

2.01 Acceptable Use of Electronic & Digital Signature Policy & Procedures

Document Owner	Executive Director Corporate & Commercial Services
Responsible Officers	Manager Governance & Risk
Date of Approval	12/03/2026
Amended/Revised/Revised	14/05/2026

1. Objective

To establish a clear, lawful and auditable framework for using electronic, digital and scanned (digitised) signatures in City of Albany documents and transactions, ensuring statutory compliance, secure recordkeeping, and appropriate delegation.

2. Scope

This Policy applies to all City of Albany officers, employees, contractors, consultants and authorised agents who prepare, approve, sign or issue documents on behalf of the City.

3. Policy Statement

The City promotes the use of electronic and digital signatures to improve organisational efficiency and service delivery where permitted by law and consistent with risk and governance requirements.

Electronic and digital signatures may be used only if:

- The transaction is permitted under applicable legislation.
- The signature method is appropriate to the transaction's risk and legal significance.
- The signatory has appropriate delegated or authorised authority.
- Adequate security, audit and recordkeeping controls exist.

Where legislation, agreement or best-practice governance requires a Common Seal or manual execution (wet signature), such requirements must be followed.

4. Legislative Authority

4.1 Local Government Act 1995 (WA)

The Local Government Act 1995 (WA) provides the framework for delegations, common seal execution, and authentication of documents. Officers may authenticate documents without the Common Seal if signed by the CEO or an authorised officer unless the Act or another law requires the Common Seal. (albany.wa.gov.au)

4.2 Electronic Transactions Act 2011 (WA)

Under the Electronic Transactions Act 2011 (WA), a requirement for writing or signature can be satisfied electronically where:

- A method identifies the person and indicates their intention;
- The method is reliable and suitable for the transaction's purpose; and
- The parties' consent to electronic execution.

Electronic execution is not permitted where excluded by law.

4.3 State Records Act 2000 (WA)

All signed documents and associated audit records are official records and must be captured, retained and managed in accordance with the State Records Act 2000 (WA) and the City's Recordkeeping Plan.

4.4 Privacy and Responsible Information Sharing Act 2024 (WA)

When signature processes involve personal information, compliance with applicable Information Privacy Principles and responsible information-sharing obligations is required.

5. Core Principles

- **Authority:** Only officers with current written delegation may sign or issue documents. Delegated authority must:
 - Be formally recorded in the City's Delegation Register;
 - Align with the officer's approved Position Description and assigned duties;
 - Be exercised strictly within any conditions or limitations of the delegation; and
 - Be supported by system access controls consistent with the delegation.
- **Accountability:** Signature actions must be attributable to an identifiable person and system user.
- **Security:** Signature methods must prevent unauthorised use or alteration.
- **Auditability:** Signature processes must leave an auditable trail.
- **Proportionality:** Signature type must align with risk.
- **Privacy:** Personal information must be protected.

6. Definitions

- **Electronic Signature (eSignature):** A typed name or email signature block indicating intent to sign.
- **Digital Signature:** A cryptographic signature applied through approved tools that verifies identity and document integrity.
- **Scanned (Digitised) Signature:** An image of a handwritten (wet) signature captured or reproduced electronically and applied to a document, excluding system-generated execution markers or system attestations that identify the authorised user through secure authentication and audit logging rather than signature imagery.
- **Approved Secure System:** A City-approved system with individual authentication, role controls, and audit logging.

7. Acceptable Signature Types

7.1 Electronic Signatures

Suitable for low to medium risk, where formal execution is not required and where legally permissible.

7.2 Digital Signatures

Required where:

- Legislation or regulation mandates it;
- Higher assurance, integrity or non-repudiation is needed; or
- The transaction involves significant legal, financial or reputational risk.

7.3 Scanned Signatures – Restricted Use

Permitted only when all conditions are met:

- Applied within an Approved Secure System;
- User authentication and role access match delegated authority;
- The system records a full audit trail;
- The image cannot be extracted or reused outside the system.

Scanned signatures must not be pasted manually into documents or used as standalone image files.

This restriction does not apply to documents generated and issued through a City-approved protected system that automates document creation and execution (including infringement notices), where:

- the issuing officer is authenticated through secure system access;
- authority is enforced through role-based controls aligned to delegation; and
- the system maintains a complete audit trail identifying the officer responsible for issuing the document.

In such cases, execution is evidenced by system authentication and audit records rather than a reproduced handwritten signature.

8. Execution Under Common Seal

8.1 General Requirements

Where a document requires sealing under legislation, Council resolution, agreement, or under the City's current **Common Seal Policy & Guidelines (1.62)**, the Common Seal must be affixed in line with that Policy. (albany.wa.gov.au)

8.2 When Common Seal is Required

The Common Seal must be affixed to documents including but not limited to:

- Local Laws and Scheme amendments;
- Land transactions (sales, leases, transfers, mortgages, caveats, etc.);
- Agreements requiring sealing under funding or legal instruments; and
- Any instrument where law or Council resolution expressly requires sealing. (albany.wa.gov.au)

Where sealing is not required, the CEO or authorised officer may authenticate documents under delegation. (albany.wa.gov.au)

8.3 Method of Sealing

Sealing must follow the procedures and witness requirements in the City's Common Seal Policy & Guidelines, including:

- Presence of the Mayor (or Deputy Mayor) and the CEO (or delegate);
- Record of the sealed document in the Common Seal Register;
- Registration of the sealed instrument in official records. (albany.wa.gov.au)

9. Governance & Recordkeeping

- Signature authority must align with written delegations.
- Systems must align access to delegation.
- All signed outputs and audit logs must be retained under the recordkeeping plan.
- Exceptions require Executive Director approval.
- Non-compliance may result in disciplinary action.

Delegations must be exercised only where:

- The function forms part of the officer's approved Position Description;
- The delegation is current and recorded in the City's Delegation Register;
- The officer has completed any required training or induction relevant to the delegated function.

Delegation must not be exercised outside assigned duties without formal written variation to role responsibilities.

10. Review

This Policy will be reviewed annually or sooner if legislative, technological, or operational change requires.

2.01 Acceptable Use of Electronic, Digital & Scanned Signatures Procedure

1. Purpose

To support the Policy by providing clear operational steps to select and apply appropriate signatures, including controls for Common Seal and statutory instruments.

2. Scope

This Procedure applies to all City officers, employees and authorised agents who sign or issue documents on behalf of the City.

3. Legislative & Governance Basis

- Electronic signatures may satisfy statutory signature requirements under the Electronic Transactions Act 2011 (WA).
- Delegated authority must be confirmed before signing.
- All signed records and audit logs must be captured under the State Records Act 2000 (WA).
- Where personal information is involved, privacy obligations under the Privacy and Responsible Information Sharing Act 2024 (WA) apply.

4. Definitions

As per Policy Section 6, plus:

- **Record Number:** The official record system identifier assigned when registered.

5. Roles & Responsibilities

5.1 Executive Directors

Ensure directorate compliance and approve permitted exceptions.

5.2 Manager Governance & Risk

Maintain Policy and Procedure; provide advice.

5.3 ICT

Maintain Approved Secure Systems and controls.

5.4 Managers

Ensure system roles match delegation and provide training.

5.5 Users

Use only approved signature methods and capture signed outputs into official records.

6. Simplified Execution Process

Step 1 – Identify the Transaction

Before signing, determine:

- Is the transaction **internal or external**?
- What is the **risk level** (low / medium / high)?
- Does the document require:
 - The **Common Seal**?
 - Statutory execution?
 - A deed or land instrument?

Consider:

- Legal effect
- Financial value
- External or funding requirements
- Any legislative signing conditions

If unsure, seek Governance advice before proceeding.

Step 2 – Confirm Authority

Before signing, confirm:

- The function aligns with your approved Position Description and assigned duties; and/or
- You hold a current written delegation or authorisation under the Local Government Act 1995 (WA);
- The delegation is recorded in the City's Delegation & Authorisation Registers;
- You are acting within any conditions or limits of the delegation/authorisation. ‘

Do not sign if authority is unclear.

Step 3 – Select the Appropriate Signature Method

Choose the method that matches the risk and legal requirement:

Situation	Signature Method
Low risk	Electronic
Medium risk	Electronic or Digital
High risk	Digital
Deed / Land / Statutory / Required by Council	Common Seal

Scanned (digitised) signatures may only be used within an Approved Secure System and do not include system-generated execution or attestation used by protected, auditable statutory systems (e.g. infringement notice systems).

Step 4 – Confirm External Acceptance (if applicable)

For external electronic execution:

- Confirm the other party accepts electronic signing;
- Preferably obtain written confirmation.

Step 5 – Execute and Register

Electronic Signature

- Apply via approved City system or email block.
- Register the signed document in the recordkeeping system.

Digital Signature

- Apply using approved signing software.
- Register the final signed version.

Statutory notices generated through a protected, automated system (e.g. infringement notices) may be issued without a handwritten or reproduced signature image, where system controls provide identity, authority, and auditability.

Scanned Signature (Restricted Use)

- Apply only within an Approved Secure System.
- Ensure audit logging is active.
- Register the final output.

Common Seal

- Follow the City's Common Seal Policy.
- Ensure required witnesses are present.
- Record the document in the Common Seal Register.
- Register the executed document in the record system.

7. System & Security Controls

Approved Secure Systems must:

- Support unique user accounts;
- Implement role-based access aligned to delegation;
- Enable audit logging of signing activity;
- Manage retention per recordkeeping requirements.

8. Recordkeeping

- Register signed documents in the record system.
- Protect audit logs for retrieval if required.
- Do not alter signed records; if corrected, issue a new version and retain originals.

9. Exceptions

Any exception to this Procedure requires Executive Director approval.

10. Data Breaches

Report suspected or actual breaches involving signature systems under the City's data breach response process and legislative obligations.