Loci technical design overview for council IT teams

Loci is partnering with the council to facilitate a secure, scalable, and low-impact civic platform. Councils do not need to provide integration work, project resources, or infrastructure to deploy Loci. The platform operates independently while safely aggregating and presenting relevant public information from council systems to residents through Loci's unified interface.

Our design principles are built around three priorities:

1. Security and trust – all data and infrastructure are handled to enterprise-grade standards.
2. Low operational impact – councils do not need to provision APIs, host data, or manage connections.
3. Scalability and resilience – Loci's architecture supports growth across multiple authorities with no additional burden on council IT teams.

How Loci ingests council information

Loci gathers publicly available information about council services using a combination of:

➔ Direct HTTPS calls to publicly available endpoints
➔ HTML parsing of council webpages
➔ Web crawling via headless browsers where appropriate

We maintain an **eventually consistent** copy of this data in our own data stores, normalised to Loci's standard model. This means that queries via Loci are to our own databases, not to the downstream website (apart from when scraping takes place).

Scraping takes place at a rate that is customisable per authority, typically once a week, but adjustable to any larger or smaller interval as needed.

All scraping mechanisms use an exponential backoff retry policy with added jitter, which prevents the **thundering herd problem** and ensures that Loci does not place undue load on any downstream system.

Infrastructure and security

All data is encrypted both at rest and in transit.

Loci's cloud infrastructure is hosted across multiple AWS availability zones within the UK, providing both resiliency and redundancy.

Our cloud environment operates within a Virtual Private Cloud (VPC), with granular ingress and egress networking policies. All machine-to-machine traffic is entirely within private networking, including the use of VPC endpoints for AWS services, ensuring no routing via the public internet.

All infrastructure follows the principle of least privilege, within a zero-trust configuration, requiring machine-to-machine authentication for all distributed transactions.

Access control and authentication

Both the Loci client application and all available API endpoints implement multiple layers of access control:

➔ Role-based access control (RBAC)
➔ Granular action-based access control (ABAC)
➔ Relationship-based access control (ReBAC)

Data ownership and deletion

Users have the ability to completely delete their account and any and all history of app activity.

Loci may retain anonymised activity records for product analytics or for safety and wellbeing purposes (for example, content moderation), but no personally identifiable data is kept once an account is deleted.

Data ingestion beyond web scraping

In addition to web scraping, Loci supports more robust and resilient data transfer mechanisms. Councils that wish to provide data directly can do so via:

➔ Secure file transfer (SFTP)
➔ Event streaming through supported providers
➔ HTTPS endpoints for webhooks
➔ Direct database connectivity

These options provide flexibility for councils that prefer alternative or supplementary data-sharing methods without requiring any additional integration or maintenance overhead.

Area	Approach
Integration	None required - no APIs, plugins, or internal setup needed
Data Model	Eventually consistent copy of council data, normalised to Loci's model
Scraping Rate	Customisable per authority (typically weekly)
Load Management	Exponential backoff with jitter to prevent thundering herd
Security	End-to-end encryption, zero-trust design, principle of least privilege
Hosting	UK-based AWS infrastructure across multiple availability zones
Networking	Private VPC with restricted ingress/egress and VPC endpoints
Access Control	RBAC, ABAC, and ReBAC
Authentication	Passwordless via Stytch - no passwords stored
User Rights	Full account deletion; only anonymised data retained
Data Ingestion Alternatives	Secure SFTP, event streaming, or webhook endpoints

Let's explore what's right for your council.

hello@lociapp.co.uk | www.lociapp.co.uk

LOCI
the community app