

How are rights, privacy, Authority and remedy protected?

Trust, Security, Jurisdiction and Data Governance



Simon Owen | Empower Your World | v2.0 FINAL

Start here

Trust is not the absence of visible failure. It is the presence of conditions that make legitimate participation, challenge, intervention, correction and exit possible before scale raises the stakes.

WP06.2 is the trust constitution. Its principles are architectural safeguards rather than slogans. The orientation layer explains the consequence each principle is designed to prevent; the canonical architecture remains the controlled constitutional statement.

Hold these ideas first

- Context governs use, not recognised identity alone.
- Purpose and Authority are required before consequential access or Action.
- Delegation remains bounded, supervised and revocable.
- Challenge, remedy and recovery exist before scale.

A worked route through the architecture

Trace one person across personal Community participation, an employer-sponsored Journey and an Agent-supported opportunity. Ask which information may move, what must remain separate, who has Authority, how challenge works and what recovery requires if a boundary is breached.

How to read this paper

- ORIENT: understand the question and architectural position.
- UNDERSTAND: use examples, distinctions and failure modes to see why the architecture exists.
- EXPLORE: inspect the canonical structures, relationships, states, controls and lifecycle.
- REFERENCE: use definitions, invariants, provenance and validation material for precision.

Status note. The canonical architecture remains authoritative. These pages add orientation and explanation without silently replacing controlled definitions or decisions.

WP06.2

Trust, Security, Jurisdiction and Data Governance

The trust constitution for a Frontier Capability Organisation

CANONICAL POSITION

Trust is a structural property of Capability Infrastructure. The constitution enables Capability formation and mobilisation while preserving autonomy, accountability, fairness, challenge, remedy, security, privacy and Renewal.

v2.0 frozen canonical architecture
Simon Owen | 21 September 2026
Internal strategic architecture

Attribute	Value
Document	WP06.2 Trust, Security, Jurisdiction and Data Governance
Version	v2.0
Status	Frozen canonical architecture baseline - full-depth Research Foundation integration
Owner	Simon Owen
Series position	WP06.2 of WP06.0-WP06.12
Purpose	The trust constitution for a Frontier Capability Organisation
Formatting	FS-017 applied; visible labelled headers; 10 pt minimum body and table text
Baseline date	21 September 2026
Supersedes	v1.0 frozen baseline and v1.1 integration candidate
Change control	Future changes require practitioner validation, implementation Evidence, a downstream proof obligation or a material contradiction.
Canonical rebuild	Full-depth integration of the v1.0 frozen baseline, RS05-derived v1.1 material and cross-suite semantic ownership. New concepts are integrated within the relevant architecture sections rather than retained as addenda.
Freeze decision	WP06 v2.0 Canonical Architecture Validation Review passed Phases A-F; frozen on 21 September 2026.

Executive summary

This constitution governs Participation Contexts, Authority, purpose, permission, Evidence, intelligence, Decision, Agent Action, publication, remedy, recovery and Renewal. It provides architecture, not legal advice or certification.

CONSTITUTIONAL PURPOSE

Enable people, organisations and ecosystems to build, mobilise and renew Capability while preserving autonomy, accountability, fairness, challenge, remedy and shared Value.

1. Constitutional hierarchy

Layer	Rule
Constitutional principle	Defines the character of the system and survives implementation choices.
Architectural invariant	Must hold in every relevant implementation and Domain Pack.
Control objective	Required trust outcome mapped to preventive, detective and corrective controls.
Control pattern	Preferred implementation approach, adaptable by technology and jurisdiction.
Prohibited use	Structurally resisted, blocked, audited and escalated.
Specialist review gate	Requires legal, privacy, security, employment, AI, ethics or safeguarding expertise.

2. Core trust principles

Principle	Required behaviour
Human Agency first	Meaningful choice, notice, voice, challenge, intervention and exit.
Context before identity	Participation Context, not recognised identity alone, governs access and use.
Purpose before access	Role, relationship or payment is insufficient without permitted purpose.

Principle	Required behaviour
Authority before Action	Capability, advice and technical ability do not create Authority.
Delegation before automation	Human and Agent delegation is explicit, bounded, supervised and revocable.
Participation before legitimacy	Affected and burdened parties receive proportionate voice and review rights.
Evidence before Claims	Activity, repetition, sponsorship and participation do not substitute for Evidence.
Independence before confidence	Source derivation, incentives, conflicts and corroboration are visible.
Override before autonomy	Consequential automation has intervention and stop rights.
Remedy before scale	Correction, appeal, restriction, withdrawal and recovery exist before expansion.
Trust before scale	Growth never justifies surveillance, hidden joins or weakened boundaries.
Renewal before extraction	Immediate Value cannot consume future Capability or ecosystem viability.

3. Participation Context and privacy

A person may participate personally, organisationally, professionally, through a cohort, in research or in a demonstration. Recognition of the same identity does not justify joining these contexts. Context carries purpose, controller or steward, permissions, visibility, contactability, retention, Evidence portability, Agent access and remedy.

- Employer onboarding does not discover or merge personal participation.
- Personal Ambition and Development Intent never feed workforce planning without explicit permitted route.
- Evidence crosses contexts only with purpose, provenance, recipient context and revocation.
- Search, facets, counts, notifications, support tooling and Agent inference cannot reconstruct prohibited information.
- People may use different identities, visibility and contact preferences in different contexts.

4. Workforce and non-surveillance protections

- Participation, absence, challenge or help-seeking are not performance, loyalty or culture-fit signals.
- Capability Evidence does not silently become employability, redundancy or disciplinary scoring.

- Community participation does not justify cross-Domain or cross-context profiling.
- Absence of public Contribution is not negative Evidence.
- Aggregate insight requires purpose, minimum-group and re-identification protection.
- The platform must resist function creep from developmental support into hidden evaluation.

5. Intelligence and judgement governance

Control	Requirement
Question legitimacy	QuestionFrames state purpose, scope, affected parties, assumptions and Decision use.
Source independence	Multiple references to one origin are not independent corroboration.
Motivation transparency	Material commercial, sponsor, authorship and institutional interests are recorded.
Disconfirmation rights	Contrary Evidence and alternative explanations can be introduced and retained.
Confidence calibration	Reliance is explainable, contextual, reviewable and proportionate.
Narrative governance	Evidence, alternatives, omissions, uncertainty and authorship remain visible.
Decision legitimacy	Authority is necessary but not sufficient; participation and appeal scale with consequence.
Intelligence remedy	Flawed Signals, Claims, narratives or Decisions can be corrected, suspended or reopened.
Observatory independence	Evidence standards and publication review resist commercial pressure.

6. Human-Agent governance

- Every Agent has stable identity, accountable owner, declared function, evidenced Capability and lifecycle state.
- DelegationGrant records purpose, Action, data, tools, Decision scope, cost, context, time, supervision and revocation.
- Agent recommendations do not become Decisions without explicit authorised policy.
- Agent-to-Agent hand-offs preserve original Authority, lineage and restrictions.
- Human takeover, emergency stop, publication hold and Claim suspension are visible and testable.
- Agent-supported intelligence retains source links, material transformations, model identity, limitations and human review.

7. Security architecture obligations

Concern	Constitutional outcome
Identity and access	Right actor has minimum appropriate access for permitted purpose.
Data security	Data classified, protected, retained and transferred according to context and jurisdiction.
Agent and tool access	Delegation cannot widen privilege, purpose or data use.
Supply chain	Providers, models, components and changes remain visible and reviewable.
Logging and monitoring	Consequential activity is traceable without disproportionate surveillance.
Incident and recovery	Containment, correction, communication, fallback and remedy are testable.
Availability and continuity	Critical participation and Evidence remain recoverable through failure or exit.

8. Jurisdiction and sovereignty

Jurisdiction is not only storage location. It includes controller and processor roles, market and feature availability, identity provider, model routing, support access, legal transfer mechanism, sector restrictions, retention and rights enforcement. Data sovereignty and operational sovereignty are distinct.

Sovereignty concern	Question
Data	Where is data stored, processed, backed up and accessed?
Identity	Who controls identity, authentication and account recovery?
Model	Which provider, location and service conditions affect inference?
Operations	Who can support, change, suspend or restore the service?
Policy	Which external provider terms or feature changes can alter behaviour?

Sovereignty concern	Question
Exit	Can data, Evidence, configuration and continuity survive provider change?

9. Trust, Value and Renewal

9.2 Human-Agent practice and judgement protection

Delegation and automation reviews must consider not only immediate decision risk but also the developmental work through which human judgement forms. Removing routine work may remove exposure to exceptions, consequences, correction and professional mental models. Where a capability remains strategically or ethically necessary, the redesign must provide alternative authentic practice, review and progression routes.

A human cannot hold meaningful accountability where the human lacks visibility, understanding, intervention rights or practical control. Nominal human approval does not cure opaque delegation. Human-Agent designs therefore state which judgements remain human, which are shared, which may be delegated, what evidence is preserved and how takeover, fallback and capability renewal operate.

9.1 Distribution, reinvestment and non-extraction test

Renewal before extraction requires more than continuity. A system may remain productive and reproduce its own capability while concentrating authority, burden and benefit. High-impact decisions therefore assess Capability Distribution, Agency Distribution and Benefit Distribution separately.

Capability Distribution asks who becomes more able and where dependency remains concentrated. Agency Distribution asks who gains meaningful voice, choice, challenge, authority, remedy and exit. Benefit Distribution asks who receives economic, developmental, reputational and social value, who carries burden or risk and whether sufficient value is reinvested into future participation and renewal.

Distribution	Constitutional question	Required safeguard
Capability	Who becomes more able, and whose expertise is consumed without transfer?	Dependency visibility, formation routes and successor obligations.
Agency	Who can shape, challenge, decide, intervene or exit?	Proportionate participation, appeal, override and non-retaliation.
Benefit	Who receives value and who carries burden, cost or displacement?	Beneficiary and burden records, transparency and reinvestment conditions.

Financial or operational Value does not override locked trust invariants. Trade-off review records beneficiaries, burdens, alternatives, constraints, residual Trust Risk and Renewal conditions. Trust Debt and Renewal Debt remain qualitative governed constructs until approved methods exist.

10. Embedded stewardship

Privacy, security, risk, compliance, architecture, service, finance and procurement stewards may participate close to practice while retaining formal independence, escalation and stop

rights. Informal guidance is not approval. Community belonging does not weaken assurance accountability.

11. Domain-aware trust constitution

DOMAIN TRUST INVARIANT

Domains are connected. People are not therefore made universally visible across them.

- Domain relationships express relevance, not permission.
- Participation in one Domain does not reveal participation in another by default.
- Evidence gathered in one Domain is not automatically portable.
- Outcome relevance does not create permission to profile a person.
- Cross-Domain Opportunity must not become cross-Domain surveillance.
- The Domain Contract declares visibility, portability, prohibited inference, challenge and remedy.

12. Domain Pack trust activation

Gate	Required Evidence
Scope and prohibited uses	Subjects, contexts, exclusions and unacceptable inference.
Ontology and Evidence	Definitions, methods, recency, provenance and contrary Evidence.
Privacy and workforce	Purpose, data classes, rights, segmentation and employment effects.
Agency and mobilisation	Authority, delegation, orchestration, override and safeguards.
Intelligence and judgement	QuestionFrames, challenge, confidence, Claim ceilings and publication.
Community and economics	Eligibility, safeguarding, Contribution rights, sponsorship and burden.
Renewal	Developmental Pathways, concentration, transfer and indicators.
Jurisdiction	Market enablement, residency, transfer, provider and feature review.
Acceptance	Denial, challenge, appeal, Agent stop, correction and recovery tests.

13. Challenge, remedy and recovery

Challenge object	Required remedy
Identity or Participation Context	Correction, separation, representation change or restriction.
Evidence or Claim	Access, explanation, counter-Evidence, suspension, correction or retraction.
Domain boundary or relationship	Review, restriction, reclassification, correction or withdrawal.
Stewardship Decision	Reasons, recusal, independent review or mandate change.
Agent Action	Stop, rollback, human takeover, redress and Delegation change.
Operational state or transition	Notice, affected-party voice, appeal, continuity and remediation.

14. Prohibited-use baseline

- Covert joining of personal and employer participation.
- Universal person ranking or composite FCO score.
- Inferring motivation, loyalty, culture fit or performance from participation.
- Using payment, sponsorship or platform ownership to control Domain truth.
- Allowing Agent transfer or tool calls to widen Authority or purpose.
- Publishing high-consequence Claims without approved Method, Evidence and review.
- Treating exit, deletion or remedy as discretionary support rather than system rights.

15. Acceptance and Trust Case

Before high-consequence activation, a Trust Case should assemble purpose, data classes, Authority, Evidence, Method Packs, affected-party participation, Agent governance, jurisdiction, failure modes, denial tests, challenge routes, rollback and recovery Evidence. Activation is an accountable Decision, not the automatic result of completing a checklist.

16. Openness, control and adversarial-misuse resolution

Stress-test concern	Frozen baseline resolution
Open participation versus controlled access	Belonging and legitimate participation may be open while data access, tool access, assured practice, Authority and stewardship remain purpose-bound, explicit and controlled. Openness never implies universal visibility or unrestricted Action.
Hidden workforce analytics	Resist joining participation, help-seeking, absence, challenge, Community activity or

Stress-test concern	Frozen baseline resolution
	personal Ambition into performance, loyalty, employability or culture-fit inference.
Vendor or Sponsor capture	Payment, platform ownership, sponsorship or service dependence cannot control Domain truth, Evidence standards, publication outcomes or challenge rights.
Agent Authority inflation	Agent Capability, confidence, recommendation frequency or technical reach cannot widen delegated Authority. Any widened scope requires a new explicit DelegationGrant.
Community status hierarchy	Recognition, visibility, badges, Contribution volume or network position cannot become permanent rank, assured competence or Decision Authority.
Marketplace extraction	Commercial exchange cannot hide unpaid burden, weaken rights, appropriate Community Assets or consume future Capability without review and remedy.

17. Architectural conclusion

FINAL POSITION

Trust is not a control layer added after innovation. It is the constitutional design of how Capability, intelligence, participation, Authority, Agents, Domains and value can operate legitimately enough to earn continued use and scale.

18. Trust Debt and Renewal Debt

The source constitution identified Trust Debt and Renewal Debt as useful qualitative governed constructs. The validation confirms that they should remain visible but must not become unsupported composite scores.

Construct	Meaning	Permitted use
Trust Debt	Known unresolved weakness in rights, permission, challenge, remedy, security or accountability.	Describe affected contexts, consequence, owner, mitigation and review.
Renewal Debt	Known consumption or neglect of future Capability, succession, learning or adaptability.	Describe what future Capability is at risk and what intervention is required.

19. Rights by lifecycle stage

Stage	Trust emphasis
Explore	Privacy by design, bounded scope, safe participation and stop conditions.
Prove	Evidence quality, affected-party voice, incident and correction routes.
Establish	Formal Authority, service accountability, jurisdiction and continuity.
Expand	Portability, aggregation, supply chain, monitoring and anti-surveillance.
Embed	Ongoing challenge, access review, remedy effectiveness and successor accountability.
Renew or retire	Export, deletion, Evidence retention, transition and consequence remediation.

20. Constitutional completeness test

- Can a participant understand purpose, context, visibility, use and exit?
- Can an affected person challenge a Claim, relationship, Agent Action or transition Decision?
- Can a formal steward advise early and still stop or escalate?
- Can the organisation recover from model, provider, data, identity or operational failure?
- Can Value be pursued without weakening locked rights or future Capability?
- Can implementation teams map each constitutional requirement to tested controls?

Cross-paper invariants

- Participation Context is the primary security, ownership and policy boundary.
- Capability, Agency, Authority, Mobilisation, Decision and Action remain distinct.
- Demand → Investment → Capability → Agency → Mobilisation → Decision → Action → Outcome → Impact → Value → Learning → Renewal is the canonical value chain.
- Observation, Signal, Pattern, Interpretation, Hypothesis, Claim and Decision remain distinct.
- Confidence is explainable and context-specific; it is not consensus, certainty or a universal score.
- Human or Agent Capability never creates Authority by itself.
- Personal Ambition and Development Intent do not become organisational workforce intelligence.
- Participation, activity, attendance, popularity and Contribution are not proof of Capability, motivation, alignment or Value.
- No high-consequence metric or Claim is activated without an approved Method Pack.
- Outcome is not Impact; Impact is not Value; positive outcomes do not override trust or Renewal.
- Challenge, appeal, override, remedy and recovery exist before scale.

- Capability and Opportunity must propagate together.
- Open belonging does not imply unrestricted access, Authority or assured competence.
- Renewal preserves and expands future Capability.

Confirmed WP06 architecture series

Paper	Title	Relationship
WP06.0	Introducing the Frontier Capability Organisation	Related paper
WP06.1	Capability Intelligence Platform Definition	Related paper
WP06.2	Trust, Security, Jurisdiction and Data Governance	This paper
WP06.3	Universal Information and Relationship Architecture	Related paper
WP06.4	Observatory, Intelligence and Judgement Architecture	Related paper
WP06.5	Personas, Participation and End-to-End Journey Architecture	Related paper
WP06.6	Adoption, Transition and Capability Propagation Architecture	Related paper
WP06.7	Domain Activation, Domain Mesh and Lifecycle Architecture	Related paper
WP06.8	Frontier Capability Operating Model	Related paper
WP06.9	Functional Requirements, Controls and Acceptance Architecture	Related paper
WP06.10	Platform, Integration and Technical Architecture	Related paper
WP06.11	Methods, Measurement and Assurance Architecture	Related paper
WP06.12	Ecosystem Participation, Value Exchange and Economics Architecture	Related paper