



E-Signing Policy

1.0 Introduction

- 1.1 Electronic signing is the creation, recording, and transmission of signatures in electronic format such as emails, web forms, and on electronic devices. It fulfils the same function as handwritten signatures (wet signatures). Both methods of signing are valid, legally binding, and signify that a person adding their signature has agreed to the terms in the document they are signing.
- 1.2 This Policy and supporting guidance is aligned with the [Electronic Communications Act 2000](#) which provides a statutory framework for the admissibility of electronic signatures in England and Wales. This Policy sets out Southern Housing's approach for the acceptable use of electronic signatures and applies to the following individuals:
- Southern Housing employees (whether permanent, temporary, full-time, or part-time)
 - Agency staff, contractors, or other people/organisations representing Southern Housing and its subsidiaries
 - Those providing services under a contract or other agreement with Southern Housing.

1.3 Definition of terms

We means Southern Housing ('SH').

E-signing or e-signature means electronic signing of documents.

2.0 Policy requirements

2.1 Use of e-signatures

Electronic signatures can take several forms, and we have grouped these into:

Digital signatures – this is an advanced electronic, encrypted, stamp of a signature created via secure platforms such as DocuSign or Adobe. It is uniquely linked to the signatory and capable of identifying the signer. Digital signatures benefit from increased security and reliability.

Non digital signatures¹ – this constitutes a simple application of an electronic signature outside a secure platform.

¹ Also referred to as 'standard electronic signatures'

Some examples of these are:

- Typing a name into a contract document or the bottom of an email containing the terms of a contract
- Inserting a signature image into an electronic document
- Using e-pens or a finger to sign a name or signature on a device
- Clicking 'I accept' on a website.

2.2 An e-signature can be used to obtain consent or approval on electronic documents. This means there is no need to print the document. The e-signature replaces a handwritten signature.

2.3 SH accepts electronically signed documents (digital and non-digital signatures) as legally binding and having the same legal value as handwritten signatures (wet signatures).

2.4 This Policy does not limit SH's right or option to conduct transactions on paper or in a non-electronic form, nor affect SH's right or obligation to have documents provided or made available in paper format when required by legislation or regulation.

3.0 Internal documents and transactions

3.1 Most internal documents, such as simple contracts, forms, letters, invoices, minutes, and credit card statements can be signed using non-digital signatures such as inserting a signature image or typing a name into a document.

4.0 External documents and transactions

4.1 SH accepts the electronic submission of external documents or transactions bearing an electronic signature if it is deemed to be compliant with this Policy.

4.2 Digital signing using a secure platform such as DocuSign should be used for high value, complex transactions, or contract signing.

5.0 Documents excluded

5.1 E-signatures (digital and non-digital) must not be used in documents where there is a regulatory, legal requirement or a specific reason for a handwritten signature, including but not limited to:

- Signing of a deed, powers of attorney or contract where a handwritten signature is required (refer to the Governance Signing Guidance)
- The third-party e.g. a resident is unable to sign electronically
- The third-party will only accept a handwritten signature.

6.0 General consent

6.1 As with handwritten signatures, signers must show clear intent to sign a document electronically.

- 6.2 No individual should be compelled or required to transact with SH using electronic signatures without their consent. If a handwritten signature (wet signature) is requested, we should consent.
- 6.3 Employees organising the signing process (digital or non-digital) should obtain appropriate authorisations from signatories prior to processing documents.
- 6.4 Where digital signatures are used in secure platforms and the document has been signed/authorised, no further changes will be possible. If changes are required, the document must be voided and re-uploaded to the platform.
- 6.5 Where an employee believes that a misrepresentation has occurred, the electronic submission or transaction should not be processed, and the respective signatory should be notified.

7.0 Document retention

- 7.1 An electronically signed record constitutes the original copy of the said record and should be maintained, accessible, and reproducible in an accurate format.
- 7.2 A digital signing platform such as DocuSign will automatically provide signed copies of documents to signers as part of the approval workflow.
- 7.3 When signing outside a digital platform, employees processing the document must retain the respective approval and signed records and reproduce this when required.
- 7.4 Electronically signed records must be retained in accordance with the *Document and Data Retention Policy*.

8.0 Responsibilities

- 8.1 Teams using e-signing will be responsible for:
- Determining and categorising documents that can be signed electronically using either a non-digital or our digital signing platform i.e. DocuSign
 - Ensuring any documents approved using our digital signing platform meet legal, regulatory, and operational requirements
 - Amending respective team procedures to incorporate e-signing
 - Ensuring documents uploaded to the digital signing platform are downloaded to the relevant folder and/or internal platform in line with SH's *Document and Data Retention Schedule*.
- 8.2 The Director of Governance and Regulation is responsible for reviewing and updating this Policy.
- 8.3 This Policy shall be reviewed every two years to address legislative, regulatory, best practice, or operational issues.

Policy controls

Version 1.0 – effective 1 July 2024