



G-Cloud 15

Service	Umbraco CMS & AI Safeguarding
Document	Service Definition

CONTENTS

Service Concept	4
Modern CMS Requirements	4
Emerging Use of AI.....	4
Service Overview	5
Statamic Pro CMS	Error! Bookmark not defined.
AI Governance Framework	5
Section 3 — Technology Architecture	6
Overview.....	Error! Bookmark not defined.
Headless content management	Error! Bookmark not defined.
API-centric architecture	Error! Bookmark not defined.
Multi-site support and digital estate rationalisation.....	Error! Bookmark not defined.
Omnichannel content delivery	Error! Bookmark not defined.
Futureproof	Error! Bookmark not defined.
Facilities for Admin Users	8
Content creation and management	Error! Bookmark not defined.
Publishing workflows and collaboration	Error! Bookmark not defined.
Governance, version control, and auditability	Error! Bookmark not defined.
Media and asset management.....	Error! Bookmark not defined.
Automation and quality guardrails	Error! Bookmark not defined.
Language & Localisation	Error! Bookmark not defined.
Forms and surveys	Error! Bookmark not defined.
Independence from developers.....	Error! Bookmark not defined.
For Public Users	10
Accessibility and inclusive access.....	Error! Bookmark not defined.
Search & Navigation	Error! Bookmark not defined.
Language and communication support.....	Error! Bookmark not defined.
Feedback and interaction	Error! Bookmark not defined.
Use of Third Party Generative AI	Error! Bookmark not defined.
Accessibility	Error! Bookmark not defined.

Integrations	13
API Centric	13
Analytics	14
Security	15
Security by design and reduced attack surface	Error! Bookmark not defined.
Access control.....	Error! Bookmark not defined.
Authentication and multi-factor authentication	Error! Bookmark not defined.
Vulnerability management and patching	Error! Bookmark not defined.
Audit, logging, and traceability	Error! Bookmark not defined.
Data protection and data residency	Error! Bookmark not defined.
Security over the life of the service.....	Error! Bookmark not defined.
AI Governance (AI Guardian).....	17
Scope of AI covered by the governance layer	17
AI objectives and use-case definition	18
Monitoring, bias detection, and performance management	18
Human Escalation.....	19
Periodic review and lifecycle management	19
Hosting & Support.....	19
Hosting options.....	19
Deployment and environment configuration	20
Ember-provided hosting (optional)	20
Support, availability, and service levels	21
<i>Scope of support</i>	22
Offboarding and Service Exit	22
Offboarding process.....	22
Access to data on exit.....	22
Data deletion and disposal	22
Account closure and access revocation.....	23
Feedback and transition support.....	23

SERVICE CONCEPT

MODERN CMS REQUIREMENTS

Public sector organisations rely on digital services as primary channels for providing authoritative information, enabling access to services and meeting statutory obligations for accessibility, inclusion, and transparency. These services must be usable by the widest possible audience, regardless of accessibility needs, language, or digital confidence, and must operate reliably under sustained public scrutiny.

Modern public digital delivery extends beyond a single website where content is expected to be consistent and accessible across multiple channels, including public websites, search, assisted digital services, and emerging interfaces. To achieve this, content must be managed centrally and reused safely and consistently, rather than duplicated across systems or maintained manually.

A modern CMS must therefore support multi-site and multi-channel delivery from a single, authoritative content platform, with structured content models, clear editorial workflows, and appropriate governance controls. This ensures content remains accurate, compliant, and easy to manage over time while supporting evolving user needs and service journeys.

This service provides a modern content management system built on Umbraco which supports accessible, multilingual and user-centred public digital services and enables organisations to manage large and complex content estates efficiently. The CMS is designed for use by non-specialist publishers, while embedding the controls and assurance needed to maintain consistency, quality, and compliance at scale.

EMERGING USE OF AI

The service recognises that many public sector organisations operate in domains where information is complex, evolving and not always well understood by users. This includes organisations with significant public communication responsibilities, such as local authorities, regulators and public bodies supporting people navigating legal, regulatory, or eligibility-based processes. In these contexts, digital services often become the primary route for both information provision and enquiry handling.

AI-assisted capabilities help users locate relevant content, understand guidance and orient themselves within complex subject areas, reducing avoidable one-to-one enquiries while maintaining accuracy, consistency, and trust. This is particularly valuable for organisations balancing high public demand with constrained operational capacity.

The service also recognises that the use of AI in public-facing services introduces material risks if not properly managed. AI is therefore operated within a defined governance and assurance framework, ensuring its use is transparent, auditable, and subject to human oversight. AI functions as an assistive capability within the Umbraco CMS and not as an autonomous decision-maker.

The service is intended for public organisations that need to manage complex public communication at scale, improve access to information across multiple channels and maintain accountability, compliance and public trust.

SERVICE OVERVIEW

This service provides a modern, headless-capable content management system designed to support the delivery of public digital services across multiple channels. Umbraco acts as the main source of public information, enabling organisations to manage content once and deliver it consistently across public websites, search services, assisted digital channels and other connected interfaces. This approach supports clarity, consistency, and trust in public-facing information while reducing duplication and manual content management.

The CMS is designed for multi-site and multi-channel use and supports API-driven content delivery alongside traditional web publishing. This enables organisations to operate multiple public-facing services from a shared content platform, while maintaining clear separation where required. Structured content models support reuse across channels and services, improving accessibility, multilingual delivery and long-term maintainability. The service is intended to support high-volume public communication and complex content estates, rather than isolated or single-channel websites.

UMBRACO CMS

Umbraco is a modern, open-source content management system built on the Microsoft .NET platform that provides a robust and flexible foundation for delivering secure, scalable digital services within public sector environments. Content is stored in a structured and governed repository, supporting complex content relationships, versioning and auditability. This architecture supports reliable publishing workflows and aligns with public sector expectations for assurance, transparency, and operational resilience.

Umbraco combines strong developer extensibility with a user-friendly editorial experience and content is modelled using clearly defined document types and content structures, enabling organisations to reflect user needs, service journeys, and policy requirements accurately. The back-office interface is designed for non-specialist publishers and includes role-based access control, approval workflows, content versioning, media management and preview capabilities to support safe and controlled publishing.

The platform supports both traditional and headless delivery models through APIs, enabling integration with modern front-end frameworks, mobile applications and other downstream services. Multi-site and multilingual capabilities allow multiple websites, services, or language variants to be managed within a single Umbraco installation, while maintaining appropriate governance and separation.

Umbraco's extensible architecture allows organisations to integrate the CMS with existing systems and services, including identity platforms, search services, analytics and accessibility tooling. This flexibility, combined with structured content, editorial governance and API-driven delivery, positions Umbraco as a scalable and future-ready CMS suitable for public digital services that must evolve over time while maintaining consistency, compliance, and public trust.

AI GOVERNANCE FRAMEWORK

Alongside the Umbraco CMS, the service includes an embedded AI governance framework that enables the safe, controlled use of AI-assisted capabilities within the CMS environment. The framework is designed to help organisations realise the operational benefits of AI, such as improved content discoverability, better user orientation within complex information and more efficient editorial workflows, while managing the risks associated with AI use in public-facing digital services.

AI-assisted capabilities are operated within clearly defined boundaries and are subject to transparency, auditability and human oversight. AI is used to support users and publishers not to make autonomous decisions or replace human judgement. The framework is deliberately technology-agnostic and is not tied to a specific AI tool, model, or vendor, allowing organisations to adapt their approach as AI technologies and regulatory expectations evolve.

The governance framework is designed to align with organisational AI policies, security requirements, and assurance practices. It provides a clear operating model, including defined controls, monitoring, and review processes, to ensure AI use remains proportionate, explainable, and appropriate in contexts where accuracy, accountability, and public trust are essential.

Together, the Umbraco CMS and AI governance framework form a single, coherent service. The CMS provides a structured, authoritative platform for managing public information, while the governance framework ensures that any AI-assisted use of that information is managed safely and responsibly. The service operates as a public-facing layer and does not replace transactional, case management, or back-office systems.

SECTION 3 — TECHNOLOGY ARCHITECTURE

The service is built on a modern content management architecture designed to support long-lived, accessible, and multi-channel public digital services. The architecture separates content management from presentation and delivery, allowing organisations to manage public information as a structured and governed asset that can be reused and adapted over time.

This approach supports flexibility, resilience and operational efficiency, while reducing duplication and overhead across complex public-sector digital estates.

HEADLESS CONTENT MANAGEMENT

The service supports a headless and decoupled content management approach using Umbraco, where content is created, governed, and stored independently of how it is presented to users. Content is managed centrally and delivered to websites and other interfaces as required, rather than being tightly coupled to a single front-end implementation.

This allows organisations to redesign websites, introduce new interfaces, or respond to changing user needs without restructuring content models or governance arrangements.

What this means for clients

- Content remains authoritative and reusable across redesigns and service changes
- Presentation changes do not require content migration or re-authoring
- Content is treated as a long-term organisational asset, not tied to a single website

API-CENTRIC ARCHITECTURE

The service is API-centric by design. Content and structured data are exposed through APIs to support delivery across multiple channels and integration with other systems.

This enables Umbraco to operate as part of a wider digital service architecture, rather than as an isolated publishing tool.

What this means for clients

- Clean integration with systems such as search, CRM, payments, and case management
- Services can be composed from multiple platforms without duplicating content
- Reduced lock-in to a single delivery or presentation model

MULTI-SITE SUPPORT AND DIGITAL ESTATE RATIONALISATION

The architecture supports the management of multiple public-facing websites and services from a single Umbraco instance. Sites can share content models, media assets and governance controls while allowing appropriate variation where required.

This supports rationalisation of fragmented digital estates and reduces the cost and complexity of operating multiple CMS platforms.

What this means for clients

- Consistent management of multiple sites from one system
- Uniform governance, accessibility, and security controls
- Reduced operational overhead and platform duplication
- Organisational change without repeated re-platforming

OMNICHANNEL CONTENT DELIVERY

The service supports delivery of public information across multiple digital channels from a single, governed content base. Content can be reused across websites, search interfaces, assisted digital services, and AI-assisted or conversational interfaces without duplication.

This ensures information remains consistent, accurate, and authoritative regardless of how users access it.

What this means for clients

- Users receive consistent information across channels.
- Accessibility and governance standards apply equally across delivery mechanisms.
- New channels can be introduced without restructuring content or compromising control.

FUTURE-PROOF ARCHITECTURE

By separating content, presentation, integration, and delivery concerns, the architecture supports long-term sustainability and incremental improvement. Each layer can evolve independently within defined controls, reducing risk and avoiding tightly coupled systems that are costly to change.

What this means for clients

- Reduced long-term technical debt
- Greater ability to adapt within constrained budgets
- Continuous improvement without disruptive replacement
- Enablement of long-term omni-channel communication strategies

FACILITIES FOR ADMIN USERS

The service provides a comprehensive set of administrative facilities delivered through the Umbraco content management system, designed to support staff responsible for maintaining public-facing digital services who are not specialist web publishers or developers. The administrative interface enables organisations to manage content, structure, and governance independently, without routine reliance on technical support, while maintaining appropriate control, assurance, and auditability.

CONTENT CREATION AND MANAGEMENT

The service supports structured content creation using Umbraco document types, properties, and reusable components. Content is created and managed within clearly defined structures rather than free-form pages, ensuring a clear separation between content and presentation and reducing the risk of layout, accessibility, or design issues.

Content can be drafted, edited, previewed, and updated through Umbraco's back-office interface, which is designed for routine operational use. Changes to text, images, documents, and page structure can be made without modifying code or templates.

What this means for administrative users

- Staff can update pages, guidance, and service information themselves without returning to a developer.
- Subject matter experts can focus on accuracy, clarity, and accessibility rather than technical constraints.
- Routine changes can be made quickly, reducing delays between policy or service change and public communication.
- Confidence in making updates reduces avoidance behaviours and reliance on workarounds such as PDFs or email-based requests.

PUBLISHING WORKFLOWS AND COLLABORATION

The service supports multi-user content workflows using Umbraco's publishing states and permission model. Multiple contributors can draft, review, and approve content before publication, with clear visibility of whether content is in draft, under review, scheduled, or live.

Preview functionality allows users to see how content will appear prior to publication, while role-based permissions ensure that only authorised users can publish content to the live service.

What this means for administrative users

- Content can be prepared collaboratively without confusion over ownership or status.
- Reviews and approvals are handled within the CMS rather than through email or offline processes.
- The risk of accidental or premature publication is reduced.
- Governance processes are followed because they are embedded into everyday workflows rather than imposed externally.

GOVERNANCE, VERSION CONTROL, AND AUDITABILITY

The service maintains a complete version history of content using Umbraco's built-in audit and rollback capabilities where all changes are recorded automatically, including who made the change and when, and previous versions can be viewed and restored where necessary. Publishing activity is logged to support accountability and review.

These controls operate as part of normal system use, without requiring additional administrative effort.

What this means for administrative users

- Mistakes can be corrected quickly without technical escalation.
- Teams can work confidently, knowing changes are reversible.
- Organisations can demonstrate accountability and traceability if content is challenged.
- Governance does not slow down publishing or unnecessarily centralise control.

MEDIA AND ASSET MANAGEMENT

The service includes a central media library within Umbraco for managing images, documents, and other digital assets. Assets can be reused across multiple pages and sections, with metadata such as titles and alternative text managed consistently.

This approach supports accessibility requirements and reduces duplication across the content estate.

What this means for administrative users

- Assets are easier to find, manage and reuse, saving time.
- Accessibility requirements such as alternative text are easier to meet and maintain.
- Teams avoid creating multiple inconsistent versions of the same document or image.
- Overall content quality improves without increasing administrative burden.

AUTOMATION AND QUALITY GUARDRAILS

The service uses structured content models, validation rules, and editorial guidance within Umbraco to provide quality guardrails that support consistency and compliance. This includes structured metadata, required-field validation, and support for search optimisation through controlled content properties.

Automation is used to guide and enforce good practice rather than to make publishing decisions automatically.

What this means for administrative users

- Editors are supported to publish well-structured, accessible, and findable content without specialist knowledge.
- Common errors are prevented before publication.
- Quality standards are maintained even when publishing responsibility is decentralised.
- Less time is spent checking compliance, allowing more focus on improving content.

LANGUAGE AND LOCALISATION

The service supports multilingual content management using Umbraco's language and content variant features. Relationships between source and translated content are maintained within the CMS, allowing language versions to be governed independently while remaining aligned.

Responsibilities for translation, review, and publication can be assigned clearly within the system.

What this means for administrative users

- Statutory language obligations can be met within a single system.
- Translated content does not drift or become outdated unnoticed.
- Language responsibilities are clear and manageable.
- Multilingual publishing does not require separate sites or duplicated processes.

FORMS AND SURVEYS

The service supports the creation and management of forms for collecting structured information from public users using Umbraco Forms and, where appropriate, integrations with third-party form or survey platforms. Forms can be configured and managed by administrative users, including validation, structured data capture, and routing of submissions to downstream systems.

Where organisations prefer to use external form or survey tools, these can be integrated while maintaining a consistent public-facing experience.

What this means for administrative users

- Forms can be created and updated internally without relying on developers for routine changes.
- Different approaches to data capture can be supported within the same service.
- Existing investments in external form or survey tools can be retained.
- Governance and control over how data is collected and routed are maintained.

Independence from Developers

The service is designed so that the majority of day-to-day content management and publishing activity can be carried out by internal teams using Umbraco's administrative tools. Developer involvement is typically limited to substantial structural changes, new integrations, or template-level enhancements.

What this means for administrative users

- Organisations retain direct control over their own content.
- Ongoing costs are reduced by limiting developer involvement to genuinely technical work.
- Publishing teams can respond quickly to change.
- Digital services remain sustainable over time without continual external dependency.

FOR PUBLIC USERS

The service provides facilities that support members of the public in accessing information and engaging with public services through digital channels delivered using the Umbraco content management system. These facilities are designed to ensure that public information is accessible,

understandable, and easy to find for users with a wide range of needs, abilities, devices, and levels of digital confidence.

ACCESSIBILITY AND INCLUSIVE ACCESS

The service is designed to support accessible public access by default. Content is delivered through structured templates and components implemented within Umbraco, supporting compliance with recognised accessibility standards and ensuring that users can access information regardless of disability, assistive technology or interaction method.

Accessibility is treated as a foundational requirement rather than a retrofit. Content models, templates, and front-end implementations are designed to ensure that accessibility is applied consistently across pages, services, and channels as content evolves over time.

What this means for public users

- Information can be accessed using assistive technologies such as screen readers, keyboard navigation, and voice input.
- Content remains accessible as it is updated, expanded, or reused across the service.
- Users are not excluded due to design, layout, or content structure choices.

SEARCH AND NAVIGATION

The service supports multiple ways for public users to find information, recognising that users do not typically understand internal organisational structures or service boundaries. Content is structured within Umbraco to support clear navigation, consistent page presentation, and effective on-site search.

The service can include enhanced search capabilities, such as integration with AI-assisted search technologies (for example Algolia or Typesense), enabling users to locate relevant information using natural language queries rather than exact terminology.

What this means for public users

- Users can locate information without needing to understand how services are organised internally.
- Relevant content can be surfaced even when users are unsure what terms to search for.
- The effort required to find accurate, authoritative information is reduced.

Note: Specific AI-assisted search approaches are defined as part of service configuration.

LANGUAGE AND COMMUNICATION SUPPORT

The service supports the delivery of public information in multiple languages and formats using Umbraco's language and content variant capabilities. This enables organisations to meet statutory language obligations and communicate effectively with diverse audiences.

Content can be managed in multiple languages while remaining linked to source content, reducing the risk of inconsistency, drift or outdated translations.

What this means for public users

- Information is available in appropriate and supported languages.

- Translated content remains consistent, aligned, and reliable.
- Users are less reliant on informal or third-party interpretations of public information.

FEEDBACK AND INTERACTION

The service supports the collection of feedback and structured input from public users through forms, feedback components, and integrated interaction mechanisms managed within Umbraco.

Feedback mechanisms can be embedded directly into digital services, allowing users to provide input without being forced into complex contact journeys or escalation routes.

What this means for public users

- Feedback can be provided quickly and easily.
- Issues with clarity, accuracy, or usability can be identified and addressed over time.
- Interaction supports service improvement without unnecessary friction or effort.

USE OF THIRD-PARTY GENERATIVE AI

The service supports the controlled use of third-party generative AI tools to provide AI-assisted public user interfaces, such as conversational chat interfaces and AI-supported search and navigation.

These interfaces operate over content managed within Umbraco and are constrained to approved purposes and datasets. AI tools are configured to respond only using information that the organisation has chosen to make publicly available through the website or digital service.

The use of generative AI is governed through an embedded AI governance framework that defines:

- the approved use case
- identified risks and mitigations
- algorithmic registrations
- the scope of permitted AI use
- the content and data sources AI tools may access
- thresholds for human escalation or intervention
- logging and audit of AI interactions

AI interfaces are not autonomous decision-making systems. They are used to support information access and guidance only and do not replace statutory processes, formal advice, or human judgement.

What this means for public users

- Users can access information through conversational or assisted interfaces when appropriate.
- AI responses are constrained to authoritative, approved public content.
- The risk of misleading, biased, or inappropriate responses is actively managed.
- Human support remains available where escalation or clarification is required.

ACCESSIBILITY (WCAG COMPLIANCE AND ASSURANCE)

The service supports the delivery of accessible public digital services that meet Web Content Accessibility Guidelines (WCAG) requirements. Accessibility is addressed through Umbraco

configuration, structured content design, publishing workflows, and front-end implementation practices.

The CMS supports the creation of standards-based content that can be rendered accessibly across devices and assistive technologies. Content models and publishing workflows encourage consistent use of headings, labels, alternative text, and semantic structure, reducing reliance on individual authors to manage accessibility manually.

Accessibility considerations are embedded into preview and review stages, enabling issues to be identified before content is published.

Subject to client approval, the service can also include deployment of an accessibility support overlay such as accessiBe. This is offered as a supplementary enhancement to improve usability for some users, not as a replacement for WCAG-compliant design and content.

The service does not assume that accessibility can be solved through tooling alone and supports compliance through a combination of platform capability, implementation approach, and organisational governance.

What this means for public users

- Information and services can be accessed in ways that suit individual needs, devices, and assistive technologies.
- Consistent content structures help users navigate and understand information more easily.
- Assistive technologies work more effectively due to semantic and standards-based implementation.
- Where an accessibility overlay is deployed, additional controls such as text resizing, contrast adjustment, and navigation aids may be available.

This approach supports inclusive and equitable access to public information and services, helping organisations meet statutory accessibility obligations while improving the overall experience for a wide and diverse public audience. Safeguards ensure that accessibility enhancements complement, rather than obscure, underlying compliance with recognised accessibility standards.

INTEGRATIONS

API CENTRIC

The service is designed to integrate with existing organisational systems and external services through an API-centric architecture, with Umbraco operating as the public-facing content and interaction layer. Core operational systems remain authoritative for transactions, case management, and data processing.

Umbraco exposes structured content, metadata, and user interactions through RESTful APIs and event-driven integration mechanisms. This enables the CMS to connect to a wide range of internal and third-party systems without duplicating data or replicating specialist functionality. Public-facing journeys are delivered through the CMS, while operational processing and data ownership remain with downstream platforms.

Typical integration scenarios include:

- **Payment services**, where transactional processing is handled by an external payment service provider and the CMS provides the public interface and supporting content.
- **Customer relationship management (CRM) systems**, including commercial and public-sector platforms, where user interactions, enquiries, or submissions are routed for follow-up or processing.
- **Case management systems**, where the CMS supports information capture and user guidance, and cases are created, updated, or progressed in downstream systems.
- **Email, notification, and communications services**, enabling confirmations, updates, and alerts to be sent as part of digital service journeys.
- **Form and survey platforms**, where organisations choose to use established external tools for surveys or specialist data capture, while maintaining a consistent public-facing experience through the CMS.
- **Business reporting and analytics tools**, allowing insight to be drawn from content usage, user interactions, and service performance.
- **Third-party systems and services that expose APIs**, allowing integrations to be tailored to specific organisational needs.

The service does not seek to replace specialist platforms such as CRMs, case management systems, payment engines, or survey tools. Instead, it provides a structured and governed interface through which public users interact with services, while operational processing and system authority remain with existing platforms.

Integration approaches are designed to be flexible and adaptable, allowing organisations to connect Umbraco to their current technology estate and to accommodate change over time as systems evolve.

ANALYTICS

The service supports the collection and exposure of usage and interaction data generated through Umbraco and any integrated AI-assisted components. This includes data relating to content usage, navigation behaviour, form submissions, search activity, and AI-assisted interactions such as conversational queries and escalation events.

Rather than providing a proprietary analytics solution, the service integrates with external analytics and business intelligence platforms through APIs and standard tracking approaches. This enables organisations to use existing analytics tools and reporting environments aligned with internal governance, data protection policies, and reporting standards.

The service can be connected to commonly used analytics and BI platforms such as Google Analytics, Firebase, Looker, and equivalent tools. The specific integration approach and configuration are defined by organisational requirements and existing analytics environments.

Analytics tooling, dashboards, and interpretation of data are provided through external platforms or complementary services rather than being embedded directly within the CMS, allowing analytics capability to evolve independently of content management and service delivery.

SECURITY

The service is designed to meet public sector security expectations through a combination of architectural choices, operational controls, and ongoing management, with Umbraco used as the content management platform. Security is treated as an outcome of how the service is designed, configured, and operated over time, rather than as a one-off configuration or compliance exercise.

The approach focuses on reducing exposure, limiting unnecessary complexity, and ensuring that security controls remain effective throughout the life of the service.

SECURITY BY DESIGN AND REDUCED ATTACK SURFACE

The service uses Umbraco's modular architecture and controlled extension model to minimise unnecessary system components. Functionality is delivered through configuration and bespoke development where required, rather than reliance on large, unmanaged plugin ecosystems.

Compared to plugin-heavy CMS platforms, this approach reduces the number of third-party components that must be assessed, patched, and monitored. This lowers the overall attack surface and reduces exposure to vulnerabilities introduced through external extensions.

What this means for clients

- Reduced security risk associated with unmanaged or outdated plugins.
- Fewer external dependencies requiring ongoing security assessment.
- A more predictable and controllable security posture over the life of the service.

ACCESS CONTROL

Access to the service is governed through Umbraco's role-based access control, aligned to the principle of least privilege. Roles can be configured to separate responsibilities such as content creation, review, approval, and administration. Administrative access is restricted to authorised users and aligned to defined responsibilities.

Permissions are applied consistently across content, media, and administrative functions.

What this means for clients

- Clear separation between editorial, approval, and administrative functions.
- Reduced risk of accidental or unauthorised changes.
- Easier demonstration of governance, accountability, and compliance.

AUTHENTICATION AND MULTI-FACTOR AUTHENTICATION

Administrative access to the service is protected using secure authentication mechanisms, including support for multi-factor authentication. Where required, Umbraco can be integrated with organisational identity and access management solutions, such as single sign-on or directory-based authentication, to align with enterprise security policies.

What this means for clients

- Reduced risk of credential compromise.

- Alignment with common public sector security baselines.
- Consistent access controls across internal systems.

VULNERABILITY MANAGEMENT AND PATCHING

The service is operated under a proactive vulnerability management regime. This includes regular monitoring, vulnerability scanning, and timely application of security updates to the Umbraco platform and supporting infrastructure.

Umbraco's release and update model supports controlled patching and predictable upgrades without reliance on large numbers of third-party components, reducing operational risk during updates.

What this means for clients

- Known vulnerabilities are identified and addressed in a timely manner.
- Security maintenance does not rely on ad-hoc or manual intervention.
- Operational burden associated with security management is reduced.

AUDIT, LOGGING, AND TRACEABILITY

Access to the service and changes made within Umbraco are logged to support auditability and operational oversight. This includes visibility of user access, content changes, and publishing activity. Logs support incident investigation, assurance activity, and compliance review where required.

Audit and traceability mechanisms are embedded into normal system operation.

What this means for clients

- Clear evidence is available to support investigations or assurance requests.
- Accountability for changes is maintained.
- Security controls can be demonstrated, not just asserted.

DATA PROTECTION AND DATA RESIDENCY

Service data is hosted in line with client requirements and applicable data protection legislation, with data residency typically within the UK or EEA. Data is protected using industry-standard encryption for data at rest and in transit.

Client data remains under client ownership, with secure processes in place for data access, extraction, and deletion on service exit, supporting compliance with data protection and retention obligations.

What this means for clients

- Alignment with statutory data protection requirements.
- Clarity over where data is stored and how it is protected.
- Confidence that data can be securely recovered or removed when required.

SECURITY OVER THE LIFE OF THE SERVICE

The security model is designed to remain effective over multi-year contracts without increasing operational complexity. Security controls are embedded into standard operational practices rather than relying on exceptional processes or specialist intervention.

This supports long-term sustainability and consistent compliance as the service evolves and changes over time.

What this means for clients

- Security posture does not degrade as the service grows or evolves.
- Governance effort remains proportionate and manageable.
- Security remains effective within normal operational capacity.

AI GOVERNANCE (AI GUARDIAN)

The service includes an embedded AI governance layer that supports the safe, controlled, and accountable use of AI-assisted capabilities within public digital services. This governance layer applies consistently across all AI components used within the CMS, including public-facing AI, internal AI tools, and AI services provided by third parties.

AI governance within the service is designed to be operational and repeatable. It provides the structures, controls, and processes required to manage AI use over its full lifecycle, from initial proposal through deployment, monitoring, and ongoing review.

SCOPE OF AI COVERED BY THE GOVERNANCE LAYER

The AI governance layer applies to all AI-assisted capabilities operating within the service, regardless of whether those capabilities are public-facing, internal, or provided by third-party AI services.

Where third-party generative AI models are used, they operate within an Ember-designed retrieval and control component (the Ember RAG module). This component forms part of the governance layer and is responsible for constraining, supervising, and evidencing AI behaviour within the CMS environment.

The Ember RAG module is configured per use case and performs three core governance functions:

First, it constrains AI operation to approved purposes and content. The module restricts the information and context available to the AI, ensuring that outputs are grounded only in authorised content and that AI behaviour remains within the defined scope of the service. This prevents AI from operating beyond its intended use or accessing unapproved data sources.

Second, it governs interaction thresholds and human escalation. The module defines conditions under which AI-assisted interactions must be escalated for human review or intervention. These thresholds are configured to reflect the sensitivity, complexity, or uncertainty of a given use case and ensure that AI does not operate beyond agreed limits of autonomy.

Third, it records and evidences AI activity. The module maintains records of AI interactions and outcomes, providing a basis for audit, assurance, and post hoc review. This supports governance, monitoring, and continuous improvement of AI-assisted capabilities over time.

The same governance layer also applies to internal AI-assisted functions used to support content management activities, such as summarisation, translation, tagging, or quality checks. These internal

capabilities are subject to the same constraints, oversight, and evidence requirements as public-facing AI use.

By applying a single governance layer across all AI components, the service ensures that AI-assisted behaviour is controlled, reviewable, and accountable, regardless of where or how AI is used within the CMS.

AI OBJECTIVES AND USE-CASE DEFINITION

Before any AI-assisted capability is deployed within the service, the governance layer supports a structured process to define and approve the intended use of AI. This ensures that AI is introduced deliberately, with clear purpose, defined boundaries, and understood risks.

The service supports early-stage consideration of AI objectives, including the problem AI is intended to address, the benefits it is expected to deliver, and the context in which it will operate. As part of this stage, proposed AI use is reviewed against the organisation's AI policy and governance principles, ensuring alignment with agreed expectations and constraints.

Following this, the service supports evaluation of how AI will be applied within the CMS environment. This includes consideration of appropriate AI components, how they will be constrained and governed, and how they will interact with content, users, and existing systems. Decisions made at this stage define the permitted scope of AI operation.

Where required, the service supports the completion of AI-specific impact assessment activity, distinct from data protection impact assessments. This allows organisations to consider potential impacts on users, fairness, transparency, and public trust, and to identify risks that must be mitigated before deployment.

Outcomes from this stage inform the configuration of the AI governance layer, including:

- approved AI use cases and exclusions
- conditions under which human review or escalation is required
- expectations for monitoring, bias detection, and performance evaluation
- review points to reassess effectiveness, risk, and continued appropriateness over time

Records of decisions and assessments are maintained to support audit, assurance, and accountability.

MONITORING, BIAS DETECTION, AND PERFORMANCE MANAGEMENT

Once AI-assisted capabilities are live, the service supports ongoing monitoring and management to ensure that AI behaviour remains aligned with approved objectives, constraints, and governance expectations.

Monitoring is treated as a routine operational activity rather than a one-off assurance exercise. The service supports continuous visibility of AI behaviour to enable early identification of issues and informed decision-making.

The service provides mechanisms to observe and review AI performance, including patterns of use, accuracy indicators, escalation frequency, and user feedback. This allows organisations to understand how AI is being used in practice and whether it is operating within agreed parameters.

Bias and inclusivity management are supported through structured testing and review. The service supports repeatable bias testing approaches that assess AI outputs across a range of representative user contexts. Results are reviewed to identify disparities in tone, accuracy, or completeness, and to inform corrective action where required.

HUMAN ESCALATION

Human escalation and fallback behaviour are monitored as part of normal operation. Escalation events are recorded and reviewed to confirm that thresholds are functioning as intended and that sensitive or high-risk interactions are appropriately redirected to human support.

The service maintains structured records of AI interactions, escalations, and feedback to support audit, assurance, and retrospective review. These records provide evidence of how AI has behaved over time and support accountability and transparency.

Performance management activity informs ongoing refinement of AI configuration, content, and governance controls. Where monitoring identifies issues or emerging risks, AI behaviour can be adjusted, constrained, or suspended in a controlled manner.

PERIODIC REVIEW AND LIFECYCLE MANAGEMENT

The service supports formal, periodic review of AI-assisted capabilities as part of ongoing performance management. These reviews are intended to assess whether AI use remains appropriate, effective, and aligned with the objectives agreed at the point of approval.

Reviews are typically conducted on a quarterly basis and consider AI performance against the original objectives defined during the AI objectives and use-case definition stage. This includes assessment of whether AI capabilities are delivering the intended benefits, operating within agreed constraints, and continuing to justify their use in the given context.

Periodic review activity considers:

- performance against agreed objectives and success criteria
- findings from monitoring, bias detection, and escalation activity
- identified deficiencies or unintended effects
- opportunities to improve effectiveness, usability, or control
- continued alignment with organisational AI policy and governance expectations, including where policies have evolved since initial deployment

Reviews may result in decisions to maintain the current AI configuration, to modify or enhance AI-assisted capabilities, to impose additional constraints, or to suspend or withdraw AI use where it is no longer appropriate.

The service supports recording outcomes of periodic reviews to provide an auditable record of decisions and to inform future governance activity. This ensures that AI use remains subject to active oversight and does not persist by default once deployed.

HOSTING & SUPPORT

HOSTING OPTIONS

The CMS and AI governance components are hosting-agnostic by design and can be deployed within any suitable modern hosting environment. This includes client-managed infrastructure, third-party managed platforms, or public cloud environments specified by the client. The service does not require a proprietary hosting model and does not impose dependency on Ember-provided infrastructure.

This allows organisations to align hosting arrangements with their own technical standards, security requirements, and procurement preferences.

DEPLOYMENT AND ENVIRONMENT CONFIGURATION

To make the service operational, the CMS and AI governance components must be deployed and configured within a hosting environment. The service includes technical deployment and configuration capability to support installation into a client-specified environment.

Deployment activities are limited to the technical configuration required to operate the service and may include:

- installation of the CMS and AI governance components
- configuration of production and non-production environments
- security and access configuration
- configuration of integrations required for core operation

Deployment does not include delivery of a wider digital project, service design, bespoke development, or content production. Any such activities are outside the scope of this service unless separately procured.

EMBER-PROVIDED HOSTING (OPTIONAL)

Where clients require hosting to be provided as part of the service, Ember offers managed cloud hosting using **Amazon Web Services (AWS)**. Ember-provided hosting is suitable for public digital services at local, regional, and national levels.

Hosting environment

- Deployed within AWS, selected for scalability, reliability, and suitability for public sector workloads
- Configured to support secure operation, resilience, and high availability
- Supports production and non-production environments as required

Data location and residency

- Service data is hosted in AWS data centres located in the UK and/or EEA, as agreed with the client
- Data residency requirements are confirmed during onboarding and reflected in deployment configuration
- All data storage, processing, and backups are managed within the hosting environment

Security and information assurance

Ember-provided hosting operates within an Information Security Management System (ISMS) certified to:

- ISO/IEC 27001
- Cyber Essentials Plus
- NCSC Cloud Security Principles

Security controls include:

- encryption of data at rest and in transit
- role-based access control aligned to least-privilege principles
- multi-factor authentication for administrative access
- segregation of client environments and data
- comprehensive logging and monitoring to support auditability

Resilience, backup, and recovery

- Hosting environments are designed with redundancy and monitoring to support service availability
- Automated backups are performed in line with Ember's business continuity policies
- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are defined to minimise disruption and data loss

Vulnerability management

- Regular internal and external vulnerability scanning, including independent third-party testing
- Identified vulnerabilities are assessed, prioritised, and remediated in accordance with Ember's security policies

SUPPORT, AVAILABILITY, AND SERVICE LEVELS

The service includes support for the CMS and AI governance components, covering incident management, fault resolution, and assistance with operation of the service within the agreed scope.

Service availability

- The service is designed to operate at **99%+ availability**
- A **minimum availability commitment of 99%** is provided as standard where Ember provides hosting

Support hours and access

- Support is provided via Ember's service desk during standard business hours, Monday to Friday
- Support requests can be logged 24/7 via email or a support portal and are triaged by priority

Incident response targets

Support requests are prioritised based on impact and urgency, with the following standard response and resolution targets:

- Priority 1 — Critical impact
Response within 1 business hour; resolution targeted within 3 business hours

- Priority 2 — Significant impact
Response within 4 business hours; resolution targeted within 1 business day
- Priority 3 — Minimal impact
Response within 1 business day; resolution targeted within 4 business days

SCOPE OF SUPPORT

Support applies whether the service is hosted by Ember or deployed into a client-specified environment and covers the CMS and AI governance components only. Support does not include bespoke development, content creation, or delivery of wider digital services unless separately procured.

OFFBOARDING AND SERVICE EXIT

OFFBOARDING PROCESS

Offboarding is initiated following formal notification from the client of their intention to terminate the service. Ember confirms the offboarding plan with the client and coordinates activities to ensure an orderly and secure transition.

The offboarding process includes:

- agreement of timescales and responsibilities
- support for data extraction and transfer
- secure decommissioning of the client's service instance (where hosted by Ember)
- contract and account closure

Where required, Ember provides reasonable assistance to support the client's transition to alternative arrangements.

ACCESS TO DATA ON EXIT

Clients retain access to their service data for the duration of the contract and during the agreed offboarding period.

Ember supports the extraction of client data in standard, machine-readable formats (such as CSV or JSON), covering data generated through use of the service, including:

- website content and media
- configuration data
- AI governance logs and audit records (where applicable)

Guidance and support are provided to ensure data can be accessed and transferred in a usable form.

DATA DELETION AND DISPOSAL

Following confirmation that data extraction has been completed, Ember securely deletes remaining client data from the service in accordance with:

- ISO/IEC 27001-aligned data sanitisation procedures
- applicable data protection legislation

No client data is retained beyond the agreed retention period following service termination.

ACCOUNT CLOSURE AND ACCESS REVOCATION

As part of offboarding:

- access to the service and associated systems is revoked
- administrative credentials are disabled
- any remaining service accounts are closed

Where any credentials or assets have been provided as part of the service, Ember coordinates their secure return or disposal as appropriate.

FEEDBACK AND TRANSITION SUPPORT

As part of offboarding, Ember may request feedback on service delivery and the offboarding process to support continuous improvement. Additional transition support may be provided where agreed.