Westmorland & Furness Council

Privacy Notice
Library Services

When processing your personal, special category personal or criminal/law enforcement data, Westmorland and Furness Council ('the council') is required under Articles 13 and 14 of the UK General Data Protection Regulation (UKGDPR) to provide you with the information contained in this Privacy Notice.

This notice explains what the council will collect, who it will be shared with, why we need it and how we will use it. The council will continually review and update this Privacy Notice to reflect service changes, feedback from customers and changes in the law.

The council is also required to comply with the data protection principles as laid out in the UKGDPR, to ensure that personal data is:

- processed lawfully, fairly and in a transparent manner
- collected for specific, explicit, and legitimate purposes
- adequate, relevant, and limited to the purposes for which it was collected
- accurate and up to date
- kept for no longer than is necessary for the purpose(s) for which it was collected
- secured using appropriate technical or organisational measures

Registration

As an organisation that processes large amounts of personal, special category personal or criminal/law enforcement data, referred to in legislation as a data controller, the council is required to register with the Information Commissioner's Office (ICO)

Name: Westmorland and Furness Council
Address: South Lakeland House, Lowther Street, Kendal, Cumbria, LA9 4DQ
Registration Number: ZB512761

The council's Registration Certificate can be viewed:
https://ico.org.uk/ESDWebPages/Entry/ZB512761

About the Service

This Privacy Notice applies to the Library Service operated by Westmorland and Furness Council.
All the information you give us will be kept safe and secure whether it is written or on a computer system. We will treat any personal information confidentially and will comply with

the UK General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018. This means that if we keep any of your personal data we must:

- tell you what information we need to collect from you
- only use the information for the reason we have agreed with you
- not ask for more information than we need to provide the services
- let you see any information we have collected about you, on request
- keep the information safe, secure, and confidential
- personal information will be deleted in accordance with council policy

Joining the Library is free and enables you to use any of the public libraries in the Westmorland and Furness Council area and in the adjoining Cumberland Council area. We offer a broad range of online and physical resources which are free to access with your library membership number.

You can find out more about the service and resources we provide at:
https://www.westmorlandandfurness.gov.uk/libraries-and-archives

Data Controller Arrangements

In most cases Westmorland and Furness Council is the data controller, however there may be instances where data is shared with another party as joint Data Controllers, or where the Council is operating as a data processor for another party.

What is personal data?

UKGDPR Article 4 defines personal data as: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

What is special category personal data?

UKGDPR Article 9 defines special category personal data as: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

What is criminal/law enforcement data?

The council is a competent authority as described in Schedule 7 of the Data Protection Act 2018 and is permitted to process data for law enforcement purposes that include: the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

What information does the council collect about me?

The council is required to process either your personal, special category/sensitive or criminal/law enforcement data to meet legal obligations and make robust recommendations and decisions.

The **Personal Data** requirements are:

The Library Service will collect and process the categories of data listed below for the following purposes:

- managing your library membership
- receiving and fulfilling requests for library resources
- providing appropriate information, support, and services
- service quality and improvement

The **Special Category Data** requirements are:

The following data is required for your library membership account:

- Title
- Name
- Postal Address
- Date of Birth
- Gender

To receive service and membership notifications, or to contact you about library/membership issues, we also require one or more of the following:

- Primary Telephone Number
- Secondary Telephone Number
- Email Address
- Postal Address

We may also collect, store, and use the following 'special categories' of more sensitive personal information:

- Health i.e. disability

The Criminal/Law Enforcement Data requirements are:

CCTV and Surveillance

We operate surveillance equipment within some of our services for the purpose of either, public and staff safety, or the prevention and detection of crime. CCTV is also installed on the outside of some of our buildings for the purposes of monitoring building security and crime prevention and detection.

How does the council collect data about me?

As part of this service the council will collect personal, special category personal or criminal/law enforcement data from you in the following ways:

- by telephone
- by email
- on paper
- in person in a Library location
- online via the Library Service website

Why does the council collect my personal data?

The Library Service collects personal, special category personal or criminal/law enforcement data to enable it to:

- manage your library membership
- receive and fulfill requests for library resources
- provide appropriate information, support, and services
- service quality and improvement

Who does the council share personal data with?

Where there is a lawful reason to do so the Library Service may share personal, special category personal or criminal/law enforcement data with:

- Our online resource suppliers

Data Sharing

We may share your information with partner organisations including the Library Management System suppliers (only in the context of administering the library systems). We may also share some information with the providers of online resources accessed via the Library Services' website. (In this context, some information is shared by the customer directly).
We may also share personal data, where it is necessary and proportionate to do so, with the Police for law enforcement purposes, such as the prevention, investigation and detection of crime.

How information is shared with online resource suppliers
Here are the responses from our suppliers regarding the storage and usage of personal data and information:

Koha - library management systems (PTFS Europe Ltd)

What information do you collect and how is it collected?
Personal information is supplied by patrons when joining Westmorland and Furness Libraries, including name, date of birth, gender and contact details.

Where/how stored?
Test and production servers are hosted in different locations within the UK. No data leaves the UK. All data is encrypted at rest. Backups are encrypted using GPG software and kept in a separate location. Encrypted filesystems are used to further reduce risk. Passwords within the application are encrypted with Bcrypt.

Is customer information storage sub-contracted?
No.

Netloan – public access computer booking system (Lorensbergs Ltd)

What information do you collect and how is it collected?
Library user's card number, first name and surname, user reservation history, reservation times and duration, public access computer details.

Where/how stored?
Data is stored on the hosted application server. Log files are stored for 7 days and contain events and errors. SQL database records all user reservations.

Is customer information storage subcontracted?
No.

The Library App (Solus UK Ltd)

What information do you collect and how is it collected?
User ID only.

Where/how stored?
Information is stored locally within the app on the user's device and is encrypted. Non-identifiable transaction data is for analytics purposes.

Is customer information storage subcontracted?
No.

Access to Research (Publishers' Licensing Services Ltd)

What information do you collect and how is it collected?
No personal information of library members is collected or stored.

Where/how stored?
Not applicable.

Is customer information storage sub-contracted?
No.

Ancestry (provided by ProQuest)

What information do you collect and how is it collected?
No personal information of library members is collected or stored.

Where/how stored?
Not applicable.

Is customer information storage sub-contracted?
No.

Borrowbox e-books, e-audiobooks & e-press (provided by Bolinda Digital Pty Ltd)

What information do you collect and how is it collected?
Library barcode number, email address, name if supplied, BorrowBox loan history.

Where/how stored?
Data is stored and processed in the EEA and in the US.

Is customer information storage sub-contracted?
Yes. Amazon Web Service (AWS).

Britannica

What information do you collect and how is it collected?

First name; last name; username; password; email address (optional); security question (optional). Personal data relating to Library users is only collected if they register for a My Britannica account.

Where/how stored?

Stored on Amazon Web Services (AWS) data servers in accordance with GDPR guidelines.

Is customer information storage sub-contracted?

Yes. Amazon Web Services (AWS).

British Newspaper Archive (provided by JCSOnline)

What information do you collect and how is it collected?

Personal data relating to Library users is only collected if they register for a British Newspaper Archive account.

Where/how stored?

Data is stored on servers in located in the UK. British Newspaper Archive has an ISO27001 Information Security Certification.

Is customer information storage subcontracted?

Yes. Brightsolid for infrastructure and data centres. Sub-contractors are also used for payment, customer support and CRM services.

Findmypast (provided by JCSOnline)

What information do you collect and how is it collected?

Personal data relating to Library users is only collected if they register for a Findmypast account.

Where/how stored?

Data is stored on servers in located in the UK. British Newspaper Archive has an ISO27001 Information Security Certification.

Is customer information storage subcontracted?

Yes. Brightsolid for infrastructure and data centres. Sub-contractors are also used for payment, customer support and CRM services.

Oxford Reference Package (provided by Oxford University Press)

What information do you collect and how is it collected?

OUP holds data of library customers on Oxford DNB, OED, Oxford Reference, Oxford Dictionaries, and gratis Oxford Research Encyclopaedias, Very Short Introduction and Oxford Bibliographies modules. On these systems, usernames are held to allow for sign-in, with secure integration to an access control system for securing passwords. Where purchasing is a website functionality, billing addresses are held within a separate secure database.

Where/how stored?

For all data collected on European customers, the data is secured, either within Amazon Web Services (AWS) within the European Union or on-premises.

Is customer information storage subcontracted?

The websites are hosted by a third party and the access control is provided by a third party, on behalf of OUP.

TheComputerSchool.net (provided by TheComputerSchool.net)

What information do you collect and how is it collected?

No personal information of library members is collected or stored.

Where/how stored?

Not applicable.

Is customer information storage sub-contracted?

No.

Theory Test Pro (provided by Well Informed)

What information do you collect and how is it collected?

Library member name and email address

Where/how stored?

Data is stored on a secure website, registered in the UK.

Is customer information storage subcontracted?

No.

The **Library Service** may receive personal, special category personal or criminal/law enforcement data about you from the third parties mentioned above and other public bodies and organisations. In this case, we will tell you the source of the information unless we are unable to do so by law.

Legal Basis

Where the council identifies the requirement to process personal, special category/sensitive or criminal/law enforcement data, depending on the specific data being shared, it must have at least one of the following:

- for personal data, a legal basis under UKGDPR Article 6
- for special category/sensitive data, a condition under UKGDPR Article 9
- for criminal/law enforcement data, a purpose under Data Protection Act 2018 - Schedule 8

If we are relying on consent to process your personal, special category personal or criminal/law enforcement data, you have the right to object at any time by contacting the service or officer the data was provided to.

If **personal data** is being processed the council must select at least one legal basis from the list below:

- **UKGDPR Article 6(1) (c) Legal Obligation**
- **UKGDPR Article 6(1) (e) Public Task/Public Interest/Official Authority**

Where the council is relying on UKGDPR Article 6(1)(c) all Relevant Legislation should be listed below.

If **special category personal data** is being processed the council must select at least one condition from the list below:

- **UKGDPR Article 9(2) (f) Necessary for the establishment, exercise or defence of legal claims**

If **criminal/law enforcement data** is being processed the council must select at least one condition from the list below:

- **UKGDPR Schedule 8(6) Legal Claims**

Relevant Legislation

These legal bases above are underpinned by acts of legislation that dictate what actions can and should be taken by local authorities, including:

- **Libraries and Museums Act 1964**

Automated Decision-Making/Profiling

Automated individual decision-making is a decision made by automated means without any human involvement. Automated individual decision-making does not have to involve profiling, although in some cases it might.

A definition of Profiling can be found in: UK GDPR - Article 4(4) and further information can be found at: ICO - Automated Decision Making and Profiling

We **do not** use your information for automated decision-making or profiling purposes.

CCTV and Surveillance

We operate surveillance equipment within some of our services for the purpose of either, public and staff safety, or the prevention and detection of crime. CCTV is also installed on the outside of some of our buildings for the purposes of monitoring building security and crime prevention and detection.

Civil Enforcement Officers (CEOs) who undertake the enforcement of parking restrictions, are each equipped with a Body Worn Video Device (BWVD), which has both video and audio recording capability.

Images captured by CCTV will be kept in accordance with the council's Retention and Disposal Schedule. However, on occasions there may be a need to keep images for longer, for example where a crime is being investigated. Images can be requested by writing to: dataprotection@westmorlandandfurness.gov.uk

We will only disclose images and audio to other authorised bodies who intend to use it for the purposes stated above. Images and audio will not be released to the media for entertainment purposes or placed on the internet for public viewing.

We operate CCTV and disclose in accordance with the codes of practice issued by the Information Commissioner and Biometrics and Surveillance Camera Commissioner.

CCTV Requests

The Police are permitted to request footage under the Data Protection Act 2018 (Schedule 2).
Officers making requests must present a completed Schedule 2 Form, signed by the authorised officer to confirm that the information is needed for the detection or prevention of a specific crime. Schedule 2 Forms should be submitted by email to: dataprotection@westmorlandandfurness.gov.uk

Personal and business (insurance and solicitors) applicants should complete the CCTV and Surveillance - Request Form (doc , 282KB)
Completed forms should be accompanied by the relevant proof of identity or authorisation.

Failure to provide the required evidence will result in the council refusing requests.

National Fraud Initiative/Data Matching

The Council is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing, administering public funds or where undertaking a public function, in order to prevent and detect fraud.
The Council is required to participate in the Cabinet Office's National Fraud Initiative: a data matching exercise to assist in the prevention and detection of fraud. The Council is obliged to provide particular sets of data to the Minister for the Cabinet Office for matching for each exercise. The Cabinet Office is responsible for carrying out data matching exercises in accordance with the https://www.gov.uk/government/publications/code-of-data-matching-practice-for-national-fraud-initiative.
Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.
For further information on the Cabinet Office exercise please see:

- https://www.gov.uk/guidance/national-fraud-initiative-public-sector-data-requirements
- https://www.gov.uk/government/publications/fair-processing-national-fraud-initiative/fair-processing-level-3-full-text

For further information please contact: nfi.WAF@westmorlandandfurness.gov.uk.
Alternatively, you can refer to the Privacy Notice - National Fraud Initiative:

https://www.westmorlandandfurness.gov.uk/your-council/data-protection-and-privacy/services-privacy-notices.

Elected Members

In order for Elected Members to act on your behalf and resolve the issues you have raised they may need to collect some personal, special category personal or criminal/law enforcement data. This could include your name and address, and/or sensitive personal data, which could be concerning your health or ethnic origin.

In some circumstances your explicit consent may be needed to allow for the processing of your data. If this is needed the relevant Elected Member will contact you directly.

Elected Members will:

- only share data with the organisations necessary to deal with your enquiry i.e., different council departments, and to resolve any issues you have raised
- not share your data with third parties, unless it is required for law enforcement purposes to prevent or detect crime, to protect public funds or where required or permitted to share data under other legislation
- keep your data secure using the council's secure IT and email systems
- retain/destroy your data in accordance with the council's Retention and Disposal Schedule

You have the right to access your personal, special category personal or criminal/law enforcement data and to rectify mistakes, erase, restrict, object or move your data in certain circumstances.
You can withdraw your consent for your personal, special category personal or criminal/law enforcement data to be processed as described above at any time. If you would like this to happen or you have a complaint about how your data is handled, please contact your Elected Member.
If you are not satisfied with the response or believe the Elected Member is not processing your personal, special category personal or criminal/law enforcement data in accordance with the law you can complain to the Information Commissioner's Office (ICO).

Data Transfers

It may sometimes be necessary to transfer personal, special category personal or criminal/law enforcement data beyond the UK to comply with legal or other obligations.

Where data is required to be transferred to the European Union or other adequate countries the council will ensure that all relevant safeguards are in place before this takes place and that all aspects of the UKGDPR/Data Protection Act 2018 are complied with.

Data requested for transfer to non-adequate countries will be subject to a Transfer Impact Assessment, that includes the identification of appropriate safeguards prior to data being authorised for transfer.

Data Security and Retention

The council is required by UKGDPR Article 32 to ensure that appropriate organisational and security measures are in place to protect your personal, special category personal or criminal/law enforcement data.

Security measures include: anonymisation, pseudonymisation, encryption, access controls on systems, regular testing of our systems, security training for all employees. You can find further information in the following documents:

- Information Security Policy
- Data Protection Policy
- PSN Connection Compliance Certificate
- NHS DS&P Toolkit - Compliance Certificate

If you access information online, the council website does not store or capture personal information, but merely logs a number called your IP address which is automatically recognised by the system. The system will record personal information if you:

- subscribe to or apply for services that require personal information
- report a fault and give your contact details for us to respond
- contact us and leave your details for us to respond

For further information visit our Cookies Policy.

Westmorland and Furness Council will only store your information for as long as is legally required in accordance with the council's Retention and Disposal Schedule or in situations where there is no legal retention period established best practice will be followed.

To help you understand the Schedule the council has published a Retention Schedule - Quick User Guide.

If you have any questions about the Schedule or the Quick User Guide, please contact record.centre@cumberland.gov.uk.

If you experience any problems in relation to your personal data or you see something that doesn't look right, contact the council by email at: databreaches@westmorlandandfurness.gov.uk.

Contacting the Council

Emails

If you email us, we may keep a record of your contact and your email address and the email for our record keeping of the transaction. We suggest that you keep the amount of confidential information you send to us via email to a minimum and use our secure online forms and services. Where available, you can sign up for email alerts for selected services using an external service from GovDelivery, with control over your preferences.

Telephone Calls

The council will inform you if your telephone calls are being recorded or monitored and will not record any financial card details if you make payments by telephone.

Your Rights - Data Subject Access

What is a Subject Access Request?

Individuals have the right to access and receive a copy of their personal data, and other supplementary information held by Westmorland and Furness Council. This is commonly referred to as a Subject Access Request or 'SAR'.

Subject Access Requests can be made verbally or in writing, including via social media. Please see 'Submitting Subject Access Requests' below for information.

Data Subjects can make requests themselves, or ask another person to do it on their behalf i.e. child (under 12), attorney, litigation friend. In these circumstances the council will need to

see evidence of permission to request the data of another person and it should be emailed at the same time as the request is submitted. Failure to provide evidence may result in delays with handling your request or it being declined.

In most cases the council does not charge a fee for handling Subject Access Requests, it can however charge a fee:

- where a request is repeated to cover administrative costs
- where a request is manifestly unfounded or excessive
- in some circumstances, we may refuse to handle Subject Access Requests where they are vexatious, manifestly unfounded or excessive

Please be aware that the council may seek evidence of your identity and clarification of your request to assist with the identification of relevant information.

Once your request has been accepted, the council will:

- provide a response within one calendar month (where possible)
- inform you if your request cannot be responded to within one calendar month, as it is complex or you have submitted more than one request (the deadline for providing a response can be extended by up to a further two months)
- conduct reasonable searches for the requested information
- inform you if information is exempt from disclosure
- provide a response via secure email unless an alternative format has been requested

Submitting Subject Access Requests

If you would like to submit a request or you would like assistance with submitting a request, please contact us:

By post: Westmorland and Furness Council, South Lakeland House, Lowther Street, Kendal, Cumbria LA9 4DQ

By email: subjectaccess@westmorlandandfurness.gov.uk

By telephone: 01539 637 437

If you have any concerns about how your personal data is used by the council please contact the Data Protection Officer: dataprotection@westmorlandandfurness.gov.uk.

Your Rights - Other

In addition to your right of access the UKGDPR gives you the following rights:

- the right to be informed via the council's Privacy Notice
- the right to withdraw your consent. If we are relying on your consent to process your data, then you can remove this at any point
- the right of rectification, we must correct inaccurate or incomplete data within one month

- the right to erasure. You have the right to have your personal data erased and to prevent processing unless we have a legal obligation to process your personal information. Where your personal data has been shared with others, we will ensure those using your personal data comply with your request for erasure.
- the right to restrict processing. You have the right to suppress processing. We can retain just enough information about you to ensure that the restriction is respected in future
- the right to data portability. We can provide you with your personal data in a structured, commonly used, machine readable form when asked
- the right to object. You can object to your personal data being used for profiling, direct marketing or research purposes
- you have rights in relation to automated decision making and profiling, to reduce the risk that a potentially damaging decision is taken without human intervention.

Unless otherwise stated above you can exercise any of these rights by contacting the council's Data Protection Officer:
Email: dataprotection@westmorlandandfurness.gov.uk
Post: Westmorland and Furness Council, South Lakeland House, Lowther Street, Kendal, Cumbria, LA9 4DQ

Consent

Where our processing of your personal, special category personal or criminal/law enforcement data is based on your consent, you have the right to withdraw your consent at any time.

If you do decide to withdraw your consent, we will stop processing your personal data for that purpose, unless there is another lawful basis we can rely on - in which case, we will let you know.

If you withdraw your consent, it won't impact any of our processing up to that point but may affect the services you are eligible for in future.

If you'd like to discuss withdrawing your consent in relation to data processing please contact the council's Data Protection Officer:

Email: dataprotection@westmorlandandfurness.gov.uk
Post: Westmorland and Furness Council, South Lakeland House, Lowther Street, Kendal, Cumbria, LA9 4DQ

Verifying Your Identity

When exercising the rights mentioned above, please be aware that under UKGDPR Article 12(6) additional information can be requested to verify that you are the data subject if your identity is unconfirmed. Please note that:

- additional documentation is only required when the council cannot verify your identity using internal council systems that relate to the service you are requesting information about

- the council will contact you for this documentation prior to processing your request
- the statutory deadline for responding to your request will start when you have provided the additional documentation
- failure to provide additional documentation may lead to the council rejecting your request.

Complaints

If you have concerns about the way the council has processed your data, please contact:

Email: dataprotection@westmorlandandfurness.gov.uk
Post: Westmorland and Furness Council, South Lakeland House, Lowther Street, Kendal, Cumbria, LA9 4DQ
If you are not satisfied with our response or believe we are not processing your personal data in accordance with the law you can complain to the Information Commissioner's Office (ICO).