Security & privacy

Connection security

All data sent to or from SETLS is protected by TLS 1.2 or above. This provides the same level of security as online banking, government and other sites.

Authentication & password management

SETLS uses form-based authentication where the password is sent as a POST parameter. The password is transmitted securely using TLS.

Passwords are stored in the database as a salted hash, and cannot be retrieved by the SETLS team. Passwords can be reset by any user with administrative permissions by

- sending a password reset email to the member, or
- manually entering the new password

After checking the password, SETLS creates a cryptographically-secure session cookie. This is used to identify the user when they return to SETLS using the same device, so they do not need to log in again.

A user with administrative permissions can remove a logged-in session, or reset the user's password. Both actions will require the user to enter their password the next time they access SETLS.

Email configuration

SETLS sends emails to members or toy library staff for a variety of reasons, including:

- reminders to return items or attend volunteer sessions
- notifications that a held item is available or membership fees are due

A full list of the automatic emails can be found in the demonstration system.

Emails are sent with a "from" address of noreply@<toylibrary>.setls.com.au. The "reply to" address can be set from the settings page.

Emails from SETLS are sent via Amazon Simple Email Services (SES). You do not need to provide SETLS with access to your mail server or a relay.

Sensitive information

SETLS can be used to record information about members that may be considered sensitive. This information includes:

Member details	*Name*	*Required*
	Email	Optional, required for online access
	Mobile phone	Optional, required for SMS
Home address	Street, suburb and phone	Optional
Alternate contact	Name, address and phone	Optional
Identity	Drivers license number	Optional

The following additional fields can be enabled from the settings page.

Member details	Date of birth Healthcare card (checkbox) Ethnicity Language Disability
Children	Name Date of birth Gender
Organisations (schools)	Name

Additional information related to library operations, such as membership type, are also recorded.

These can be seen in the demonstration system.

Financial transactions

SETLS can be used to manually record member charges and payments, including membership fees and penalties.

SETLS also supports online payment of membership fees using PayPal. This requires creation of a PayPal account.

The SETLS team are currently investigating integration with Square for online and in-person payments.

Data validation

SETLS uses model-driven design and all input fields are:

- Type-checked against the database
- Protected from SQL injection using parameterised queries

Many scenarios for business rule checking are covered by workflow operations rather than manual data entry. For example, when loaning an item, the loan and due dates are derived automatically instead of being entered manually.

Model-driven design allows business rules to be centralised in the model rather than being distributed throughout the user interface. Examples include:

- When changing an item location, only valid destinations are available for selection
- When manually updating a loan record, the return date must be on or before the loan date

SETLS servers

The following service providers are used by SETLS:

Feature	Provider	Location
Web application	Amazon	Sydney, Australia
Database	Amazon	Sydney, Australia
Email	Amazon	Sydney, Australia
SMS	Amazon	Sydney, Australia

The list of IP address ranges currently used by the Amazon is available from AWS IP address ranges - AWS General Reference (amazon.com)

Database encryption

The SETLS database is encrypted using AES-256 with platform-managed keys. All data, logs and backups are encrypted. For more information, see Encrypting Amazon RDS resources.

Revision #13
Created 4 September 2021 01:17:59 by Gavin Morris
Updated 14 June 2025 04:26:31 by Gavin Morris