to quote your library card number if you have one, and please include details of the problem you're experiencing.

[Cheshire East Libraries privacy notice](#)

[Cheshire West and Chester Libraries privacy notice](#)

Informing citizens

Display or link to your Privacy policy on your OPAC

In the Tools module

- Pages section: create a Privacy policy page on your OPAC
 - Create new entry; display location: OPAC.
 - Add your content; save.
 - Copy the page URL.
 - The hyperlink will be like: `yoursite.name/cgi-bin/koha/opac-page.pl?page_id=23`
- HTML customizations section: add a link from your OPAC
 - Footer: add link to your existing opaccredits entry or create one
 - Homepage main navigation: use OpacNav entry



OPAC usage

System preferences

- *EnableOpacSearchHistory* - allows you not to store citizens' search history
- *TrackClicks* - you can choose not to track or to anonymously track links citizens click on in the OPAC.



Giving citizens choices

- Recording consent: use patron attributes
 - Create a patron attribute in Admin > Patron attribute types
 - Make it editable in the OPAC
 - Can run a report to check which library members have consented
- Individual messaging preferences
 - *EnhancedMessagingPreferencesOPAC* - allows library members to tick / untick which notices they want to receive



Giving citizens choices

- *OPACPrivacy* system preference
 - Allows library members to choose their own privacy settings for their borrowing history and holds history
 - Keeping borrowing history: Never / Default / Forever
 - Uses *AnonymousPatron*



Guarantees and guarantors

- Who needs a guarantor?
 - Review age limit of Child patron categories
- Choices for guarantees
 - *AllowPatronToSetCheckoutsVisibilityForGuarantor* and *AllowPatronToSetFinesVisibilityForGuarantor* system preferences let young library members decide what their guarantor(s) can see on their accounts.



Data retention (or rather its opposite!)



What personal data is it *necessary* to process?

Tips when reviewing what personal data you collect:

- Make patron form fields optional rather than mandatory
 - *BorrowerMandatoryField* system preference for the staff interface
 - *PatronSelfRegistrationBorrowerMandatoryField* for the OPAC self registration
 - *PatronSelfModificationMandatoryField* for the patron account in the OPAC



What personal data is it *necessary* to process?

Tips when reviewing what personal data you collect:

- Hide unused fields (so no data is entered)
 - *BorrowerUnwantedField* for the staff interface
 - *PatronSelfRegistrationBorrowerUnwantedField* for the OPAC self registration
 - *PatronSelfModificationBorrowerUnwantedField* for the patron account in the OPAC
- Delete existing data in unused fields
 - Using a report and the Batch patron modification tool



Anonymisation

Anonymise old circulation data

- Set up *AnonymousPatron*: this will be used to replace the borrower data.
- Set up the `batch_anonymise.pl` cronjob with your preferred period after which returned items will be anonymised.
 - = Default used in Patron category *Default privacy* and for *OPACPrivacy* options
- You can also manually anonymise library members' circulation history using Tools > Batch patron deletion/anonymization.
Tip: run a report first!



Pseudonymisation

- *Pseudonymization* system preference: enable for circulation transactions and selected borrower information to be collated in the database's pseudonymised tables.
 - These tables with limited personal data can be queried for statistical purposes.
 - No direct identifiers for the patron are recorded; the `pseudonymized_transactions` table uses an encrypted version of the `borrowernumber`.
- *PseudonymizationPatronFields*: choose user data to be retained with the transaction information
 - Patron category, home library, postcode, patron attributes...



Data retention? Data deletion!

Set up scripts on your server to delete automatically:

- Library members' expired accounts
- Deleted accounts
- From current accounts:
 - Older reservations information
 - Older issues
 - Older notices sent
 - Older transactions

Use [delete_patrons.pl](#) and [cleanup_database.pl](#)



Security options



Passwords

- Apply to all users
 - *FailedLoginAttempts* - block a user after a wrong password was entered a specified number of times
 - *NotifyPasswordChange* - notify a user whenever their password has been changed
- Apply default or amend in patron category settings:
 - *minPasswordLength* - set minimum password length
 - *RequireStrongPassword* - force password to include at least one number, one lower case and one upper case letters



Passwords

- In patron category settings or in individual user account:
 - Password expiration (days)

- Options for new password once the previous one has expired:
EnableExpiredPasswordReset


OPAC/Staff interface login

Username:

Password:

Minimum password length: 9

Confirm password:

Password expiration date: 

Additional security for staff logins

- Restrict staff access by IP range
 - Add IP ranges in Libraries settings.
 - Enable *AutoLocation* system preference.
- *TwoFactorAuthentication* - staff will have to generate a one-time password through an authenticator app every time they need to log into the staff interface.
 - Enable or enforce through the system preference.
 - Each staff member then need to enable it in their account.



Who should have access?

Staff permissions

- Patrons with either *superlibrarian* or *catalogue + borrowers* permissions can login and view personal data held in the system.
- Update [permissions](#) of team members leaving.
- Use a [report from the Koha SQL reports library](#) to identify which of your users currently have staff permissions. Update or delete users who do not need access anymore.



What else would be helpful?



Improvements to existing functions?

- Anonymisation
 - Ability to set different days by patron category
 - [Bug 34534](#)
- Pseudonymisation
 - How do we report on users who have used the library but not borrowed through Koha?



Dealing with Subject Access Requests

- Currently, to retrieve Koha data about a library member:
 - Use the Export option: find it above the table, e.g., on patron's Circulation history tab.
 - Create reports to query all the required tables.
- In the future?
 - [Bug 20028](#) - Export all patron related personal data in one package



**Is there anything else
you would recommend?**

**What is your experience of using
these features?**

What else would be helpful for you?

