



# Leading the Way

A guide to privacy  
for public library staff

## **Carnegie UK Trust**

The Carnegie UK Trust works to improve the lives of people throughout the UK and Ireland, by changing minds through influencing policy, and by changing lives through innovative practice and partnership work. The Carnegie UK Trust was established by Scots-American philanthropist Andrew Carnegie in 1913.

## **Newcastle Libraries**

Newcastle Libraries provide access to information, culture, heritage and learning opportunities for everyone in the City of Newcastle upon Tyne and beyond.

## **CILIP**

CILIP, the library and information association, is the leading voice for the information, knowledge management and library profession. Our goal is to put information and library skills and professional values at the heart of a democratic, equal and prosperous society. CILIP is a registered charity, no. 313014.

## **Acknowledgements**

This guide would not exist without the help, support and suggestions received from a number of people. Aude Charillon would especially like to thank:

Luke Burton (Digital Development Manager: Community Hubs, Libraries and Parks, Newcastle City Council), Trisha Ward (Assistant Director, Libraries NI), Martyn Wade (Chair, IFLA Committee for Freedom of Access to Information and Freedom of Expression), Ciara Eastell (Chief Executive, Libraries Unlimited), David Fay, Nik Williams (Project Manager, Scottish PEN), Alex Haydock, Ben White (Head of Intellectual Property, British Library), Simon Bowie (Senior Systems Developer [Open-Source Systems], SOAS, University of London), Kevin Sanders, Adam Walsh, Andrew Venus (Customer, Culture and Skills Assistant, Newcastle City Council) and Tony Durcan (Assistant Director, Transformation, Newcastle City Council).

## **Disclaimer**

The Carnegie UK Trust, CILIP, Newcastle Libraries and the authors are not responsible for any errors or omissions, or for the results obtained from the use of this information in this publication. All information is provided with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information. No responsibility can be accepted for any loss or other consequences of following the advice in the guide.



The text of this guide has been dedicated to the public domain; the Carnegie UK Trust, CILIP and Newcastle Libraries have waived any copyright over it. You can copy, modify and distribute the text, including for commercial purposes, without asking permission.

# Contents

<b>Foreword</b>	<b>2</b>
<b>Introduction from Aude Charillon: Privacy and the role of library staff</b>	<b>3</b>
<b>How to use this guide</b>	<b>6</b>
<b>Chapter 1: Managing Data in the Library – Key Concepts and Principles</b>	<b>7</b>
<b>Chapter 2: Inside the Library – Library Systems</b>	<b>13</b>
<b>Chapter 3: Inside the Library – The Internet</b>	<b>19</b>
<b>Chapter 4: Inside the Library – Physical Space</b>	<b>23</b>
<b>Chapter 5: Working with others – Colleagues</b>	<b>24</b>
<b>Chapter 6: Working with others – Suppliers</b>	<b>28</b>
<b>Resources</b>	<b>33</b>
<b>Glossary and Technical Terms</b>	<b>34</b>

# Foreword

Library staff and public libraries have historically played a critical role in promoting and enabling access to a very wide range of published materials, supporting educational advantage, acquisition of knowledge, open access to information and democratic participation.

As safe spaces in communities that enable access to information, knowledge and culture, public libraries have a clear role to play when it comes to data privacy. It is important that public library users feel confident and well informed about how their data is being collated, stored or shared by the library service and its contractors, or by the online services offered in library buildings.

Public libraries also have a responsibility to enable library users to make informed decisions in relation to their privacy. CILIP's new Ethical Principles commit their members to uphold, promote and defend the confidentiality of information provided by clients or users and the right of all individuals to privacy. These responsibilities go beyond fulfilling any legal requirements regarding privacy – they stem from the values and purpose that position public libraries as the trusted and safe hearts of their communities.

This guide is designed to help library staff to consider the data their library service collates, holds and shares and how privacy friendly their systems and resources should be. It also outlines steps that can be taken by those seeking to enhance the approach to privacy across different aspects of their service.

Whilst this guide is not primarily aimed at training staff in how to engage library users on data privacy, engaging library users on data privacy is an important role for staff and we hope that working through the issues outlined in the guide will enable library staff to feel better equipped to have these conversations with the public.

We hope you find the information in this guide helpful in both sparking discussions about becoming more privacy conscious and developing and enhancing an approach that facilitates and protects library users' privacy.



**Martyn Evans**  
Chief Executive, Carnegie UK Trust

# Introduction from Aude Charillon: Privacy and the role of library staff

## Library staff defend human rights

I personally believe that libraries exist to defend people's rights to enrich and improve their own lives, their environment and society. We library and information professionals make this happen by facilitating access to and by sharing information, knowledge and culture.


We stand for freedom of information and freedom of expression; and, as highlighted in the International Federation of Library Associations and Institutions (IFLA) [Statement on privacy in the library environment](#), 'privacy is integral to ensuring these rights'.

Without privacy citizens may feel uncomfortable searching for the information they need; if they feel observed they may refrain from exercising their right to access information for fear of the potential consequences. In a similar way, citizens may be careful of revealing opinions; if they are afraid of their words being brought to public attention they may choose not to express themselves.

In public libraries there may be a risk that citizens refrain from using their freedom of access to information and freedom of expression when they search for and borrow books, when they use public computers to look up information on the internet or to use online platforms to interact with others.<sup>1</sup>

Each of us has layers of values, sometimes from different sources. As individuals we have our own personal ethical principles; as employees we would also take into account the values of our employer. CILIP, the Library and Information Association, has an ethical framework that its members sign up to. The 2004 CILIP Ethical Principles started with the statement that:

*Library and information professionals are frequently the essential link between users and the information they require. They therefore occupy a position that carries responsibilities.*



Privacy is defined by [Oxford Dictionaries](#) as 'a state in which one is not observed or disturbed by other people'. 'Other people' can refer to individuals but also to organisations such as government agencies or businesses. Another Oxford Dictionaries definition is 'the state of being free from public attention'.

Privacy is a fundamental human right enshrined in article 12 of the [Universal Declaration of Human Rights](#) adopted by the United Nations in 1948:

*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

<sup>1</sup> IFLA (2015) <https://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf> [Accessed October 2018]

The [current Ethical Principles](#), adopted in 2018, make our stance even clearer:

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

- *Human rights, equalities and diversity, and the equitable treatment of users and colleagues [...]*
- *Intellectual freedom, including freedom from censorship [...]*
- *The confidentiality of information provided by clients or users and the right of all individuals to privacy.*

It is clear that we public library staff have a responsibility to enable citizens to access information while ensuring their privacy is protected in the process. However, balancing access to information and privacy of individuals is sometimes tricky; examples being the discussions around the 'right to be forgotten' or the compliance with surveillance and counter-terrorism legislation.

### **Privacy is about making an informed choice.**

Many citizens (library staff included!) do not think their online privacy is very important, often because they do not fully understand how their personal information is collected and used.

In 2016 the Carnegie UK Trust commissioned Ipsos MORI to conduct the [Digitally Savvy Citizens](#) survey, which asked people in the UK and Ireland about their behaviour regarding online information searching, privacy and security. About 48% of respondents in the UK said they do not turn off the location services on their phones. For me the question is: do those citizens know how their location is used but have decided leaving the location services on is more convenient, or are they unaware of the privacy issues?

**Privacy should be about choice:** people need to be aware of the risks to their personal data and of the tools that may help them protect it better, so they can make an informed choice about whether to take steps to actively protect their privacy.

This is where library staff have a practical role to play. We already enable citizens to learn new skills by offering access to a learning environment or learning materials, by supporting external courses in our buildings or by delivering sessions ourselves. We should be providing resources or events for citizens to learn about online privacy issues; these could be incorporated into existing materials and digital skills sessions or into new activities created from scratch. By doing this we are fulfilling our role to provide access to information and to enable citizens to make informed decisions – regarding how their personal data is used by online services. But we also need to ensure we practice what we preach and take steps to ensure our internal processes and systems are privacy friendly.

## Taking a stand

Citizens should be able to make informed decisions when it comes to using library services. They are entitled to know what personal data is collected about them, when and for what purpose, how it is processed and stored.

Compliance with the GDPR includes the principles of transparency and of limiting the handling of personal data to what is necessary to deliver the service. As library and information professionals we should not simply comply: we should be leading the way and showing best practice of what, for example, 'being transparent' means.

I believe we should go further than respecting the privacy of citizens using library services: we should be taking a stand for it. If we do not take action we are allowing businesses, intelligence agencies and mal-intentioned individuals to potentially invade the privacy of citizens. We cannot be neutral; in order for libraries to remain safe spaces and for library staff to remain trusted professionals we must adopt a proactive attitude to protecting citizens' privacy in libraries.

I hope this guide and accompanying resources will provide you with useful information and ideas in order for you to take a stand for privacy in your library.

### Aude Charillon

Library and Information Officer, Newcastle Libraries



# How to use this guide

## Who this guide is for

This guide has been designed to support public library staff in the UK – at any level of their organisation – to promote and protect the privacy of library users. **If you are interested in what you read, please share this guide with your colleagues.** Parts of the guide may also be useful for library and information professionals in other sectors or countries, and other colleagues and members of the public interested in libraries and privacy.

## What this guide does

This guide is designed to **help library staff to consider the kind of data they collate, hold and share about those who engage with their services; and how 'privacy-friendly' their systems and resources are.** It also offers a range of practical ideas that library staff can take to make their service more privacy focused, to go beyond legal compliance and lead the way in delivering services that protect users' data privacy. We recognise that library services operate in different ways across the UK, and we have aimed to include options in this resource that can be adapted to suit local situations.

## What this guide doesn't do

This guide is not a manual on how to engage the public about data privacy. For those seeking this type of guide, there are existing resources that may be of interest.<sup>2</sup>

<sup>2</sup> Scottish PEN, in collaboration with Scottish and American library organisations, has published a detailed online data privacy and security [toolkit](#) which explains key issues for library staff and library users. It also recommends practical steps that can be taken to improve the privacy of library users.

## What this guide covers

This guide is organised around the following topics:

- Managing Data.
  - Key concepts and principles.
- Inside the Library.
  - Library systems.
  - The internet.
  - Physical space.
- Working with others.
  - Colleagues.
  - Suppliers.

## How to use this guide

The chapters in this resource can be read individually or consecutively. Each chapter covers:

- ✓ Why the topic is important.
- ✓ What this means for libraries
  - some practical considerations.
- ✓ Taking action (questions to help identify areas where you are already working on privacy, and areas for further action).
- ✓ Further information (hyperlinks to further online resources and information).

A number of chapters provide case studies from Newcastle Libraries to help illustrate a point or a practical action that can be taken.

A list of the main [resources](#) and a [glossary](#) of key terms can be found after the last chapter.

Hyperlinks are used in this guide; links to external sources are [blue](#) and links within this document are [purple](#).



# Chapter 1:

## Managing Data in the Library

### Key Concepts and Principles

#### Why it's important

Data privacy is a pressing public policy issue. There have been allegations that data analytics firm Cambridge Analytica harvested and used personal data from Facebook to influence the outcomes of the Brexit referendum and 2016 US Presidential election. This has brought to the forefront of our attention that personal data matters and that how it is collated, stored and shared merits serious consideration.<sup>3</sup>

Data is a core part of how public libraries operate. Public libraries handle a huge amount of personal data about those that use their services. This can range from data that can help to identify a library user, such as their name, address, contact details and date of birth, to data about library usage such as borrowing and reservation history, and data about lapsed or former library users. What then, should public libraries be mindful of in relation to the personal data it handles?

This chapter sets out key issues to be considered in all areas where data is being collated, retained and shared.

#### What this means for libraries – some practical considerations

As those committed to promoting access to information and knowledge in a safe and trusted environment, it is important that public

library staff protect users' data and their privacy.

There is also a legal imperative as libraries are required to comply with data protection rules and regulations.

#### GDPR: data collation and data retention

The main data protection legislation covering the UK comes from the EU in the form of the General Data Protection Regulation (GDPR).<sup>4</sup> GDPR applies to organisations and businesses that collect, handle and store the personal data of European Union residents whether in digital or paper form, when the data is systematically filed and arranged according to a specific criteria in a way that allows for their easy retrieval.

Public libraries, independent organisations running public libraries and a range of third party suppliers, from library systems suppliers to those that provide event registration websites, all come under the remit of GDPR as they are organisations that process the personal data of library users.

It is the responsibility of the library service and its parent organisation (such as the local authority) to ensure that any third-party supplier handling library users' personal information provides guarantees that they comply with a) GDPR and b) the local authority's or library organisation's own data processes. There are more details on this in [chapter five](#).

<sup>3</sup> BBC News (2018) Cambridge Analytica: The story so far BBC News (online) <https://www.bbc.co.uk/news/technology-43465968> [Accessed August 2018]

<sup>4</sup> The [Data Protection Act 2018](#), which complements GDPR, also applies in the UK.

Under GDPR, **'personal data'** is any information that can help identify a living person, including:

- name;
- library card number;
- date of birth;
- contact details; and
- computer and mobile devices'  
**IP addresses.**

**'Sensitive personal data'** includes:

- ethnic origin;
- religious beliefs;
- biometric data;
- health data; and
- sexual orientation.

Rules (and penalties) are even stricter regarding the protection of sensitive personal data.

As a reminder, GDPR sets out six **principles relating to the processing of personal data**:

1. Personal data must be processed **'lawfully, fairly** and in a **transparent** manner'.
2. The collection of personal data must only take place for 'specified, **explicit** and **legitimate** purposes'; no further use outside those specified purposes is allowed without legal grounds for that processing.
3. The data held by organisations must be **'adequate**, relevant and **limited to what is necessary**' for the purposes for which it is being processed.
4. Personal data held must be **'accurate** and, where necessary, kept up to date'.
5. Data that permits identification of individuals must be **retained 'for no longer than is necessary'** for the purposes for which it is being processed.
6. Personal information must be handled 'in a manner that ensures **appropriate security**' of the data.

GDPR also sets out six situations in which processing of personal data is considered 'lawful'. The situations most likely to be relevant in public libraries are:

1. The provision of a service under official authority, which covers public functions and powers set out in the law.
2. When performing a specific task in the public interest set out in law (known as 'public task'). For example, when providing a library service as laid down in the Public Libraries and Museums Act 1964.
3. When citizens have given their consent for their data to be used in this way.<sup>5</sup>
4. When handling personal data is necessary to fulfil a contract citizens are party to. For example, for the provision of e-books to library users.

Information and resources regarding GDPR and other data protection matters are available **from the ICO website**.<sup>6</sup>

5 Note that consent must involve a **positive action**. Positive action can include ticking a box to agree to a specified use or answering a yes/no question. For young people under the age of 13 years old, consent to the processing of personal data must be given by their parent or guardian.

6 The Information Commissioner's Office (ICO) is responsible for monitoring the application of GDPR in the UK.



### What does GDPR mean for libraries?

- ✓ Public libraries staff and their third-party suppliers can only collect and use personal information in a way that complies with GDPR.
- ✓ There has to be a legitimate reason for the collection of personal data.
- ✓ Library staff and suppliers must not collect and process personal information that is not necessary for delivering the offered service.
- ✓ Efforts must be made to keep data up-to-date, and to either correct or delete inaccurate information.
- ✓ Personal data must only be kept for the time that it is necessary to deliver the service.
- ✓ Library staff and suppliers must take steps to ensure the security of the personal data they hold and manage, and protect it against unauthorised access and accidental disclosure.
- ✓ Library users must be made aware in an easy-to-understand way what data is being collected about them and how it is being processed.

## Other relevant legislation

There is legislation in place that means the library service may be required to retain or disclose personal data of library users.

Under the [Investigatory Powers Act](#),<sup>7</sup> a public library, an entire public library service, or the parent organisation or internet supplier of a library service, is obliged to keep internet connection records if the Secretary of State issues a notice under the Act that that specifically requests the retention of such records.<sup>8</sup>

7 The [Investigatory Powers Act 2016](#) establishes the circumstances in which police and intelligence agencies can legally obtain information from a “telecommunications operator”. For example information about citizens’ internet use from an internet service provider. Under the definition of the Act, a local authority, a library or a third-party contracted to provide internet services in libraries is a telecommunications operator, so this law therefore applies to them. The Act is deliberately broad when defining ‘internet connection records,’ as it states this is “data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication”.

8 Once a notice has been issued, the Act makes it illegal for people implementing the notice to reveal its existence or its content to others. This means that library staff would not necessarily know if a retention notice is in place in their organisation. It would therefore not be possible to know if a retention order is the reason why it is not possible, for example, to reduce the time period library users’ internet browsing history on public computers are retained.

The UK Government’s [Prevent Strategy](#)<sup>9</sup> and the [Counter-Terrorism and Security Act 2015](#) place a duty on local authorities in Scotland, England and Wales, to develop plans to safeguard individuals from getting involved in terrorism. Whilst the Prevent Strategy does not require local authorities to retain information about library users’ activities, it may be used as a reason to ask public libraries to retain all library users’ borrowing history or internet browsing history.

It is worth noting that the [police are able to request data from public libraries about library users](#). In these circumstances, before any identifiable personal data is shared, library staff should take formal legal advice from the Council or library organisation’s legal department. This department will be able to advise on what library staff may be legally required to share.

9 The aim of the Prevent Strategy is to “reduce the threat to the UK from terrorism by stopping people becoming terrorists or supporting terrorism”. The [Prevent Duty Guidance \(2015\)](#) provides details of best practice to implement the UK Government’s Prevent Strategy.

## Privacy notices

A privacy notice brings together the information library users are entitled to have regarding how and why their personal data is being processed when they use library buildings and services, in a clear and transparent way.

Best practice includes concise pieces of information given to library users at the point their data is collected. Information could be communicated orally, with signs, or (for example) next to the relevant line of an online form. It should signpost library users to a source of more detailed information.

The UK Information Commissioner's Office (ICO) website offers guidance on privacy notices, via its [Right to be informed](#) page.

Here is an extract from [Newcastle Libraries' privacy notice](#):

### **Borrowing items from Newcastle Libraries**

When you borrow items from us we record the time, date, library and details of the item. We do the same when the item is returned. This is necessary for us to manage our collections and the lending process.

We keep this information – called your circulation history – for 12 months. After 12 months it is anonymised: we keep the information about the item having been borrowed but we do not know by whom.

We keep the circulation history for 12 months before anonymising it to allow library members who use our home delivery service to benefit from an efficient service. We choose items for housebound members before dispatch; we need to know what items those users have had recently to make sure they do not receive the same items all the time. We do not have the technical capacity to apply different anonymisation rules for different categories of members; therefore all library members' circulation history is kept for 12 months.

We keep records of holds you have placed and fees you may owe us. We collect this information because again it is necessary for us to manage our collections and the lending process.

We do not have the technical capacity to delete this type of information after a chosen amount of time so it is currently kept until your membership is deleted (see [Joining Newcastle Libraries](#) section).



## Taking Action

Below are some key questions to ask yourself and your colleagues about the library service. These questions apply to any system or service you offer that collates library users' data. They are therefore applicable to the subsequent chapters in this guide.

### Data collation

- Do we understand what personal data is collected, when it is collected, from whom, for what purpose, how it is used, how long it is stored and what happens when it is not needed anymore? If not, could we do an audit?
- Are we clear why personal data is handled and whether that data is necessary to provide the service?
- Are library users giving their consent for the processing of their personal information by taking a positive action?
- Are we documenting the findings of information audits and recording all other steps taken to comply with GDPR (reviewing policies, staff training)?
- Are our privacy statements or notices which explain to library users why their data is collected and what their rights are fit for purpose?
- Have we made library users aware in an easy-to-understand way what data is being collected about them and how it is being processed?

### Storing Data

When reviewing your data retention policies, it could be helpful to ask:

- When or by what system is potentially personally-identifiable information collected?
- How long is that data stored?
- Why is it kept for that duration?
- What is it used for?
- For what period of time is it used?
- How long is the collated data realistically needed to deliver the service?
- Is there a way to securely anonymise the data?
- Are we giving library users a choice regarding the duration their data is kept?

## Ongoing Practices

You may find that some of the points in the 'Taking Action' section will need to be revisited or reviewed on an ongoing basis.

- Do you have a proactive policy in regard to monitoring how data privacy friendly your library service is?

There are many potential areas where data may be collated and stored for a specific length of time, which could be reviewed. These include:

- ✓ computer usage logs (from a computer booking system);
- ✓ printing history (from a printing solution);
- ✓ internet browsing history and cookie settings on public computers;
- ✓ information from online forms and website logins saved on public computers;
- ✓ files used or saved by library users on public computers;
- ✓ Wi-Fi usage logs;
- ✓ library users' borrowing history (from a library management system);
- ✓ library users' reservation history (from a library management system);
- ✓ former library users' details (from a library management system);
- ✓ library users' payments history (from a library management system and other payment systems);
- ✓ online catalogue/online library account usage logs;
- ✓ website analytics;
- ✓ attendees lists and personal registration details for events;
- ✓ CCTV logs; and
- ✓ back-up databases and server logs (internal to the library organisation and on suppliers' own servers).

## Further information

- Information and resources regarding GDPR and other data protection matters are available from the [ICO website](#).
- [Briefing: Impact of the General Data Protection Regulation 2018](#) prepared for IFLA by Benjamin White.
- A practical guide to data protection for information professionals by Naomi Korn and Carol Tullo; [available via CILIP](#).

# Chapter 2:

## Inside the Library

### Library Systems



#### Why it's important

Systems hold a lot of data about people. A breach in the security of systems can therefore mean that personal data is compromised. In 2016, a data breach led to the personal data of 57 million Uber drivers and customers being exposed.<sup>10</sup> Data breaches like this can involve the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.



#### What this means for libraries – some practical considerations

Libraries deliver services using a wide variety of software and electronic platforms. From library management systems to computer booking systems, from e-book platforms to other subscription-based external databases. **Weak data protection practices in relation to such software and platforms can make them vulnerable to data breaches.** Ensuring data collated within electronic systems and platforms is secure guarantees the protection of library users' personal information by making sure no unauthorised person can access it. There are more and more software and platforms with privacy-conscious features.

The following points will help enhance privacy and security in your services.



#### Updates

Library systems and the software and operating systems they rely on can have vulnerabilities or weaknesses. These vulnerabilities become a security concern if hackers uncover the weakness and create a code that targets it and (for example) access the system and extract personal data from the software or system.

When software vulnerabilities are discovered, developers issue a **patch** to update the system and close any gaps in the security. **The most basic but essential thing that can be done to keep systems secure is therefore to ensure they are maintained and kept up-to-date.** Patches need to be installed in a timely manner to protect systems from known flaws.<sup>11</sup>



#### Creating passwords

Logging into library systems usually requires passwords. Passwords ensure that data is kept confidential and secure. Several electronic systems in the library will require users – library users or staff – to choose a password to access their account or the whole platform.

**Having strong passwords is critical for data security.** The longer and more random a password, the more difficult it will be to break. It is therefore recommended that people use a **passphrase** rather than a **password**. A passphrase is a sequence of text or words and is therefore longer than a password.

10 BBC News (2017) Uber concealed huge data breach BBC News (online) <https://www.bbc.co.uk/news/technology-42075306> [Accessed August 2018]

11 In May 2017, NHS hospitals and GP surgeries in England and Scotland were hit by a 'ransomware' attack which took advantage of a vulnerability in Microsoft. Although a patch had been issued to fix this vulnerability in March, it had not been installed – leaving the vulnerability open. <https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/> [Accessed October 2018]

Following from this, it is worth considering changing a system's settings to enforce a lower limit for the number of characters in a password, and to allow the use of numbers and special characters. Again, it is good practice to remove upper limits for the number of characters in a password so library users and staff can use more secure passphrases. It is also important not to use the same password for multiple systems or accounts, especially passwords used for personal accounts.

### **\*\*\*\_ Storing passwords**

Several library systems will store passwords, for example those used by library staff to access the system's staff interface or those used by library members to view their account online. It is important to reflect on how securely these are stored.

It is best practice for passwords to be accessible only to their owner. Library staff should not be able to view library members' passwords or PINs stored within the library systems, as they should be hidden by asterisks.

Finally, passwords stored within a system should be encrypted using up-to-date methods, and library staff should check that suppliers are using these. The American Library Association's *Library privacy guidelines for library management systems* has more information in regard to encryption.



### **Operational database and log files**

When reviewing data privacy in the library it is important to consider operational databases and log files. Library users' details are stored on both the 'live' database, which library staff amend and update when library users' details change, and the backup database. Furthermore, the log files that are generated when a change is made to the live database can also contain personal data and information about when and how this was altered.

It is therefore important to encrypt data on live and backup databases, and to encrypt the log files. Again, records pertaining to library users should be anonymised by dissociating records of transactions from an individual user. For example, it should be possible to retain the information that a particular item has been borrowed within the last 8 months, but not that it was borrowed by library member X. Library staff should ask suppliers to enable encryption of the operational database and log files. Further information about working with suppliers is covered in [chapter 6](#).



### **Radio-Frequency Identification (RFID) technology**

RFID technology allows library users to borrow and return items using self-service kiosks. Information about the item is stored in an electronic circuit ('the RFID tag') attached to the item. This RFID tag is read by kiosks or other devices linking to the library management system.

However, more and more common devices – such as smartphones – are equipped with technology that can read RFID tags. This causes concerns over what information is stored on tags, who may be able to read it and how this may impact individuals' privacy.

Recommendations from the Book Industry Communication on the use of RFID technology include ensuring that no library borrower details are stored on RFID tags, and informing citizens about RFID tags on items by using signage in the library building. Further information can be found at the end of this chapter.





## Library websites

This section considers privacy in relation to the library website, and the [next chapter](#) considers browsing the internet more generally.



## HTTPS

When a library user wants to access a page on a library website, for example when searching their library's online catalogue or when logging into their online account, the browser they are using makes a request to the library website via several servers. It is relatively straightforward for third parties to intercept this request on its journey between the browser and the library website.

If the connection to the library catalogue is not secure (that is, if the data that travels along the connection is not encrypted), the information contained in the request can be read. This information includes anything the library user has typed on the website: their library login, their password, the content of their search and so forth, compromising the privacy and security of the library user.

To protect library users' personal information it is essential that data travelling to and from a library website is encrypted. **HTTPS** is an internet protocol that encrypts data travelling from a browser to a website and vice versa. As such, HTTPS prevents information being read by encrypting the data travelling to the website. As the content of the request is encrypted it will be unreadable even if the content is intercepted.

If library web pages are hosted by the library authority, it is crucial to discuss obtaining a security certificate with the IT department. HTTPS means that the connection is encrypted, and the security certificate proves that the encryption is working correctly. If library web pages are hosted by a systems supplier, it is important to ask them about enabling HTTPS for all the library webpages.



## Cookies

Public library web pages are likely to use internet **cookies**.

**Cookies** are small files that function in the background of a website. Some are essential for a webpage to display properly, others are designed to remember information about the person browsing the internet to improve their future experience (eg a user's preferences and past behaviours), and others still are an add-on to a website to offer a specific service.

In terms of 'remembering' information about the person browsing the internet, cookies can 'remember' who we are, meaning that there is no need to memorise multiple passwords or constantly re-type personal data.

Cookies can also allow recent search history and preferences to be retrieved for quicker and easier web browsing, and websites are customised based on past preferences. For example, a library's online catalogue may have accessibility options for the text to be displayed on a different coloured background. If a user chooses this option then a cookie may be placed by the library website on their internet browser, so that the next time they visit the online catalogue it will have remembered their preferred accessibility option and immediately display the text on a different coloured background.

However, if a library website allows 'third party cookies', this can impact on privacy as these cookies enable another commercial entity to 'scoop up' our preferences and user behaviour, which could then be used for commercial gain. In this way, commercial third parties that we have no knowledge of can gain access to personal preferences and characteristics.

For example, widgets and **plugins** are third party cookies that can be used to enhance the way in which content can be arranged on a library website, or improve site functionality. They may collect information about the person browsing a website, even if the user doesn't click on a function that the widget or plugin has made available. For example, a plugin such as a 'share to this social network' button sends information back to the social network about the internet user site even if the user has not clicked the button.

It is a **legal requirement** for websites to inform citizens of the use of cookies, to explain what they do and to obtain citizens' consent for their use.

It is therefore good to **clarify whether the cookies on a library website are necessary and to be transparent about the cookies the library webpage utilises**. It is best practice to:

- ✓ review which cookies the library web pages use, and whether they are all necessary;
- ✓ limit the use of cookies that track user behaviour;
- ✓ be transparent about what cookies are used for; and
- ✓ explain to library users how to disable or erase them.



## Web analytics

Many library websites use analytics to collect data that measures and analyses how visitors use and access the site. This can help services better understand what people are looking for and using. In turn, this can help optimise the website. However, **library website analytics may collect data that can help identify an individual**. It is important to ask whether: the data gathered is required to offer the service; there is a way members of staff can access this data; and whether the practice of collating data is clear to library users.

If library website analytics collect information that could potentially identify an individual, it is essential to comply with data protection legislation and **ensure that the use of analytics is explained to library users in a clear and transparent way**.

It may also be worth considering using a web analytics platform which: allows control over what data is collected, can anonymise data and generally offer guarantees that library users will be given the choice of allowing their information to be used when they visit your website. For example, **Matomo** (formerly known as Piwik) is a more privacy-conscious alternative to **Google Analytics**.



## Taking Action

Below are some key questions to ask yourself and your colleagues about the library service. Please note that these questions are limited to actions library staff can take in relation to library systems. A list of questions to ask of suppliers who design and provide systems can be found in [chapter six](#).

### General

- 1) Are we using the latest updated version of all our systems?
- 2) Are we encouraging staff and library users to choose strong passwords?
- 3) Can library users set their own passwords without having to reveal them to library staff?
- 4) Are our systems allowing the use of passphrases by not having a higher limit for the number of characters in passwords and by not requiring numbers, capital letters or special characters?
- 5) Do our current systems use up-to-date encryption methods to store records, passwords and transactions?
- 6) Are the system's transaction records that contain personal information anonymised after an amount of time?
- 7) Are we limiting the members of staff who can access library users' data so that only those who need to use it are able to access it?

### Library website and catalogues

- 1) Are our library webpages and online catalogue provided using a secure (HTTPS) connection?
- 2) Have we reviewed cookies on our website in order to limit those that collect personal data?
- 3) Are we clearly explaining on our website what cookies are used, what they are used for, and how to disable or erase them?
- 4) If we use website analytics, have we enabled settings or chosen an analytics platform that guarantees information collected about library website visitors is not sent to other parties?

## Further information

### Passwords

- See the Electronic Frontier Foundation's Surveillance [Self-Defence guide](#) section on passwords.

### RFID

- You can [register](#) to receive a free copy of the full BIC RFID privacy in libraries toolkit via email. This guidance covers what library staff and suppliers need to know about the use of RFID in the library and being transparent with library users.
- The Electronic Frontier Foundation have also produced guidance on [how to deploy HTTPS correctly](#).

# Chapter 3:

## Inside the Library

### The Internet

#### Why it's important

When we browse the internet, we generate a mass of information about ourselves that we may not realise that we are generating. Personal characteristics and preferences – like gender, age, sexual orientation and income – can be gleaned from what we look at online. This data may be collected by platforms and software providers for commercial advantage or interest.

For example, consider how Amazon generates recommended products for us to buy based on our previous purchases; or how we may see targeted adverts indicative of our sexual orientation based on our browsing activities. This can be problematic if we don't want to disclose this information to others – especially if using a shared computer in a public space where other people may be able to see this targeted advertising.

#### What this means for libraries – some practical considerations

Public libraries play a critical role in providing people both with access to the internet and the skills to use the internet effectively.

Many internet users are not aware that personal data may be collected by platforms and software providers for commercial advantage. Research by Doteveryone has shown that 45% of people are unaware that information they enter on websites and social media can help target adverts to you.<sup>12</sup> It is critical that we

inform library users about these practices and enable them to make informed decisions about managing their personal data whilst online. It follows that building data privacy into the core digital training offer in libraries is an essential part of libraries' digital offer, and will enable library staff to play a practical role in enabling users to make informed decisions about their data privacy.

Scottish PEN, in collaboration with Scottish and American library organisations, has published a detailed [toolkit](#) which outlines features and tools that could better protect the personal data of those using the internet on their premises, and lists recommended practical steps. Here we present a smaller selection of basic privacy practices, features and tools.

As described in the [previous chapter](#), issues such as HTTPS, cookies and passwords are relevant and must be considered. In addition to this, there are a number of pieces of software and tools that you can utilise or install on computers to enhance the privacy of library users when they browse the internet.

#### **Tool 1: Resetting computer profiles**

To ensure that users cannot see or access the saved files or browsing history of previous users, [computer profiles should be reset to their original configuration after each user logs off](#). This can be done through software such as Deep Freeze.

<sup>12</sup> Doteveryone (2018) People, Power and Technology: The 2018 Digital Understanding Report; online. <http://understanding.doteveryone.org.uk/> [Accessed October 2018]

## Tool 2: Search engines

One of the key reasons library users utilise the internet is to search for information. There are search engines which are designed to keep and use as little personal data about library users as possible. Typically, this means that the search engine will not collect information about the user, or store and sell a user's search history to advertisers – unlike more mainstream search engines such as Google or Bing.

It is possible to set the default search engine of a library's public computer browsers to a more privacy-conscious engine such as:

- **DuckDuckGo** – an American search engine which promises to keep users' search history private and to protect library users from tracking;
- **Qwant** – a French search engine available in English, which is committed to not collecting data about users;
- **SearX** – a free software engine which aggregates other search engines and can be hosted locally.

An alternative could be to let computer users know about these search engines so that they can use a different engine if they so wish.

## Tool 3: Private browsing modes

To enable library users to prevent creating a history of what they have been browsing online for the next computer user to see, consider informing library users about 'private' browsing mode or else making these the default browsing mode. These 'private' browsing modes are a more privacy-focused alternative built into mainstream browsers: Chrome's is called **Incognito**, Microsoft Edge's is called **InPrivate** and **Firefox** and **Safari**'s are both simply called 'Private browsing'. Private sessions can usually be opened from the browser menu.

Whilst the 'private' features may differ from browser to browser, generally they prevent the browser from keeping and using information in relation to:

- websites and webpages visited;
- information entered in forms, including logins and passwords;
- information entered in search boxes;
- list of documents downloaded;<sup>13</sup> and
- cookies, for example, site preferences such as language.<sup>14</sup>

Whilst private browsing modes mean that the browser will not retain the data listed above, some of it may be collected by the websites visited or by the Internet Service Provider.

The main browser on public computers at Newcastle



Libraries is Chrome. Chrome was set up to open in Incognito mode, which guarantees that a computer user will not be able to see which websites the previous user has visited or what they looked for via the browser's search engine box.

## Tool 4: Browser 'add-ons' and 'extensions'

Another option for improving privacy where the default browser is Chrome or Firefox is the installation of privacy-enhancing 'add-ons' or 'browser extensions'. Two helpful add-ons are **HTTPS Everywhere** and **Privacy Badger**.<sup>15</sup>

### HTTPS Everywhere

When a library user wants to access a webpage, the browser they are using makes a request to the webpage via several servers. HTTPS uses encryption to protect requests sent to a website, so that even if it is intercepted it is not possible to read the information contained in the request. It also encrypts data generated by a user as they interact with the webpage. **HTTPS Everywhere** directs you to a secure HTTPS version of the webpage if one is available.

<sup>13</sup> It is worth noting that these documents may be saved in the computer's download folder.

<sup>14</sup> If a library service resets user profiles between computer sessions, some of this information may be deleted.

<sup>15</sup> **HTTPS Everywhere** and **Privacy Badger** were created and are maintained by the Electronic Frontier Foundation, a US-based non-profit organisation 'defending civil liberties in the digital world'.

## Privacy Badger

Third parties can track internet users as they use the internet and collect information about the user. Privacy Badger blocks third-party content, such as adverts, that it notices tracking and collecting information. On a webpage where there should have been adverts that collect information about you there will be a blank space – adverts that are not tracking the user will remain. In cases where a webpage is not displaying properly because Privacy Badger is blocking too many things, the settings can be adjusted. In this way, Privacy Badger blocks spying ads and invisible trackers, giving control back to the user over what third-party content they allow to track and collect information about them.

## Tool 5: Browser settings

Amending browser settings can also be an effective way of protecting the online privacy of library users. ‘Do Not Track’ is a browser setting that requests websites to stop tracking an individual user as they browse the internet. When ‘Do Not Track’ is enabled, the browser sends a request to the websites an individual visits to disable tracking. However, ‘Do Not Track’ requests can be ignored by websites.

## Tool 6: Privacy conscious browser

Providing a privacy conscious browser – such as Tor Browser<sup>16</sup> – is a more radical option when it comes to protecting the privacy of library users. Tor Browser anonymises internet browsing by routing the library users’ connection via Tor relays. That means that any website accessed does not see the IP address or location of the library users’ device or location. Instead the website accessed sees the IP address and location of the Tor exit relay. Furthermore, neither the Internet service provider nor the

organisation providing library users with the internet connection will know what sites a library user visits. Tor Browser also uses privacy tools such as DuckDuckGo and HTTPS Everywhere.

It is worth noting that due to privacy settings being maximised on Tor Browser, any website using potentially insecure plugins such as Adobe Flash will not display properly.

Critically, the strong privacy settings mean that ICT colleagues may be reluctant to install it on library computers as it makes it impossible to determine what library users are browsing on the internet in library buildings.

## Tool 7: Mixed methods

It is possible to offer a choice to those who use your public computers. For example, it would be possible to keep your current default browser and its familiar settings, and in parallel provide a different browser with privacy-enhancing features.

A sample offer using mixed methods could be:

- An original default browser such as Microsoft Internet Explorer with Google as its default search engine.
- An alternative browser such as Mozilla Firefox, with:
  - ✓ DuckDuckGo as the default search engine;
  - ✓ the privacy settings set to reflect the features of a private browsing mode: with the browsing history option set to ‘Never remember history’;
  - ✓ ‘Do Not Track’ enabled;
  - ✓ Privacy Badger add-on;
  - ✓ HTTPS Everywhere add-on; and
  - ✓ a homepage with a description of the privacy friendly settings and tools in this browser.

16 Tor Browser is maintained by the Tor Project.



## Taking Action

Below are some key questions to ask yourself and your colleagues about the library service:

- 1) Do we have any software or solution in place so that any trace of a library user's activity (websites visited, searches entered, logins saved within the browser, files downloaded, etc.) is deleted when they leave a public computer?
- 2) Do any of the internet browsers offered on our library's computers have a private browsing mode?
- 3) Do any of the internet browsers offered on our library's computers use a privacy-conscious search engine such as DuckDuckGo by default?
- 4) Would we consider offering a browser equipped with privacy-enhancing add-ons and features alongside the current default browser on staff and public computers?
- 5) Do we include data privacy in our library's digital skills courses, and do we have a clear process for reviewing these elements to ensure they are up to date?

## Further information

For more guidance on these tools and how to incorporate them into training for library users see [Libraries for Privacy: a digital security and privacy toolkit](#).



# Chapter 4:

## Inside the Library

### Physical Space

#### Why it's important

A library provides users with access to computers which can be used for internet access as well as word processing and other software. Library users' activity on computers needs to be protected physically as well as virtually. A user's privacy can be infringed by computer screens being overlooked or visible to others.

#### What this means for libraries – some practical considerations

Individuals may use library computers to look up sensitive information, such as financial or health-related information. They may feel less comfortable about doing this because of the layout of the computer desks: they may not want other people (including staff) seeing what they are looking at, and therefore may refrain from accessing the information they need. For library users to feel comfortable using computers to access information in a library, the computer area should have a privacy-friendly layout. It is possible to make changes to enhance privacy as follows:

#### **The layout of computer areas**

The way public computers are facing could be changed, to provide more privacy to library users making use of them. One change could be to the layout of public computers so that library staff cannot see everything from their own desks.

#### **Offer privacy screens for public computers**

Public libraries could offer privacy screens, which mean that the content displayed on the computer screen can only be seen when looking straight at it; people looking from the side will only see a black screen. Privacy screens cost on average £60,<sup>17</sup> depending on the size of the screen and on the supplier.



#### **Taking Action**

Below are some key questions to ask yourself and your colleagues about the library service:

- 1) Are public computers laid out so that they provide library users with some privacy when using them? That is, in a way where staff can't see the content of the screens from their own desks and where other library users cannot easily see what their fellow computer users are doing. If not, is there scope and space for the layout to be changed?
- 2) Would privacy screens for staff computers – to prevent library users waiting to be served seeing other individuals' private information – be appropriate?
- 3) Would privacy screens on public computers be a practical and affordable option for our library?

<sup>17</sup> Cost estimated as a rough average from prices of screens in February 2018.

# Chapter 5:

## Working with others

### Colleagues

#### **Why it's important**

Change requires shared vision, shared goals and teamwork. Those who manage libraries will need frontline staff to be aware of privacy issues and to assist library users. Library assistants will need the support of more senior staff in their organisation to make change happen. Any changes that involve the library's IT facilities will require discussion with ICT colleagues.

#### **What this means for libraries – some practical considerations**

Taking privacy conscious decisions and actions to protect library users' privacy may only be possible or effective with the cooperation and support of colleagues, both in the library and the ICT department.

#### **Engaging library colleagues**

There are various ways in which library staff may be able to raise awareness amongst colleagues of privacy issues and the actions that can be taken to enhance privacy within the library.

#### **Talk about privacy**

Making privacy a regular discussion point helps to situate the topic as an area where library staff can play a role. Library staff can start by simply mentioning the topic to colleagues. Regular meetings in your organisation (one-to-ones, team meetings or full staff briefings) can be forums to raise particular points such as encouraging users to choose strong passwords for online accounts or organising events to help library users learn to protect their privacy online.

#### **Create a group of interested staff**

It may be possible to bring together a group of colleagues, who are interested in the topic, to share resources and learn from one other. This could provide a forum for discussing in more detail what should and could be done in the library service. Or it could be possible to organise and run events or training sessions and generally champion the issue across the service.

#### **Run training sessions**

Training colleagues on how library users' privacy is affected online and what library staff can do to support library users is the best way to engage colleagues. It does require some prior knowledge, but there are resources that can be used for personal learning and delivering possible training sessions. These are listed in the 'Further Information' section at the end of this chapter.

## Working with ICT colleagues

Making changes to library computers and installing new software and tools will most likely involve working with ICT colleagues. These colleagues could be based within the library service or the parent organisation. Working with ICT colleagues will require library staff to: clearly explain why they are looking to install software or tools, listen to any concerns voiced by ICT colleagues and plan for ways to alleviate those concerns. Key topics it would be helpful to have considered ahead of meeting with ICT colleagues are: security, maintenance and legal requirements and reputational damage.<sup>18</sup>

### Security

One of the main concerns for ICT departments is the security of systems and networks. ICT Security colleagues are responsible for ensuring that communications and data are transmitted and stored securely and that malicious software will not infect systems, compromise the security of information used by the library service (or parent organisation) or interrupt services.

Some local authorities will also need to comply with [Public Services Network](#) (PSN) requirements. The PSN is a network shared by government departments and public sector organisations; to use it, organisations have to demonstrate that they meet specific security obligations set out by the Government Digital Service PSN team. PSN requirements do not directly apply to library networks, but they are often regarded as best practice.

It is important to understand that ICT colleagues will be reluctant to implement policies or install software that they see as a risk to systems security. To help prepare for a discussion with ICT colleagues, being able to explain clearly and in detail why a particular tool should be installed on computers and how this tool works, will facilitate discussion about any security risk posed.

<sup>18</sup> The National Cyber Security Centre has produced guidance on how organisations can protect themselves in cyberspace, which may be a useful resource to inform staff ahead of discussions with ICT colleagues. <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security> [Accessed October 2018]

### Maintenance

Any additional or new software and tools may require maintenance or updates. It is important to consider whether security patches are issued for the tool and whether ICT colleagues would be able to install updates on a regular basis on all library computers. Going into a meeting with a clear view of this – and therefore the ask of ICT colleagues – is essential.

### Legal requirements and reputational risk

ICT colleagues are involved in the implementation of policies that impact upon the organisation's systems and networks. They may invoke their responsibilities under the [Investigatory Powers Act](#) or the [Prevent Strategy](#), though more generally their concern may be to avoid criminal activity being conducted on library computers.

Criminal activity can have an impact on the security of systems and on the reputation of the library organisation or local authority. ICT managers and library managers may understandably be unwilling to take the risk to install a new tool on computers if it could be seen as making it easier for individuals to conduct criminal activities incognito. Browsers that facilitate anonymity, such as Tor Browser, can be perceived this way. Having an awareness of the legal framework that ICT colleagues work within, and being prepared to alleviate any concerns about the installation of a tool or introduction of a new way of working, will allow for a better informed conversation with ICT colleagues.

## Working with ICT colleagues



Staff and library users at Newcastle Libraries were previously able to use either Microsoft Internet Explorer or Google Chrome to browse the internet. Library staff requested that the Mozilla Firefox browser also be installed on all computers at all libraries – this open-source browser (with browser extensions enabled) is a more privacy-conscious browser.

ICT colleagues initially declined the request because they were unable to install updates to Firefox centrally; they would have to visit individual libraries to install updates and security patches on each computer, which they did not have capacity to do. In contrast ICT colleagues were able to install updates centrally for both Internet Explorer and Chrome. However, following further discussions between library staff and ICT colleagues it was agreed to purchase software that would centrally update the Firefox browser, and therefore the browser was installed on library computers.



### Taking Action

Below are some key questions to ask yourself and your colleagues about the library service:

- 1) Are there any regular meetings in our library organisation in which we can raise awareness of privacy issues?
- 2) Are there colleagues (in our team, another team or at a more senior level in our organisation) with whom we can discuss improving the privacy of library users?
- 3) Can we or other colleagues attend privacy-related training?
- 4) Can we or other colleagues run training on the topic for other library staff in our organisation?
- 5) Do we know who in our organisation makes decisions about software or tools to be installed on public and staff library computers?
- 6) Are we able to contact these individuals or have a short meeting to discuss security and privacy tools?

## Further Information

### Training sessions

The Tactical Technology Collective, a non-profit organisation with an interest in how technology impacts individuals' rights, provides a freely available [Training Curriculum](#) on their *Me & My Web Shadow* website. The materials aim to support facilitators training other people on data and privacy. Topics include: browsing, mobile communication and how the internet works.

The Electronic Frontier Foundation's [Security Education Companion](#) website contains information on how to train people as well as lesson plans and training materials on: passwords, threat modelling and using specific tools.

The [Library Freedom Project](#) is a US-based organisation that works with American librarians to protect library users from mass surveillance when using libraries. The resources pages on the Project's website contain training session slides and useful links. The Library Freedom Project is also running a six-month course called Library Freedom Institute, and [course materials](#) are available for re-use.

The [Data Privacy Project](#) was developed by staff at the Brooklyn Public Library and New York-based partners to teach local library staff. The website includes short online learning modules as well as a detailed curriculum for a facilitator to deliver face-to-face sessions.

In the UK, Scottish PEN has been running workshops for library staff across Scotland, which helped to inform their online data privacy and security [toolkit](#). Inspired by this, staff at Newcastle Libraries created a one-hour introduction for a small group of library colleagues. The materials for the Newcastle Libraries session are available under an open licence on [GitHub](#).

As part of the process of creating this guide, Aude Charillon held six workshops on online data privacy with library staff across the UK. The slides for this workshop are available under CC0 on [GitHub](#). Whilst these slides informed the guide, they serve as an introduction to online data privacy alone and are not designed to cover the content of this guide as a whole.

# Chapter 6:

## Working with others

### Suppliers

#### Why it's important

In 2014 concerns were raised in the library sector over the discovery that e-book reader application Adobe Digital Editions was transmitting reader data in plain text over the internet. This example demonstrates the need for library services to have mechanisms in place to ensure that suppliers protect library users' personal data through compliance with data privacy legislation, and with other privacy requirements that libraries may choose to stipulate. This is critical as suppliers deliver many essential services for libraries which rely on user data, such as library management systems, computer booking systems and library apps.

#### What this means for libraries – some practical considerations

Third party suppliers provide access to systems that facilitate the running of the library service and provide library users with electronic resources and online services. Systems may include library management systems, self-service kiosks, computer booking systems, library apps, e-book platforms, online encyclopaedias, subscription-based external databases and wifi. These products handle library users' information.

It is the responsibility of the library service to ensure that third party suppliers guarantee that they comply with GDPR and the library service's own policies, ensuring that personal information is kept private and is secure against unauthorised access.

#### GDPR compliance

Library suppliers processing users' personal information must comply with the General Data Protection Regulation (see [Chapter one](#)) and provide guarantees to libraries that they do so. These guarantees must demonstrate that:

- the product only collects or processes personal information that is necessary to deliver the service;
- the supplier only collects and processes information as instructed and for the purpose set out by the library service; and
- the supplier has a process in place to deal with data breaches which includes notifying the library.

GDPR requires an organisation to have a written contract with any supplier that processes library users' personal information. The Information Commissioner's Office has a useful [checklist](#) of the areas and terms the contract must cover. Under GDPR, it is also a legal requirement to consider 'privacy by design' in the way systems process personal information.

#### Privacy by design

'Privacy by design' is an approach to developing technology where privacy is considered from the start and built into systems and technology from the outset. In this way, privacy is embedded as default. It is worth thinking about whether and how public libraries can take a joined-up approach to work with suppliers and contribute to developing systems that have a 'privacy by design' approach.

## Auditing suppliers' commitment to data privacy

When tendering for, or choosing, a new system or electronic resource for the library, staff will need to assess suppliers' practices and commitment to data security and data protection. It may also be useful to undertake an audit of current systems and subscription-based databases.

In *Measuring library vendor cyber security: seven easy questions every librarian can ask* (Code{4}lib Journal, 2016), US authors Alex Caro and Chris Markman identified the following questions as ways of rapidly assessing a system:

- “
1. **Data breach policy:** is there a formal process in place to report data breaches if or when they occur?
  2. **Data encryption:** if patron data is stored by the vendor [supplier], is it encrypted?
  3. **Data retention:** does the vendor purge the search history records of patrons on a regular basis?
  4. **Terms of Service 'ease of use':** can the average patron read and fully understand the vendor's terms of use policy?
  5. **Patron privacy:** does the vendor use Google Analytics or other tracking software to monitor users?
  6. **Secure connections:** does the vendor's website enforce secure connections only? (HTTPS or better?)
  7. **Advertising networks:** does the vendor's website participate in ad networks?<sup>19</sup>
- ”

For suppliers working with libraries in the UK and the rest of the EU, answers to some of those questions will be covered by GDPR requirements.

Library staff may want to use a more in-depth checklist. The Electronic Frontier Foundation's 2018 *How to assess a vendor's data security* article and the UK Information Commissioner's Office 2012 *Guidance on the use of cloud computing* offer some pointers for more detailed questions to ask suppliers. Here are examples of such questions:

- In which country or countries is the supplier processing data?
  - If personal data is transferred outside of the European Union, does the supplier offer guarantees regarding its data protection obligations under GDPR?
- Are there any guarantees that no data is shared with third parties?
- Has the supplier's system undergone an external security audit?
  - Are the results available?
  - How were any gaps addressed?

<sup>19</sup> This abstract is reproduced here under the [Creative Commons Attribution 3.0 United States licence](https://creativecommons.org/licenses/by/3.0/).

## Technical specifications



When tendering for a new system or electronic resource, staff can take a privacy conscious approach by making sure that privacy and security requirements are included in the technical specifications.

Below are some examples of requirements that could be asked of a supplier of a library management system. The examples draw on a 2016 tender by Newcastle Libraries.

### Mandatory requirements

- **System hosting:** a supplier must specify hosting options ie hosted by the supplier, hosted by a third party or hosted internally by the library service, and provide details of each option including the country in which the servers are located, whether the servers are multi-tenant or single-tenant, whether they are physical or virtualised.
- **Architecture:** if the system is to be hosted on site, a full architecture diagram for the solution – including all third-party arrangements – is essential and must be supplied.
- **Information security:** a supplier must provide a compliance statement with respect to the BS ISO / IEC 27002 Code of practice for information security controls.
- **PSN Compliance:** a supplier must outline what industry standards they comply with (eg [ISO 27001](#)).
- **Data retention:** a supplier should demonstrate evidence of data retention and disposal policies in compliance with the data retention policies of the library service. Such policies should be in place on 'go live' date.
- **Data protection:** a supplier must provide evidence of measures in place to protect and limit access to information by authorised personnel only, and provide evidence of compliance with the GDPR and the library service's data protection policies.
- **Encryption:** all data in motion and data at rest must be encrypted using best practice encryption methods, eg HTTPS, salted hashing for passwords.
- **Accessibility:** any web interface must be accessible over the Tor network.
- **User authentication:** access to the system must be password protected. The system must be able to integrate with the organisation's existing central authentication systems or single sign-on systems.

### Highly desirable

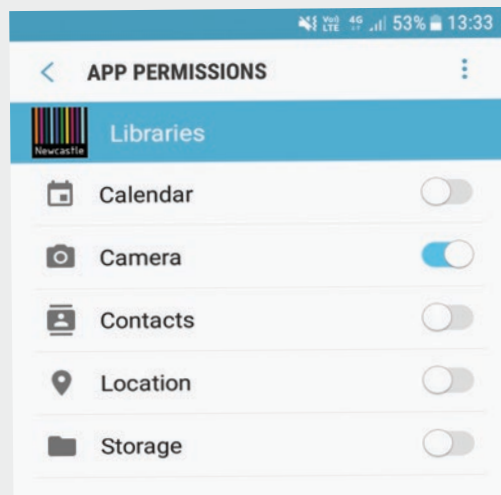
- **Anonymisation:** there should be capability to retain transactions in anonymised form after a period of time decided by the library service.
- **User privacy settings:** could there be the possibility for the library service to enable library members to set their own preferences for the retention of their loan and item reservations history.



## Library apps

The supplier of a library app will need to demonstrate how they comply with GDPR; for example what personal information they are using and collecting, how long they are retaining it and if it is all necessary to deliver the app's services.

Library apps can also give users some control over their personal data. This example from Newcastle Libraries' app shows how users can choose permissions for their app, for example giving the app access to the phone's camera but not location.



Newcastle Libraries App permissions (screenshot taken on Android operating system April 2018).



## Taking Action

Below are some key questions to ask yourself and your colleagues about the library service.

- 1) Does our library service have written contracts with all suppliers that process library users' personal information?
- 2) Have contracts and agreements with suppliers been updated to include GDPR requirements?
- 3) Has the supplier explained how their product and processes comply with GDPR?
- 4) Has the supplier communicated or discussed its data retention policy with the library service?
- 5) Do suppliers offering a service directly to library users have a clear, easy-to-find and easy-to-understand privacy statement?
- 6) Does the supplier use encryption (eg HTTPS for websites) to keep data secure?
- 7) Does the supplier use encryption by default for all processes – both when the data is in transit and when it is stored?
- 8) Does the supplier offer the option of opting out of personalisation features?
- 9) Has the supplier's system undergone a security audit? If so, are the results available? How were any gaps addressed?
- 10) Could your library service work with others (in a consortium or a national library organisation) to approach suppliers to ask for changes?

### Further information

- American Library Association: [Library privacy guidelines for library management systems](#).
- American Library Association. [Library privacy guidelines for e-book lending and digital content vendors](#).
- Marshall Breeding. Privacy and security for library systems. ALA Library Technology Reports, May-June 2016 Vol. 52 no.4. Freely available to [download from ALA TechSource](#)

# Resources

Scottish PEN: [Libraries for privacy toolkit](#)

Brooklyn Public Library and partners:  
[Data Privacy Project](#) – Training course for library staff

Library Freedom Project:  
[Resources, information and advice](#)

American Library Association:  
[Choose Privacy Every Day resources](#)

Electronic Frontier Foundation:  
[How to deploy HTTPS correctly](#)

[How to assess a vendor's data security](#)

[Surveillance Self-Defence](#)

[Security Education Companion](#)

Information Commissioner's Office:  
[information for organisations](#)

[Measuring Library Vendor Cyber Security: Seven Easy Questions Every Librarian Can Ask.](#)  
code{4}lib Journal, issue 32, 2016-04-25

IFLA:  
[Internet Manifesto](#) (2014)

[Statement on privacy in the library environment](#) (2015)

[Statement on the Right to be Forgotten](#) (2016)

BIC: [RFID privacy toolkit](#)

National Cyber Security Centre: [10 Steps to cyber-security](#)

# Glossary and Technical Terms

## Browser add-on / extension

A browser add-on or browser extension is a piece of software that provides additional features or functionalities to the browser.

## Cookies

Cookies are small files that function in the background of a website and are designed to remember information about the browser. Some cookies are essential for a webpage to display properly, some are linked to a user's preferences, some are an add-on to a website to offer a specific service and some are used to gather information about user behaviour.

## Hosting

Hosting refers to the owners and the location of the servers on which a system runs.

## Hosted locally

Hosted locally means that the system 'lives' on a server that belongs to the organisation. The server owner has more control over the settings, such as what to record and not to record about the use of the database. Usage logs can constitute personal information.

## HTTPS

HTTPS is an internet protocol that encrypts data travelling from a browser to a website and vice versa.

## ICO

The Information Commissioner's Office (ICO) is responsible for monitoring the application of GDPR in the UK. Information and resources regarding GDPR and other data protection matters are available [from the ICO website](#).

## IP address

An IP (Internet Protocol) address is a number that uniquely identifies a device connected to the internet (computer, smartphone, etc.). Similarly to a postal address, an IP address allows network communications to be directed to the right place.

## ISO/IEC 27001

[ISO/IEC 27001](#) specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001 are generic and are intended to be applicable to all organisations, regardless of type, size or nature.

## Log files

Log files are files where users' activity on a system is logged. They typically contain the date and time a user accessed the system, what parts of the system they viewed and what actions they took.

## Patch

A patch is a piece of code that fixes issues in a computer programme or system.

## Plug-in

A plug-in is another word for an add-on or an extension. It is a piece of software that adds a new feature to an existing software eg a web browser. A particular plug-in may be considered insecure because of known vulnerabilities.

### Personal data

In data protection law, 'personal data' encompasses any information that can help identify a living person, such as their name, date of birth and contact details.

### Positive action

GDPR sets out that when relying on [consent as the legal basis](#) for processing personal data, citizens should take a positive action to give their consent. A positive action can be citizens ticking a box on an online form to agree to a specified use or verbally answering a yes/no question. Already ticked-in boxes or statements that do not require the citizen to make a clear affirmative act to agree to the processing of their personal data are not considered valid forms of consent.

### Sensitive personal data

In data protection law, sensitive personal data is a specific set of 'special categories' that must be treated with extra security. These categories include:

- ethnic origin;
- religious beliefs;
- biometric data;
- health data;
- sexual orientation

### Tracking

Tracking is when third-parties follow and record the behaviour of someone using the internet from one website to another without the user knowing or having agreed to this.



This report was written by Aude Charillon with Dr Jenny Peachey and Rachel Heydecker

November 2018



Andrew Carnegie House  
Pittencrieff Street  
Dunfermline  
KY12 8AW

Tel: +44 (0)1383 721445  
Fax: +44 (0)1383 749799  
Email: [info@carnegieuk.org](mailto:info@carnegieuk.org)  
[www.carnegieuktrust.org.uk](http://www.carnegieuktrust.org.uk)

Carnegie United Kingdom Trust  
Registered Charity No: SC 012799 operating in the UK  
Registered Charity No: 20142957 operating in Ireland  
Incorporated by Royal Charter 1917



CILIP The library and information association  
7 Ridgmount Street  
London  
WC1E 7AE  
[www.cilip.org.uk](http://www.cilip.org.uk)

Registered charity no: 313014



City Library  
Charles Avison Building  
33 New Bridge Street West  
Newcastle upon Tyne  
NE1 8AX

[www.newcastle.gov.uk/libraries](http://www.newcastle.gov.uk/libraries)



Carnegie United Kingdom Trust  
Registered Charity No: SC 012799 operating in the UK  
Registered Charity No: 20142957 operating in Ireland  
Incorporated by Royal Charter 1917

