MLS Hosted Privacy Statement

1.1

Scope

We take care to protect the privacy of customers and users of Capita websites and Products. Set out below is an explanation of how we process and manage the information.

1. Introduction

Capita Education Software Services – trading as MLS are fully committed to keeping your information safe.

This privacy notice is to help you understand what information MLS collects, the purpose for which it is collected and who we share the information with. It also explains the decisions that you can make about your information.

This notice will provide you with the following information:

- Accountability
- Who is collecting information about me?
- What information is transferred?
- Why are you collecting this information?
- What is the legal basis for processing the information?
- Where the data is stored?
- Security of the data stored
- Where the data is processed
- Data Retention
- Data protections/GDPR Awareness
- Staff Vetting
- Additional Third Party Processing

For the purposes of this Privacy Notice:

"Information" means either the data held within Library System or the School and contact contractual and support information, this will be specified where referred to.

"MLS" means Capita Education Software Services – trading as MLS.

"Customer" means the establishment that purchases the service. i.e. individual school, Multi Academy Trust

"Data Controller" refers to the Customer

"Data Processor" refers to MLS

"Data Subject" refers to a living person details that are recorded in the SIMS application by the Data Controller

"Individual" refers to a person or employee who is associated with a named Customer

"EEA" is the European Economic Area

2. Accountability

MLS provides you, the customer with the Library Management system. As you are responsible for the information that is entered and maintained the Library Management system, this makes you, the customer, the Data Controller. MLS delivers the service that provides you with the ability to store this information and as such does not enter your information into this system for you, this makes MLS the Data Processor.

As a Data Processor, MLS provide a hosted service that includes the application and customer data as well as support services to the customer. As the Data Controller you are responsible for the information in the Library Management system and must be able to demonstrate compliance with the 8 Principles of the Data Protection Act for the processing of personal information.

Details of the 8 Principles are detailed on the Information Commissioner Office's website: https://ico.org.uk/fororganisations/guide-to-data-protection/data-protection-principles/

3. Who is collecting information about me?

Capita Education Software Services – Trading as MLS

Arden House
Shepley Lane
Hawk Green
Marple
Stockport
SK6 7JW
Website : www.microlib.co.uk

Should you have any queries relating to the collection of your information or about this policy please contact the MLS Data Privacy Officer at privacy.mls@capita.co.uk

4. What information is transferred?

One of the key features of GDPR is to be transparent with data subjects about the information collected and processes of the data. It would be advisable to include in information to parents/students and in privacy notices that schools do transfer personal data to the library system. What data transferred is up to the school. To allow the full function of the library system MLS recommends the minimum of the following be transferred:

- Forename
- Surname
- Gender
- Date of Birth
- Tutor group
- Year Group
- Management System ID

Date of Birth is key to restricting age appropriate resources on issue thus is a mandatory field when transferring via csv file or MLS Connect. There is optional data which can be transferred – Photograph, Address, Telephone, Ethnicity and guardian information.

5. Why are you collecting the information?

The School Library Association believes that the purpose of a school library is:

- to provide a flexible space with a wide and inclusive range of resources to support learning and teaching throughout the school.
- to have a vibrant role in the development of a culture that promotes wider reading, motivated readers and learners for life.
- to provide a place for collaborative learning, creativity, and for developing independent research and information literacy skills.

To facility the library a computerise library management system by MLS can be utilised to aid in searching for resources, reporting, loan management and so on. MLS collect the inform above to be able to provide this function and the necessary features needed to operate a library system.

6. What is the legal basis for extracting and processing this information?

For many of the tasks which a school completes with the processing of data it can be with the legal basis that it is in the public interest or compliance with a legal obligation to which it is subject to. A school has a public interest or in some instances a legal obligation to educate the students in its care. Therefore, it is reasonable to assume that schools operate a library as a tool to assist them in their purpose. On this assumption it is not necessary for schools to gain consent for borrower data to be able to be transferred to the library system.

The customer has entered into a contract with MLS which allows the processing of data for the purposes of providing a Library system.

7. Where the data is stored?

All data held by MLS is within the EEA in a UK Microsoft Azure data centre. All MLS employees are located within the EEA. Therefore, your data will not be transferred outside of the EEA.

8. Security of the data stored

MLS have combined the advantages of CloudFlare and Microsoft Azure to bring a highly available and securely hosted library system to customers.

CloudFlare Security:

- Anycast Network - With 118 data centres across 57 countries and 10 Tbps of capacity, Cloudflare's Anycast network absorbs distributed attack traffic by dispersing it geographically, while keeping Internet properties available and performant
- DNSSEC is the Internet's non-spoofable caller ID. It guarantees a web application's traffic is safely routed to the correct servers so that a site's visitors are not intercepted by a hidden "man-in-the-middle" attacker
- Web Application Firewall (WAF) Cloudflare's enterprise-grade web application firewall (WAF) detects and block common application layer vulnerabilities at the network edge, utilising the OWASP Top 10, application-specific and custom rulesets.
- Rate Limiting protects critical resources by providing fine-grained control to block or qualify visitors with suspicious request rates.
- Transport Security Layer (TLS) encryption enables HTTPS connections between visitors and origin server(s), preventing man-in-the-middle attacks, packet sniffing, the display of web browser trust warnings, and more.
- Cloudflare is an ICANN accredited registrar, protecting organizations from domain hijacking with high-touch, online and offline verification for any changes to a registrar account.
- Cloudflare Orbit solves security-related issues for Internet of Things devices at the network level.

Microsoft data centre physical security:

- Multi Layer physical and logical security
- High Security perimeter fence
- 24/7/365 surveillance
- Vehicle check points
- World-class access control procedures
- Multi-factor biometric entry point
- Full Body metal detection
- On-site hard drive destruction

- State-of-the-art fire suppression systems
- 24/7/365 protection from Microsoft's Cyber defences operations centre
- 300 billion user authentications processed each month
- Transport Layer Security/Secure Sockets Layer (TLS/SSL), which uses symmetric cryptography based on a shared secret to encrypt communications as they travel over the network.
- Internet Protocol Security (IPsec), an industry-standard set of protocols used to provide authentication, integrity, and confidentiality of data at the IP packet level as it's transferred across the network.
- Advanced Encryption Standard(AES)-256, the National Institute of Standards and Technology (NIST) specification for a symmetric key data encryption that was adopted by the US government to replace Data Encryption Standard (DES) and RSA 2048 public key encryption technology.
- Microsoft Azure Storage Service Encryption encrypts data at rest when it's stored in Azure Blob storage.
- Transparent Data Encryption (TDE) encrypts data at rest when it's stored in an Azure SQL database.

9. Where the data is processed

The Library system is hosted on a secure and highly scalable managed service, with the main system hosting provided by Microsoft Azure® UK, which is reliable and resilient. All data is securely stored and processed within the EU and complies with UK data protection standards and requirements.

10. Data Retention

When you are using a library system that is hosted by MLS, we take a lot of care to ensure that your data is looked after and regularly backed up. The backup procedure is configured automatically during your conversion, which means that from the moment you move to a hosted system, your data is being protected and backed up.

A backup of your hosted website is taken every 5 minutes for that last 35 days to allow more accurate restores to take place if you need it. For backups older than 35 days we retain the backup taken at the start of the week up to 1 year ago. These backups are stored at the data centre.

After a year the backups are automatically deleted.

If you wish to terminate your contract with MLS, the valid notice period will need to be completed which is in the terms and conditions along with the completion of MLS Cancellation form. As the Data controller/owner as part of this form MLS will request instruction on provision of your data. You will be will be provide in a universal format file e.g. csv. After 90 days if there has been no response the data will be removed from all our systems including backups. They will then be available for a further 35 days before they are removed from the Azure platform completely.

For a summary of our data retention policy please see below:

- SFTP logins and folders will only be kept active for 30 days.

- Customer data files will be destroyed within 90 days of a Support Incident being closed.
- Customer data files will be destroyed within 180 days of the customer go-live for Data Conversion work. This is to allow for both school holidays and issues where corrections may be required.
- Masked data will be destroyed either within 90 days of any related Support Incident being closed, or at the end of a time period agreed with the customer.
- Information relating to Support Incidents is to be held within CRM for 6 years+ current. This does not include screenshots, or data files.

Similarly to keeping data up to date and accurate, it is the responsibility of the Data Controller to ensure the Data stored within the library system is deleted when it is deemed no longer relevant. The Data Controller will determine the retention period for the recycled borrowers. MLS have provided the tools within the library system to be able to remove borrowers. Once a borrower is removed from the borrowers recycle bin all associated information e.g. loans, reviews, and reservations are also removed.

11. Data Protection/GDPR Awareness

As part of MLS taking Data Protection seriously, we ensure all our staff undertake annual online Data Protection training which includes an assessment which must be passed. Management are under strict instruction for their staff to complete mandatory training which is reported at board level.

12. Staff Vetting

When starting at MLS all staff are vetted to ensure they have a right to work in the UK and criminality checks – Disclosure Scotland Basic and Disclose and Barring Service standard. These are reviewed on a 3 yearly basis

13. Is there any additional Third Party processing of Library data?

MLS use certain subprocessors and content delivery networks to assist in providing the Library management system.

What is a Subprocessor:

A subprocessor is a third party data processor engaged by MLS, who has or potentially will have access to or process library data (which may contain Personal Data). MLS engages different types of subprocessors to perform various functions as explained in the tables below.

Due Diligence:

MLS undertakes to use a commercially reasonable selection process by which it evaluates the security, privacy and confidentiality practices of proposed subprocessors that will or may have access to or process Service Data.

MLS BookShop

MLS work in partnership with Peters to deliver an online bookshop to customers. In order to be able to provide this service customer details are passed to Peters to create a unique bookshop accessible through MyMLS and MLS library products.

Entity Name	Purpose	Entity Country
Peters Ltd.	Peters are the UK's leading supplier of books and furniture for nurseries, schools, academies and public libraries. Their aim is assisting in creating inspiring library spaces for children and young people to have access to great books and an enjoyable place to read them. MLS only provide details of the schools to Peters no borrower data is transferred or accessible from Peters. They do have access to resource information such as those currently in the library system.	United Kingdom

Infrastructure Subprocessors – Service Data Storage

As previously mentioned MLS stores and controls access to the infrastructure within the Microsoft Azure located in the United Kingdom. Microsoft employees do not have access to the library data.

Entity Name	Entity Type	Entity Country
Microsoft Azure	Cloud Service Provider	United Kingdom

Content Delivery Networks

As mentioned above MLS use CloudFlare as content delivery networks ("CDNs") , for security purposes, and to optimize content delivery. CDNs do not have access to library data but are commonly used systems of distributed services that deliver content based on the geographic location of the individual accessing the content and the origin of the content provider. Website content served to website visitors and domain name information may be stored with a CDN to expedite transmission, and information transmitted across a CDN may be accessed by that CDN to enable its functions.

Entity Name	Purpose	Entity Country
Cloudflare, Inc	Cloudflare, Inc. ("Cloudflare") provides content distribution, security and DNS services for web traffic transmitted to and from the library system. This allows MLS to efficiently manage traffic and secure the library system. The primary information Cloudflare has access to, is information in and associated with the library website URL that the End-User is interacting with	United Kingdom

	(which includes End-User IP address). All information (including library data =) contained in web traffic transmitted to and from the library system is transmitted through Cloudflare's systems, but Cloudflare does not have access to this information.	

Optional Subprocessors

MLS vend a number of solutions which customers have the options of purchasing, therefore, these do not apply to all customers:

Entity Name	Purpose	Entity Country
GroupCall - MLS Connect	For automatic transfer of staff and student data from your Management Information System (MIS) to the library system. The software sits within the school network or at the MIS hosted servers to transfer over a secure connection the information to the library system. The mandatory field below are automatically transferred to the library system: ▪ Forename ▪ Surname ▪ Gender ▪ Date of Birth ▪ Tutor group ▪ Year Group ▪ Management System ID The customer does have the facility to transfer optional data: ▪ Address ▪ Phone numbers ▪ Photographs ▪ Email address ▪ UPN ▪ Ethnicity ▪ House ▪ Guardian details including address, phone numbers and email address. GroupCall employees do not have access to the library data. They maybe used to consult on issues relating to support incident on which the customer will be inform this is taking place.	United Kingdom

Overdrive	Ebook Platform provider - allows borrowers to be able to access ebooks from the MLS library system. This software has 2 authentication mechanisms 1. Recommended by MLS - Library Industry standard protocol, SIP2 , is used to communicate with their platform and borrower data is not transferred to Overdrive. Overdrive queries the library system at each stage. Therefore, overdrive do not have access to the library data 2. Library Card Manager is an OverDrive-powered authentication system that allows your library to upload a list of library card numbers. This option will require you to import your borrowers.	United States
BioStore	Biometric identification for staff and students to the library system to allow circulation. Borrower data is imported into locally stored BioStore's database held on a server at the schoo via csv file or GroupCall scheduled task. MLS then use a unique identifier the same in both systems to match the biometric data to the student and find their account in the library system. BioStore employees have no access to the library database unless assisting with support enquiries and authorisation is sort before this commences. • The BioStore database is stored on the organisation's servers, not outside of the network. • BioStore would expect the organisation to apply the same level of physical security to biometric data as they do to other sensitive data held within the organisation. • BioStore would expect an organisation to destroy the records of individuals who have left the organisation. • BioStore uses AES256 encryption – a US Government and worldwide encryption standard. This also applies to communication between different parts of the BioStore system.	United Kingdom

	• Each organisation has a unique key that is used for encrypting the database, so a database cannot be transferred to another system and viewed. For more information see the link: https://biostore.co.uk/technology-security/common-questions/#section4	
Other 3rd Party using SIP2	Customers are able to purchase a license for SIP2 integration which allows their suppliers to interact with the library system on an industry standard protocol. These include security gate providers such as SA Secure, D-tech and PSP and Self-service machine including 3M, D-Tech and others. These companies query the library data each time and do not transfer the data to their services.	