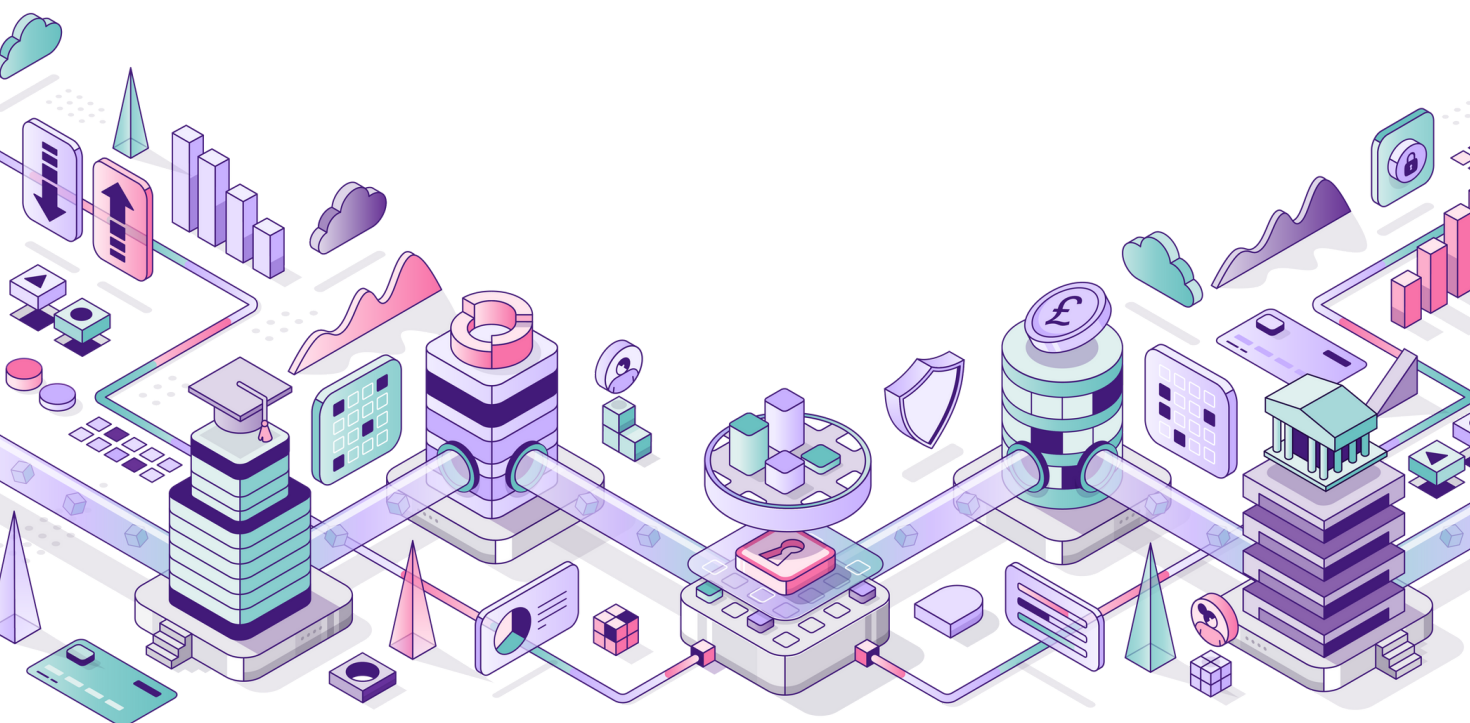


G-Cloud15

Service Definition – Economic Wellbeing Explorer



Service Overview

Service name: Economic Wellbeing Explorer (EWE)

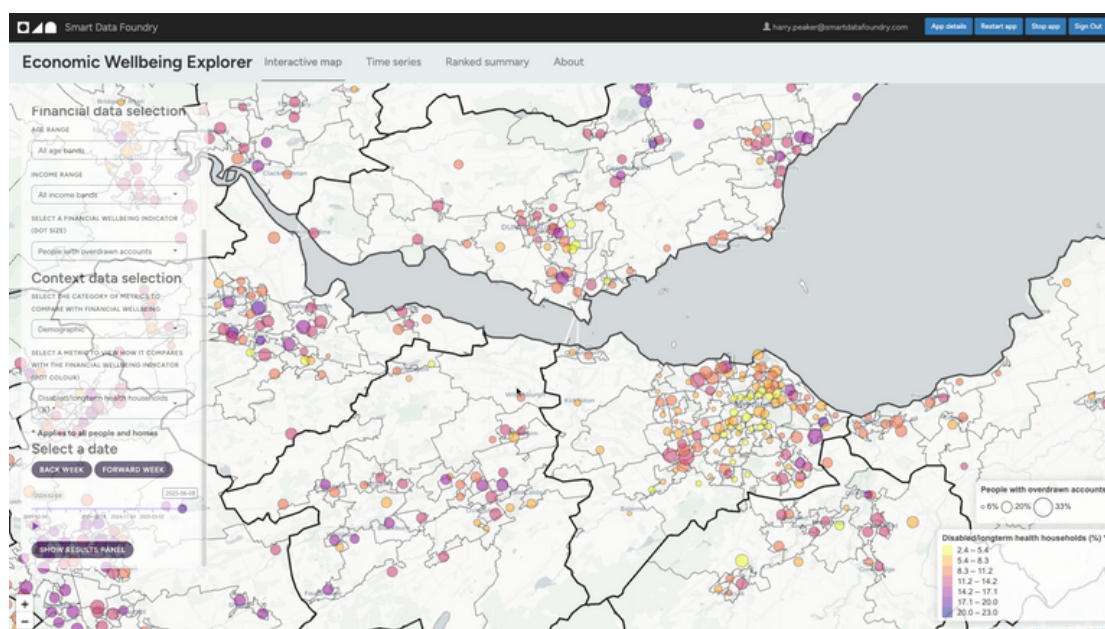
1 Service type: Software as a Service (SaaS) - Service Overview

The Economic Wellbeing Explorer (EWE) is a cloud-based analytical platform designed to support public sector organisations to explore, analyse, and interpret economic wellbeing data. The service brings together curated datasets and analytical tools to support evidence-based policymaking, research, and service design.

EWE enables users to:

- Access and explore economic wellbeing datasets through a secure web interface
- Analyse trends and patterns at different geographic and demographic levels
- Generate insights to inform policy development, evaluation, and strategic planning

The service is accessed via a standard web browser and does not require local installation. A free version is available providing national and regional insights. Localised and contextualised instances are available via subscription.



Screenshot, Economic Wellbeing Explorer

Service Overview

2. Cloud Hosting and Infrastructure

The Economic Wellbeing Explorer is delivered as a Software as a Service (SaaS) solution hosted within the United Kingdom.

Hosting model: Public cloud (Amazon Web Services), supported by a hybrid architecture utilising EPCC (Edinburgh Parallel Computing Centre) for secure data hosting.

Resilience features include:

- Multi-Availability Zone architecture
- Independent power, cooling, and network infrastructure
- Automated backups across geographically isolated zones
- Multi-zone replication to eliminate single points of failure
- Regular disaster recovery testing
- Documented Recovery Time Objectives (RTOs)

Both AWS and EPCC facilities align with recognised standards including ISO 22301 for business continuity.

3. Service Availability and Performance

We work to achieve 99.999% availability, supported by resilient infrastructure and monitored environments.

Availability targets may be defined per customer depending on service configuration. The platform is designed to support elastic demand and scale in response to usage requirements.

Service Overview

4. Backup, Restore, and Disaster Recovery

The service incorporates automated backup processes with encryption at rest.

Data resilience measures include:

- Scheduled automated backups
- Geographic isolation of backup environments
- Regular disaster recovery testing
- Incident response and recovery procedures
- Annual resilience plan reviews

These controls support business continuity and rapid restoration of service in the event of disruption.

5. Onboarding and Offboarding

Onboarding

Users are supported through:

- Online help materials
- Getting started guides
- Instructional videos
- Customer Success Manager support

Contextualised instances of the platform can be configured for customer requirements.

Offboarding

Access is provided via annual subscription.

At contract end:

- User access is revoked if the subscription is not renewed.
- Customer-provided contextual data is deleted from the instance.
- Smart Data Foundry retains ownership of underlying platform data.

6. Service Constraints

Known constraints include:

- VPNs or highly restricted corporate networks may affect performance (for example, slower loading or session timeouts).
- The service is browser-based and requires JavaScript and cookies to be enabled.
- Customisation is limited to contextualised platform instances rather than full platform redesign

Service Overview

7. Technical Requirements

Users require:

- A standard internet connection
- Latest versions of mainstream browsers (Chrome, Edge, Firefox, Safari)
- Minimum recommended screen resolution of 1080p

No software installation or additional licences are required.

The platform is not currently designed for mobile device use.

8. Maintenance and Outage Management

We provide service notifications via:

- Platform dashboards
- API portals
- Email alerts

Maintenance is planned to minimise disruption wherever possible.

9. Support

Support hours:

Monday to Friday, 09:00–17:00 (UK time)

Response times:

Users typically receive a response within 3 hours during standard support hours.
Support is provided via email or online ticketing.

Each customer is allocated a Customer Success Manager.

There are no differentiated support tiers.

Service Overview

10. After-Sales Support

Ongoing support includes:

- Technical assistance
- Platform guidance
- Issue resolution
- Customer success engagement

Online help resources remain available throughout the contract period.

11. Data Import and Export

Supported formats:

- Import: CSV, ODF
- Export: CSV (where required)

12. Access to Data Upon Exit

Customer-owned contextual data remains the property of the customer and is deleted from the platform at contract termination.

Underlying platform data remains the property of Smart Data Foundry.

13. Security

Smart Data Foundry operates a comprehensive corporate policy framework covering:

- Data protection
- Information security
- Records management
- Freedom of information

The organisation complies with:

- ISO/IEC 27001
- UK GDPR
- Data Protection Act 2018
- PECR

Security governance aligns with recognised standards including CSA CCM.

A named board-level individual is responsible for service security.

Service Overview

14. Operational Security

Change Management

Structured lifecycle aligned to ISO 27001 and NCSC guidance, including:

- Risk and impact assessments
- Testing in non-production environments
- Controlled implementation
- Post-change review

Infrastructure is managed using version-controlled repositories and infrastructure-as-code

.

Vulnerability Management

- Automated internal and external scanning
- Annual penetration testing
- Risk-based prioritisation
- Automated patching where feasible

Protective Monitoring

Continuous monitoring is implemented across environments using:

- Centralised logging
- Security alerts
- Anomaly detection

Confirmed incidents trigger formal response procedures including containment, eradication, and recovery.

Incident Management

A formal incident management process is maintained with:

- Defined response targets
- Escalation procedures
- Stakeholder communications
- Root cause reporting
- Post-incident reviews

Service Overview

15. Data Protection

Data in transit: Protected using IPsec or TLS VPN gateways.

Data at rest: Protected through physical access controls and recognised standards.

Data sanitisation: Secure data erasure processes are applied prior to disposal or reuse in line with NIST 800-88 Rev. 2.

16. Datacentre Security

Facilities comply with recognised security standards and include:

- Secure physical access controls
- Environmental protections
- Surveillance systems

Data storage and processing remain within the United Kingdom.

17. Identity and Access Management

Access is controlled via username and password authentication.

Role-based access controls help prevent unauthorised configuration changes.

Access restriction testing is conducted at least annually.

18. Secure Development

Secure software development practices conform to recognised standards (self-assessed) and follow industry best practice.

19. API Access

The service provides API access to underlying data.

- Documentation is available in PDF format.

20. Accessibility

User support accessibility aligns with WCAG 2.2 AAA standards.