

CIVIC DECISION ENGINE

User Handbook

Step-by-Step Document Governance, Publication, and Record Association

Version 2.0

Prepared for the Civic Decision Engine



A practical handbook for controlled document intake, review, approval, publication, and explicit association with public CDE records.

Document control

Field	Value
Document title	Civic Decision Engine User Handbook
Version	2.0
Status	First operational edition
Purpose	Provide a repeatable, governed, step-by-step method for using the CDE document workflow
Primary audience	CDE administrators, reviewers, publishers, maintainers, and future authorised users
Scope	Document intake, review, approval, publication, associations, corrections, and quality control

Important

This handbook explains both what to do and why each step exists. The CDE is not a conventional file repository: it preserves independent objects, explicit lifecycles, provenance, verification, and governed relationships.

Contents

- 1. Purpose and operating model
- 2. Core governance principles
- 3. Understanding CDE objects
- 4. Preparing a document for intake
- 5. Completing the New Pending Document form
- 6. Workflow transitions
- 7. Declaring a document published
- 8. Creating record-document associations
- 9. Communication wrappers, attachments, replies, and receipts
- 10. Evidence boundaries
- 11. Corrections and immutability
- 12. Worked examples
- 13. Reusable note templates
- 14. Quality-control checklists
- 15. Recommended operating sequence

1. Purpose and operating model

The Civic Decision Engine (CDE) is a governed public-record, verification, and information-relationship platform. Its purpose is not merely to store files. It preserves the identity, provenance, lifecycle, evidential scope, and explicit relationships of each object entering the system.

Operating principle

A document should remain understandable without requiring its author to explain it. Meaning should arise from structure, evidence, provenance, and explicit relationships.

1.1 The standard workflow

Stage	Meaning	Primary responsibility
Pending Intake	The artifact has entered the governed process but has not yet been substantively reviewed.	Confirm the correct file and complete accurate metadata.
Under Review	The artifact is classified, its explicit contents are summarised, and its evidential boundaries are identified.	Separate what the document establishes from what it does not establish.
Approved	A reviewer confirms that provenance, metadata, integrity, and evidential scope are sufficiently defined.	Approve the artifact for publication; do not endorse every statement as independently true.
Published	The approved artifact enters the Public Document Library under a deliberate publication declaration.	Preserve the public state and publication note.
Associated	A published document is explicitly linked to an existing public CDE record.	Explain why the relationship exists without merging the objects.

2. Core governance principles

Structure before visibility

Publication, access, and transparency do not create trust where the information structure cannot be understood.

Independent identity

Documents, records, associations, source items, and relationships remain independent objects.

Controlled publication

Nothing becomes public merely because it was uploaded. Publication follows review and explicit approval.

Provenance preservation

Origin, transmission, capture, review, and publication dates must not be collapsed into one timestamp.

Evidence boundaries

Every review identifies both what a document explicitly supports and what it does not establish.

No silent rewriting

Published objects are not silently corrected. Errors are preserved and addressed through governed correction or explanatory context.

Relationships are explicit

Context is created through visible associations rather than implied folder placement.

Search metadata is not evidence

Keywords improve discovery but do not prove facts or establish findings.

3. Understanding CDE objects

Object	What it represents	What it must not be confused with
Published Document	A preserved source artifact such as a letter, receipt, email, prescription, image, audio file, spreadsheet, or statutory extract.	A public CDE record or a conclusion drawn from the artifact.
Public CDE Record	A structured civic record describing an event, institutional state, trajectory, finding, condition, or complaint milestone.	The document files that support or contextualise it.
Association	An explicit governed link between one public record and one published document.	A merge, evidence import, lifecycle change, or verification-hash change.
External Reference Identifier	An identifier assigned by an external source, such as a case number, form number, invoice number, or institutional reference.	The permanent Document Identifier assigned automatically by the CDE.
Verification Data	Integrity and identity information generated by the CDE.	A statement that every claim in the artifact is substantively true.

4. Preparing a document for intake

4.1 Decide whether the file contains one object or several

Before uploading, determine whether the artifact should be preserved as one document or separated into multiple independent documents. The decision should follow evidential function, not convenience.

Artifact encountered	Recommended treatment	Reason
Secure email notification with attached letter	Intake the notification and the letter separately.	The notification proves transmission; the letter proves substantive content.
Email reply to the secure communication	Intake separately.	The reply proves acknowledgement or response.
Automated read receipt	Intake separately.	The receipt proves access to the message, not agreement with it.
Clinical letter plus consultation receipt	Intake separately.	Each establishes a different fact and retains its own provenance.
Prescription plus pharmacy claim form	Intake separately.	One records prescribing; the other records dispensing.
Statutory extract saved during a case	Intake separately as legislative reference material.	It supplies legal context rather than case-specific evidence.

Decision test

Ask: “Would this artifact still have a meaningful independent evidential function if separated from the other material?” If yes, preserve it as an independent document.

4.2 Pre-intake checklist

- Confirm the file is readable and complete.
- Confirm the artifact is not an accidental duplicate.
- Identify the source institution or author.
- Identify the date belonging to the artifact itself.
- Check whether a source-assigned reference appears.
- Consider personal or sensitive information before publication.
- Decide whether a communication wrapper and its attachment must be separated.
- Choose a neutral, precise title before entering the form.

5. Completing the New Pending Document form

5.1 Document file

Upload the original artifact in a supported format. File conversion should not alter meaning. Where an image or screenshot is the source artifact, preserve it as such rather than presenting it as a typed reconstruction.

5.2 Title

A good title identifies the source, document type, and principal subject. It should be neutral, concise, and distinguish the artifact from related documents.

Good title	Why it works
Medical Council – PPC Investigation Notice under Section 59(7)	Identifies the institution, procedural document type, and statutory basis.
Doctor 365 – Receipt for Intramuscular Injection	Identifies source, artifact type, and service.

Medical Council – Secure File Transfer Notification (25 November 2020)	Distinguishes the transmission wrapper from other notifications.
Tesco Pharmacy – Prescription Claim Form for Fucidin H Cream	Identifies the dispensing institution, form type, and medication.

Avoid

Do not use a title that adds an allegation, conclusion, motive, or finding not stated in the source.

5.3 Institution / Source

Enter the originator of the artifact, not every person or institution later connected with it. A Doctor 365 prescription remains sourced to Doctor 365 even when transmitted to a Medical Council case worker.

5.4 Document date

Use the date belonging to the artifact: letter date, email date, consultation date, dispensing date, transaction date, or capture date. Do not substitute the CDE upload date for the historical artifact date.

5.5 Category

Common category	Use for
Official Correspondence	Formal institutional letters and notices.
Email Correspondence	Ordinary sent or received email content.
Administrative Correspondence	Transmission notices, confirmations, and operational messages.
Clinical Correspondence	Letters recording treatment or clinical facts.
Prescription	A prescribing record.
Receipt	A financial or transactional record.
Prescription Claim Form	A dispensing or pharmacy claim record.
Legislation	A statutory extract or legislative reference.
Read Receipt	Automated proof that a message was opened.

5.6 Keywords

Keywords support governed search and discovery. Use descriptive terms that are present in or directly connected to the source. They do not create evidential meaning or factual verification.

Example

Medical Council, Darren Smith, C397/19, Preliminary Proceedings Committee, Section 59(7), secure file transfer

5.7 Optional Reference Identifier

Use only an identifier assigned outside the CDE. Examples include C397/19, 004/683, an invoice number, or a source-issued case reference. Leave the field blank where no external identifier exists.

Do not enter

Names, recipients, institutions, descriptions, transmission details, or explanatory prose. The CDE assigns the permanent Document Identifier automatically after upload.

5.8 Description

The description should objectively state what the artifact is and what it records. It should not assess credibility or make findings beyond the source.

Description pattern

[Document type] issued or sent by [source] on [date], recording [specific content or event].

5.9 Notes

Notes preserve operational and provenance context: transmission history, relationship to attached material, reason for separate preservation, limitations, or later administrative use.

Notes example

Communication wrapper accompanying a substantive attached letter. Preserved separately to maintain evidence of transmission and administrative chronology.

5.10 Visibility

New documents should normally begin as Private. Visibility does not replace lifecycle status. A document is not public merely because it has entered the intake system.

6. Workflow transitions

6.1 Pending Intake

Pending Intake means the artifact has been stored but has not yet received substantive review. The purpose of this stage is controlled entry and metadata validation.

Pending administrative note

Initial intake of [document type] from [source], dated [date]. Stored as pending for metadata verification and evidential review.

6.2 Begin Review

Review should classify the artifact, summarise only its explicit contents, identify provenance, and define evidential boundaries.

Required review components

- Document classification
- Evidence class
- Institution or source
- Document date
- Evidence summary
- Evidence boundaries
- Review recommendation

Review recommendation

Ready for Approval. The document has identifiable provenance, a clear date, readable content, and defined evidential boundaries.

6.3 Approval

Approval confirms that the artifact is suitable to proceed within the lifecycle. It does not mean that every statement in the artifact has been independently proven true.

General approval note

Approved as an authentic [document type]. The document contains identifiable provenance, a clear date, and defined evidential boundaries. It is suitable for publication as [evidence classification].

6.4 Declare Published

Publication is a deliberate governance action. The publication note should state what kind of artifact is entering the Public Document Library and preserve the limits of publication.

General publication note

Published as an authenticated [document type]. This document preserves the contemporaneous record, its provenance, and its evidential boundaries. Publication does not extend beyond the information recorded in the source document.

7. Declaring a document published

7.1 Final pre-publication checks

- Title is neutral and accurate.
- Institution or source is correct.

- Artifact date is correct.
- External reference is genuine or blank.
- Description does not overstate the source.
- Notes preserve context without becoming a finding.
- Sensitive information has been considered.
- Approval note is complete.
- The consequences of immutability are understood.

Publication warning

Published document metadata should be treated as immutable. Perform the final metadata check before declaring publication.

8. Creating record-document associations

An association connects one existing public CDE record and one existing published document. It does not merge them, import evidence into the record, alter either lifecycle, or change verification hashes.

8.1 Select the public record

Search by canonical reference, title, institution, trajectory, finding, system state, conditions, signals, tags, or public summary. Read the selected-record context before proceeding.

8.2 Select the published document

Search by Document Identifier, title, description, institution, reference, date, filename, extracted text, or keywords. Confirm the correct artifact where several documents share a date or subject.

8.3 Relationship type

Supporting document is appropriate where the artifact supports, contextualises, transmits, acknowledges, or supplies reference material to the public record.

8.4 Public label

The public label is a short reader-facing description of the relationship. It should be immediately understandable.

Document function	Recommended public label
Clinical or pharmacy artifact	Supporting Clinical Evidence
Email or letter	Supporting Correspondence
Secure transfer wrapper	Secure transmission notification
Read receipt	Encrypted email read receipt
Acknowledgement reply	Acknowledgement of Medical Council correspondence
Procedural notice	Medical Council investigation notice
Statutory extract	Statutory legislative reference

8.5 Public note

The public note explains why the relationship exists. It should identify the document function and preserve the evidential boundary of both objects.

Public note pattern

Documents [specific event or function] within the [record] chronology and preserves its contextual relationship to the public record without extending the evidential scope of either object.

8.6 Administrative note

The administrative note records the governance reason for the association, chronological role, related artifacts, and any boundary that future administrators should understand.

Administrative note pattern

Associated with [record reference] as [role]. This document [specific function]. The association preserves provenance, chronology, and evidential boundaries without altering the lifecycle or verification state of either object.

9. Communication wrappers, attachments, replies, and receipts

9.1 Recommended sequence

1. Intake the secure email or transmission wrapper first.
2. Intake the attached substantive letter separately.
3. Intake any reply separately.
4. Intake any automated read receipt separately.
5. Publish each object through its own lifecycle.
6. Associate each object independently with the relevant public record.

9.2 What each object proves

Object	What it establishes	What it does not establish
Secure transfer notification	Sender, recipient, transmission time, secure method, existence of attachment.	The contents or correctness of the attached letter.
Attached official letter	The substantive administrative or procedural content.	That the recipient opened or accepted it.
Reply	Acknowledgement, response, or continued communication.	Agreement with every part of the source message unless expressly stated.
Read receipt	That the intended recipient opened the message.	Agreement, action, or substantive consideration.
Receipt	Payment, date, service description, transaction method.	Diagnosis, clinical reasoning, or outcome.
Prescription claim form	Dispensing or pharmacy processing.	Clinical diagnosis or why the medication was prescribed.

10. Evidence boundaries

Evidence boundaries are a core CDE safeguard. A review must separate explicit source content from inference, interpretation, or later context.

10.1 Boundary method

7. List the facts directly visible in the artifact.
8. Identify facts that require another document.
9. Avoid importing knowledge from related records into the artifact review.
10. State missing information explicitly.
11. Do not convert a transmission event into proof of substantive content.
12. Do not convert a receipt into proof of clinical outcome.

Artifact	May establish	Does not by itself establish
Clinical letter	Treatment date, medication, route, stated reason, author.	Long-term outcome or wider responsibility.
Consultation receipt	Attendance/payment for a consultation.	Clinical findings or diagnosis.
Prescription	Medication, dose/instructions, prescriber information.	Dispensing or treatment outcome.
Pharmacy claim form	Medication was processed/dispensed.	Reason for prescription or clinical assessment.
PPC investigation notice	A formal procedural step was directed.	Final outcome or practitioner response.
PPC decision letter	The decision and reasons stated by the PPC.	Whether those reasons were factually or legally correct.

11. Corrections and immutability

The CDE does not silently rewrite published objects. This protects reproducibility and auditability, but it requires care before publication.

11.1 Before publication

- Correct metadata while the object remains within the editable pre-publication workflow.
- Verify the external reference field carefully.
- Check the selected file, title, source, date, category, description, and notes.

11.2 After publication

Where a metadata error is discovered after publication, preserve the published state. Use a supported correction, superseding object, explanatory association, or administrative record rather than pretending the original publication never occurred.

Governance principle

Publication preserves history. Governance preserves context.

12. Worked examples

12.1 Secure transfer notification

Title

Medical Council – Secure File Transfer Notification (25 November 2020)

Description

Secure ShareFile notification from Darren Smith, Case Officer, Medical Council of Ireland, advising that an encrypted message containing an attached letter had been sent in relation to complaint C397/19.

Approval note

Approved as a contemporaneous communication record documenting secure transmission by the Medical Council. No alterations made to content or provenance.

Publication note

Published as a supporting communication documenting the secure delivery of correspondence within complaint C397/19. Preserved independently from the attached letter to maintain a complete administrative record and communication chronology.

Public label

Secure transmission notification

Public note

Documents the secure electronic transmission of Medical Council correspondence on 25 November 2020. Preserved independently from the attached letter to maintain communication provenance and administrative chronology.

Administrative note

Associated as supporting evidence for complaint record CMP-MC-20191202-001. This document records the transmission event only; the attached letter remains an independent published document with its own lifecycle and evidence relationship.

12.2 Procedural investigation notice

Public label

Medical Council investigation notice

Public note

Official Medical Council correspondence documenting that the Preliminary Proceedings Committee directed a notice under Section 59(7) of the Medical Practitioners Act 2007 in relation to complaint reference C397/19. This document records a formal procedural step within the complaint process and preserves the associated statutory context.

Administrative note

Associated with CMP-MC-20191202-001 as primary procedural evidence. This document records commencement of the Preliminary Proceedings Committee's formal investigative process. The association preserves procedural provenance without extending the evidential scope beyond the published correspondence.

12.3 Read receipt

Public label

Encrypted email read receipt

Public note

Documents that the encrypted correspondence was viewed by the intended recipient, preserving communication provenance within the complaint chronology.

Administrative note

Associated with CMP-MC-20191202-001 as supporting communication provenance. This document evidences recipient access to the encrypted correspondence and complements the transmission notification and associated procedural correspondence without extending their evidential scope.

12.4 Consultation, prescription, and dispensing chain

Document	Independent function	Suggested label
Consultation receipt	Confirms consultation and payment.	Supporting Clinical Evidence
Prescription	Confirms what was prescribed.	Supporting Clinical Evidence
Pharmacy claim form	Confirms processing or dispensing.	Supporting Clinical Evidence

Why separate them

Together they form a coherent chain, but each document proves a different part of the sequence and must retain its own identity and evidential boundary.

13. Reusable note templates

Begin Review – general

Reviewed as a [document type] with identifiable provenance and a clear document date. The document explicitly records [facts]. It does not by itself establish [boundaries]. Ready for Approval.

Approval – general

Approved as an authentic [document type]. The document contains identifiable provenance, a clear date, readable content, and defined evidential boundaries. It is suitable for publication as [classification].

Publication – general

Published as an authenticated [document type]. This document preserves the contemporaneous record, its provenance, and its evidential boundaries. Publication does not extend beyond the information recorded in the source document.

Association – public note

Documents [specific event or function] within the [record] chronology and preserves its contextual relationship to the public record without extending the evidential scope of either object.

Association – administrative note

Associated with [record reference] as [role]. This document [specific function]. The association preserves provenance, chronology, and evidential boundaries without altering the lifecycle or verification state of either object.

14. Quality-control checklists

14.1 Before storing as Pending

- ☐ Correct file selected
- ☐ Artifact readable and complete
- ☐ Neutral and precise title
- ☐ Correct source institution
- ☐ Historical date preserved
- ☐ Category matches function
- ☐ External reference genuine or blank
- ☐ Description source-grounded

- ☐ Notes preserve context
- ☐ Visibility appropriate

14.2 Before Approval

- ☐ Metadata checked against source
- ☐ Provenance identifiable
- ☐ Evidence summary limited to explicit content
- ☐ Evidence boundaries stated
- ☐ Related artifacts separated where required
- ☐ Sensitive information considered
- ☐ Review recommendation justified

14.3 Before Publication

- ☐ Final title check
- ☐ Final date check
- ☐ Final source check
- ☐ Final external reference check
- ☐ Approval note complete
- ☐ Publication note complete
- ☐ Immutability understood
- ☐ Public visibility deliberate

14.4 Before Association

- ☐ Correct public record selected
- ☐ Correct published document selected
- ☐ Relationship type appropriate
- ☐ Public label concise
- ☐ Public note explains relationship
- ☐ Administrative note records governance context
- ☐ No claim exceeds source boundaries

15. Recommended operating sequence

1. Review the artifact outside the intake form and decide whether it contains one or more independent objects.
2. Upload one artifact and complete the pending metadata carefully.
3. Begin Review and write an explicit evidence summary and evidence boundaries.
4. Approve only when provenance and metadata are sufficiently defined.
5. Perform a final metadata check, then declare the document published.
6. Locate the correct public CDE record.
7. Create an explicit association with a short public label, bounded public note, and administrative note.
8. Repeat separately for wrappers, attachments, replies, receipts, and statutory context.
9. Preserve errors and corrections through governance rather than silent rewriting.

Final rule

Each object should explain itself. Each transition should explain why it occurred. Each relationship should explain

why it exists.

Appendix A – Compact field reference

Field	Question to answer
Title	What is this artifact?
Institution / Source	Who created or issued it?
Document Date	When did this artifact originate or occur?
Category	What function does this artifact perform?
Keywords	How should it be discovered?
External Reference	What identifier did the outside source assign?
Description	What does the artifact objectively record?
Notes	What provenance or operational context should be preserved?
Approval Note	Why is it suitable to publish?
Publication Note	Why and within what bounds is it public?
Public Label	How should the relationship be understood at a glance?
Public Note	Why does the association exist?
Administrative Note	What governance context must future administrators retain?

Appendix B – Definitions

Term	Definition
Artifact	The source file or object entering the CDE.
Provenance	The origin, custody, transmission, and lifecycle context of an object.
Evidence boundary	The line between what a document explicitly establishes and what requires other evidence or inference.
Canonical record reference	The permanent reference identifying a public CDE record.
Document Identifier	The permanent identifier assigned automatically by the CDE after upload.
External Reference Identifier	A source-assigned identifier preserved separately from the CDE identifier.
Publication declaration	The deliberate transition making an approved document publicly accessible.
Association	A governed, explicit relationship between a public record and a published document.

CIVIC DECISION ENGINE

Trust begins with structure.

CIVIC DECISION ENGINE

User Handbook — Part II

Platform Governance Features: CDE v12.2 – v13.0

Version 1.0

Continues Civic Decision Engine User Handbook v1.0

A practical guide to the Administration Console, extended document intake, audit traceability, publication provenance, associations, archive collections, governed corrections, canonical record types, the Public Archive Explorer, the Traceability Map, and Governed Public Transmissions.

Preface to Part II

Part I of this handbook (Version 1.0) documented the original document-governance workflow: intake, review, approval, publication, and record association. Since that edition, the Civic Decision Engine has been extended through a long series of governed releases, from CDE v12.2 through CDE v13.0.5.

Part II documents what those releases added: the Administration Console, extended intake formats, administrative audit traceability, publication provenance, the record–document association workflow in its current searchable form, archive collections, governed intake correction, canonical record types, the Public Archive Explorer, the Traceability Map, and Governed Public Transmissions.

Part II assumes familiarity with Part I. The governance principles set out in Chapter 2 — structure before visibility, independent identity, controlled publication, provenance preservation, evidence boundaries, no silent rewriting, explicit relationships, and search metadata not being evidence — continue to apply without modification. Every feature described here was built to extend those principles, not to replace them.

Important

This handbook describes governed platform behaviour as released. It does not certify legal validity, evidential sufficiency, factual correctness, or institutional authority for any object it describes.

Contents — Part II

- 16. The Administration Console
- 17. Extended Document Intake
- 18. Administrative Audit Traceability
- 19. Publication Provenance
- 20. Record–Document Associations
- 21. Archive Collections
- 22. Governed Intake Correction and Document Reassignment
- 23. Canonical Record Types and Creating Records from Documents
- 24. Public Archive Explorer and Traceability Map
- 25. Public Document Previews
- 26. Governed Public Transmissions
- 27. Updated Quality-Control Checklists and Operating Sequence

16. The Administration Console

The Administration Console at /admin brings the authenticated administrative workflow into one place. A shared navigation bar connects the dashboard, document intake, intake review, record evidence, administrative audit, associations, archive collections, and the Public Document Library.

16.1 Console areas

Console area	Purpose
Dashboard	Lifecycle counts, active review-queue links, record-reference navigation, and session logout.
New Document Intake	Capture a new pending document (Chapter 17).
Intake Management / Review	Move documents through Pending Intake, Under Review, Approved, Published, Rejected, Archived.
Administrative Audit	Read-only lifecycle-history traceability (Chapter 18).
Associations	Create and govern record–document relationships (Chapter 20).
Archive Collections	Create collections and govern membership (Chapter 21).
Intake Corrections	Reassign misfiled archived intake records (Chapter 22).
Record Evidence	Inspect existing public CDE records.
Public Document Library / Public Archive Explorer	Jump to the equivalent public-facing views.

16.2 Named administrator authentication

Administration Console login uses named administrator credentials: the required ADMIN_USERNAME and ADMIN_PASSWORD environment variables. There is no password-only fallback, and the system fails closed if either variable is absent or empty.

On successful login, the administrator's username is stored in the protected server-side session. That session identity — not a query parameter, form field, header, or client-supplied value — is what gets recorded as the acting administrator for every new document-intake and lifecycle-history action going forward. A restrained indicator, “Signed in as: <username>”, is shown throughout the Console so the acting identity is always visible.

Why this matters

Historical actor values recorded before named authentication (for example, generic “admin” entries) are preserved exactly as they were. Only new actions are attributed to the named session identity. This is the same no-silent-rewriting principle from Chapter 11: the record of who acted is never retroactively rewritten.

16.3 Practical guidance

- Confirm the “Signed in as” indicator before beginning review, approval, or publication actions, particularly on shared administrative machines.
- Do not rely on notes or descriptions to record who performed an action — actor attribution is handled automatically by the session and should not be duplicated manually.

- Session logout is available from the dashboard; use it when stepping away from an authenticated session.

17. Extended Document Intake

The intake workflow described in Chapters 4–5 now accepts a wider range of original file formats. Every format uses the same private lifecycle — Pending Intake, Under Review, Approved, Published, Rejected, Archived — and the same provenance, hashing, keyword, and Public Document Library search behaviour as the original PDF workflow.

17.1 Accepted formats

Format	What CDE does	What CDE does not do
JPEG / PNG (images)	Validates file type from both extension and byte signature; stores original bytes; shows a restrained inline image on the public detail page once Published; serves a separate view route and a separate download route.	OCR, image interpretation, automatic metadata extraction, image conversion, thumbnailing, or galleries.
M4A / MP3 / WAV (audio)	Same private intake and publication lifecycle; Published detail pages provide an HTML5 audio player using the original file plus a download.	Transcription, speech recognition, waveform extraction, or transcoding.
XLS / XLSX (spreadsheets)	Validates workbook structure server-side; identifies the artefact as a spreadsheet; displays available metadata such as worksheet names; retains original-file download.	Executes formulas, macros, external links, data connections, or scripts. Rejects macro-enabled, encrypted, malformed, or mismatched packages outright.
RTF (Rich Text Format)	Recognises application/rtf, text/rtf, and application/x-rtf variants; validates structure; retains original-file download.	Converts, renders, executes, or extracts full text from the file during intake or publication.

JPEG intake accepts the legitimate marker variants produced by different editors and redaction tools (JFIF, EXIF, ICC-profile, Adobe, and similar), and treats .jpg and .jpeg as equivalent, case-insensitively. Server-side byte detection remains authoritative throughout: a PNG renamed as a JPEG, a JPEG renamed as a PNG, or a JPEG 2000 / JP2 file renamed with a .jpg extension is rejected rather than admitted under the wrong type. Export JPEG 2000 files explicitly as JPEG before intake if JPEG is the intended governed format.

17.2 Keywords

The KEYWORDS field on the intake form accepts comma-separated descriptive terms. Keywords are normalised into a stable set and preserved through review, approval, publication, correction, and archival. They are included in Public Document Library search and in the Published-document selector used when creating associations.

Evidence boundary reminder

As with the original Keywords guidance in Chapter 5.6, keywords improve discovery. They do not change

document bytes, SHA-256, lifecycle status, publication rules, associations, or the evidential weight of the artefact.

17.3 Pre-intake checklist additions

- ☐ Confirm the file's true format by inspection, not by filename or extension alone.
- ☐ For spreadsheets: confirm the workbook is not macro-enabled, encrypted, or password-protected before upload.
- ☐ For images: preserve the original file rather than a screenshot of a screenshot, where the original is available.
- ☐ For audio: confirm the recording is the original captured file, not a re-encoded copy, where possible.
- ☐ Enter keywords that are present in or directly connected to the source artefact.

18. Administrative Audit Traceability

The Administrative Audit page at `/admin/audit` consolidates every Document Intake lifecycle-history entry into one read-only traceability table.

18.1 What the audit table shows

Column	Content
Timestamp	When the transition occurred.
Document / Reference / Filename	Which document was affected.
Previous status → New status	The lifecycle transition recorded.
Actor	The administrator attributed to the transition (Chapter 16.2).
Transition note	The note entered at the time of the transition.
Current document status	Where the document sits now, with a link back to its review page.

The page reads from the authoritative lifecycle history already stored with each intake record — it does not create a parallel record of events. Filtering is conservative, ordering is deterministic (newest first), and results are paginated.

18.2 When to use it

- Reconstructing the chronology of a specific document before relying on it in a public association.
- Confirming which administrator performed a review, approval, or publication action.
- Preparing the administrative note for a Governed Intake Correction (Chapter 22), where the prior chronology needs to be understood before a new corrected intake is created.

Limitation

The audit view is read-only. It does not add mutation controls, create new lifecycle states, rewrite historical actors, or expose underlying storage paths.

19. Publication Provenance

Every Published document's public detail page includes a Publication Provenance section and a Publication Pathway section, giving readers the same chronological grounding an administrator already has internally.

19.1 What appears on a Published document page

- Intake timestamp and server-detected format
- Original filename and file size
- SHA-256 digest
- Recorded lifecycle actors for review, approval, and publication
- Review, approval, and publication timestamps
- Current lifecycle state and public reference identifier
- Presentation mode and original-file download availability

Where a document was Published more than once in its history (for example after correction), the displayed publication timestamp is the earliest recorded transition into Published, so the page reflects when the document first entered the public record rather than the most recent administrative touch.

What SHA-256 does and does not tell a reader

The SHA-256 digest identifies the exact bytes admitted to the CDE. It does not certify authorship, factual truth, legal status, or external authenticity — the same boundary already set out for evidence generally in Chapter 10.

20. Record–Document Associations

Chapter 8 described how an association connects one public CDE record and one Published document. That workflow now uses a governed, searchable selector rather than free-text record entry, and associations carry their own stable public references and history.

20.1 Creating an association

13. Open Associations in the Administration Console and start a new association.
14. Search for the public record using the searchable selector. Results show the canonical reference first, with institution code, trajectory, system state, and finding summary in a context panel so you can confirm you have the right record before selecting it.
15. Search for the Published document by Document Identifier, title, description, institution, reference, date, filename, extracted text, or keyword.
16. Choose the relationship type — Supporting document is appropriate where the artefact supports, contextualises, transmits, acknowledges, or supplies reference material.
17. Write a short, reader-facing Public Label (Chapter 8.4) and a bounded Public Note explaining why the relationship exists (Chapter 8.5).
18. Write an Administrative Note recording the governance reason, chronological role, and any boundary future administrators should understand (Chapter 8.6).
19. Submit. The system assigns a stable reference in the form CDE-ASSOC-YYYYMMDD-NNN.

The selector is a presentation aid, not the source of truth

The searchable record selector improves accuracy and readability, but server-side validation remains authoritative underneath it. A submission must resolve to exactly one canonical stored record reference;

display labels, search text, and context-panel content are never themselves stored as association values.

20.2 Public association pages and discovery

Each association has its own public page at `/associations/{association_reference}`, showing the association summary, the linked public record, the linked Published document, the governance boundary, and a public-safe Association Pathway drawn from the association's own history.

The public index at `/associations` lists active, public, eligible associations with search, filters, and pagination, so a reader can discover associations without already knowing a specific reference.

20.3 What an association changes — and what it does not

An association	Does	Does not
Relationship state	Creates an explicit, inspectable link with its own identity and history.	Merge the record and the document into one object.
Evidence	Shows the document alongside the record for context.	Add the document to the record's evidence, or imply evidential sufficiency.
Integrity	—	Alter record verification hashes or document SHA-256 values.
Lifecycle	—	Change either object's lifecycle state.
Interpretation	—	Imply factual verification, legal status, authorship, responsibility, or endorsement.

21. Archive Collections

An Archive Collection is a governed object that groups other governed public objects — Canonical Records, Published Documents, and Associations — into an ordered, publicly presentable set, without absorbing their identity.

Design principle

“Collections do not absorb identity.” A collection presents governed memberships, not copies. Every member remains independently governed, independently addressable, and independently provenanced.

21.1 Creating a collection

20. In the Administration Console, create a new Archive Collection. The system assigns a stable public reference in the form `CDE-COLL-YYYYMMDD-NNN`.
21. Add members by creating Collection Memberships — governed objects in their own right, each with an immutable reference in the form `CDE-MEM-YYYYMMDD-NNN` — that reference an existing document, record, or association without copying it.

22. Set each membership's `display_sequence` to control ordering. Active memberships must use positive, non-duplicate sequence positions.
23. Move each membership through its own governance path: create, review, approve, activate. Members can later be removed and restored without losing history.
24. Publish the collection so it appears at `/collections` and at `/collections/{collection_reference}`.

21.2 Sequence diagnostics

The collection detail page shows sequence diagnostics: continuity state, active member count, sequence range, any missing or duplicate positions, and previous/next context for each membership. Public collection pages only ever render active, publicly eligible members in safe order — administrative gaps or hidden memberships are never revealed publicly.

What a collection does not do

Creating or reordering a collection does not alter document provenance, lifecycle, SHA-256 values, record verification, association semantics, Publication Provenance, or Administrative Audit history for any member.

22. Governed Intake Correction and Document Reassignment

Chapter 11 established that the CDE does not silently rewrite published objects. Governed Intake Correction is the mechanism referred to there: a controlled path for fixing an archived intake record whose preserved bytes were assigned to the wrong metadata, without pretending the original entry never happened.

22.1 Correction lifecycle

Stage	Meaning
Draft	A correction has been proposed for an archived intake record.
Under Review	The correction is being checked against the original artefact and metadata error.
Reviewed	The reviewer has confirmed the correction is appropriate.
Authorised	An administrator has authorised the correction to be executed.
Completed	The correction has been executed and a new corrected intake identity created.

22.2 What completion does

- Creates a new, corrected intake identity from the exact same preserved bytes and the exact same SHA-256 digest.
- Leaves the original archived source intake and its full history unchanged and in place.
- Starts the new destination intake as ordinary Pending Intake — it must still pass through the full review, approval, and publication workflow described in Chapters 6–7.
- Does not accept client-supplied actor or reference overrides; attribution follows the same session-based identity rule as every other action.

Why the source record is preserved

Preserving the archived source intake rather than editing it in place keeps the original chronology intact. Anyone who saw the earlier, incorrect metadata can still verify what the system showed at the time; the correction is visible as a governed event, not an erasure.

23. Canonical Record Types and Creating Records from Documents

23.1 Record types

Canonical CDE records now carry a governed `record_type` field, allowing records to represent distinct kinds of civic and administrative event: Strike, Complaint, Investigation, Decision, Proceeding, Administrative Action, Public Submission, Policy Event, and Research Record. Existing records without an explicit type continue to behave exactly as Strike records — their references, URLs, lifecycle state, verification hashes, and history are unaffected.

Record type is searchable in the Public Record Index and is shown during association creation, so a Published document can be attached to a Complaint record rather than an unrelated Strike record simply because the selector makes the type visible. Record type is not part of the legacy verification-hash inputs, so existing hashes remain verifiable exactly as before.

23.2 Creating a canonical record from a Published document

Where a Published document itself describes an event that should have its own canonical record, the document's admin view offers a “Create canonical record from this document” action.

25. Open the Published document in the Administration Console.
26. Select “Create canonical record from this document.” The system prefills editable record metadata from the document's title, description, institution/source, document date, category, keywords, and reference identifier where available.
27. Review and correct the prefilled fields — this is a starting point, not an automatic transcription.
28. Save the record as a new, separate canonical object.
29. If a Record–Document Association should exist between the new record and the source document, create it explicitly through the ordinary association workflow (Chapter 20). It is not created automatically.

Object boundary preserved

The document remains an independent published evidential artefact. The record is a separate canonical public object. The document's SHA-256 is never reused as the record's verification hash, document bytes are never copied into the record, and OCR or body text is never converted into findings.

24. Public Archive Explorer and Traceability Map

24.1 Public Archive Explorer

The Archive Explorer at `/archive` is a unified public discovery doorway across every governed public object type: Canonical Records, Published Documents, Record–Document Associations, and Governed Public Collections. It offers counts, search, filters, sorting, and pagination, and links back to each object's own native public page.

The Explorer is not itself a governance object and does not duplicate provenance. It does not alter lifecycle state, change verification hashes, mutate publication eligibility, expose private metadata, or replace /records, /documents, /associations, or /collections — it sits alongside them as a way to search across all of them at once.

24.2 Public navigation and governance principles

Consistent breadcrumbs, archive return links, and governed object-type badges appear across Canonical Record, Published Document, Association, and Collection pages, so a reader can always tell what kind of object they are looking at and how to get back to the Archive.

Governance principles behind the navigation

Identity exists before association. A record is not its evidence. Evidence is not the record. The relationship is governed. Collections do not absorb identity. Provenance belongs to every object. History should never be overwritten.

24.3 Traceability Map

The Traceability Map at /traceability is a public discovery interface over declared relationships between governed public objects. It is not itself a governed object — it reveals relationships without owning them.

Each traceability result represents one governed Association chain:

Canonical Record → declared by → Governed Association → links to → Published Document

Collections appear only as governed membership context on the map — they do not own, contain, or absorb the Records, Documents, or Associations shown. The Map provides public-safe filters, unique object counts, bounded pagination, and safe return links, and it does not create or infer relationships that were not already explicitly declared through an association.

25. Public Document Previews

The Public Document Library shows compact previews so a reader can recognise a Published artefact before opening its detail page.

- Published JPEG and PNG documents show a constrained image thumbnail linking to the Published Document page.
- PDF, Rich Text, Spreadsheet, Audio, and unknown media types show a compact fallback preview with a visible media-type label and a descriptive link.

What a preview is not

A preview is a presentation of an existing governed document, not a new governed artefact. No derived thumbnail is stored as a separate object, SHA-256 semantics are unchanged, and no lifecycle, publication, or eligibility rule is affected.

26. Governed Public Transmissions

26.1 Platform identity transition (v13.A)

Before Transmissions were introduced, v13.A aligned the platform's visible identity — name, short name, version references, page titles, navigation identity, watermarks, and public and administrative presentation — with the governance architecture already established across the v12 series. The current platform identity is: canonical name Civic Decision Engine; short name CDE; tagline “Independent · Transparent · Traceable.” This stage changed presentation only; every existing governed object, identifier, lifecycle state, publication rule, association, collection, traceability view, and public URL was preserved unchanged.

26.2 What a Transmission is

A Public Transmission is a first-class governed public object that records the public communication context in which one or more other governed public objects were communicated. It has its own reference, metadata, lifecycle, publication state, provenance, covering communication, and public page.

Governance boundary

A Transmission governs communication. It does not govern the objects communicated. Published Documents, Canonical Records, Associations, and Collections remain independently governed and independently addressable when referenced by a Transmission. Nothing is copied into the Transmission, converted into a Transmission, or assigned a new SHA-256 value.

26.3 Creating a Transmission

30. In the Administration Console, start a new Transmission Intake.
31. Enter the covering communication's metadata — the context in which the communication occurred — and the sender/recipient model appropriate to that communication.
32. Search for and select one or more existing governed Documents to include. Selected documents are reviewed before submission and keep the order in which they were chosen.
33. Confirm and submit. Each included Document receives its own separate governed inclusion relationship to the Transmission; none of them are copied or re-hashed.
34. Documents, Records, Associations, or Collections can also be added to a Transmission after creation, using the same post-creation inclusion workflow.
35. Move the Transmission through its own lifecycle to Published when it is ready to appear in the Public Transmission Library.

26.4 What a Transmission establishes — and what it does not

A Transmission	Establishes	Does not establish
Communication context	That a specific communication event occurred and which governed objects were included in it, in what order.	Agreement with, or endorsement of, the contents of anything included.
Included objects	A typed relationship between the Transmission and each included object.	New evidential weight beyond what each included object already independently establishes.
Identity	—	That any included object was altered, copied, or re-identified.

		Each keeps its own CDE Document Identifier, lifecycle, provenance, and verification hash.
--	--	---

Transmissions are discoverable through the Public Transmission Library, the Archive Explorer (Chapter 24.1), and appear as Transmission nodes on the Traceability Map (Chapter 24.3). A Collection may also include a Transmission as a governed member, following the same membership model described in Chapter 21.

What Transmissions are not

This feature does not add email sending, mailbox integration, messaging, notifications, reply threading, or correspondence storage. It does not create duplicate document storage or derived documents, and it does not redesign the existing intake, review, approval, or publication workflow described in Chapters 4–7. The distinct roles of a communication wrapper, an attached letter, a reply, and a read receipt (Chapter 9) remain independently governed objects — a Transmission simply gives the communication event itself its own governed identity, rather than leaving it implicit in separate document notes.

26.5 Document Identifier on intake (v13.0.5)

Every governed Document now receives a CDE-assigned, immutable Document Identifier in the form DOC-YYYY-NNNNNN at the moment of New Document Intake, before the initial Pending Intake lifecycle event is even recorded. This identifier is mandatory and permanent, and is distinct from the optional external Reference Identifier described in Chapter 5.7 — a blank external reference remains entirely valid, because the Document Identifier is the governed Document's own intrinsic identity, not a substitute for a source-assigned number. Existing documents that predate this change have been backfilled safely, without replacing any identifier already present.

26.6 Reusable note templates — Transmissions

Transmission — public note pattern

Records the communication of [governed object(s)] as [covering communication type] on [date]. Preserves the communication context without extending the evidential scope of any included object.

Transmission — administrative note pattern

Transmission Intake for [covering communication type], dated [date], including [governed object(s)] in [order/role]. This entry records communication context only; each included object retains its own independent lifecycle, provenance, and verification state.

27. Updated Quality-Control Checklists and Operating Sequence

27.1 Before extended-format intake

- ☐ Correct format confirmed by inspection, not filename
- ☐ Spreadsheet: not macro-enabled, encrypted, or malformed
- ☐ Image: original file preserved, not a re-capture
- ☐ Audio: original recording preserved, not re-encoded
- ☐ Keywords are source-grounded

27.2 Before creating an association (searchable selector)

- ☐ Correct public record confirmed in the context panel before selecting
- ☐ Correct Published document confirmed where several share a date or subject
- ☐ Relationship type, public label, public note, and administrative note all completed
- ☐ No claim exceeds either object's independent evidential boundary

27.3 Before creating or publishing a collection

- ☐ Collection reference and purpose clearly stated
- ☐ Each membership reviewed, approved, and activated individually
- ☐ Sequence positions checked for gaps or duplicates before publication
- ☐ No document, record, or association identity duplicated into the collection

27.4 Before executing a Governed Intake Correction

- ☐ Original archived intake and its full history reviewed
- ☐ Correction has passed Draft, Under Review, and Reviewed stages
- ☐ Correction has been explicitly Authorised before execution
- ☐ New destination intake understood to require its own full review/approval/publication

27.5 Before publishing a Transmission

- ☐ Covering communication metadata and sender/recipient model complete
- ☐ All included governed objects reviewed in their intended order
- ☐ Public note and administrative note describe communication context only
- ☐ No included object's evidential scope has been extended by the Transmission

27.6 Updated recommended operating sequence

36. Complete the Part I intake-through-association sequence for each independent artefact.
37. Where the artefact is an image, audio file, spreadsheet, or RTF document, apply the format-specific checks in 17.3 before storing as Pending.
38. Use the Administrative Audit page to confirm chronology before relying on a document in a new association or Transmission.
39. Create associations through the searchable record selector, confirming the context panel before submission.
40. Group related published objects into an Archive Collection only where a governed, ordered public presentation adds genuine value beyond individual publication.
41. If a document's metadata was assigned incorrectly after archiving, use Governed Intake Correction rather than editing the archived record.
42. Assign the correct canonical record_type when creating new records, and use “Create canonical record from this document” only as a starting point for review, not as an automatic transcription.
43. Where a communication event itself needs its own public identity, create a Governed Public Transmission rather than relying on document notes alone.
44. Preserve errors and corrections through governance — Intake Correction, superseding objects, or explanatory association — rather than silent rewriting, exactly as in Part I.

Each object should explain itself. Each transition should explain why it occurred. Each relationship should explain why it exists.

CIVIC DECISION ENGINE

Trust begins with structure.