THE FIRST FEDERATION TRUST

ELECTRONIC SIGNATURE POLICY

Adopted:	June 2025
Review cycle:	3 years
Next review due by:	June 2028

1. Introduction

1.1 The First Federation Trust (FFT) recognised that the introduction of electronic processes can improve efficiencies in work practices. This policy is concerned with use of electronic signatures. These can exist in many different forms and not just as digital images of hand-written signatures. The policy is to ensure that any individual or the FFT:

- Is not misrepresented;
- Does not suffers loss of reputation;
- Is not exposed to any liability or other adverse consequence through the unauthorised use of electronic signatures.

1.2. The FFT has a duty to meet local and national requirements in relation to the security and integrity of information. As the FFT requires electronic signatures which can be used in place of written signatures in order to increase the efficiency of its business processes, it is important that they fulfil the same functions as written signatures and provide the appropriate levels of authentication, integrity and non-repudiation to a document. This policy sets out the functional requirements for electronic signatures and defines acceptable uses of electronic signatures for signing documents, electronically as an equivalent to a handwritten signature.

2. Scope

2.1 This policy and associated procedures is targeted at all personnel who may act in some capacity as signatories on behalf of the FFT.

2.2 This policy operates in accordance with the existing framework of approvals and authorisation within the FFT, as set out in the Scheme of Delegation, financial regulations, the FFT Finance Policy and financial procedures, and other policies that may be relevant to the approval being provided. Any authorisation or approvals given in the form of electronic signatures under this policy are therefore subject to any authorisation limits and restrictions as set out elsewhere.

3. Definitions

3.1 Electronic signature. The legal definition of an "electronic signature" is anything in electronic form which is:

(a) Incorporated into or otherwise logically associated with any electronic communication or electronic data; and

(b) Purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of a communication or data, the integrity of the communication or data, or both.
Electronic Communications Act 2000 and Electronic Signatures Regulations 2002.

Non repudiation. In reference to digital security, non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

4. Duties

All staff have a responsibility to:

- Make themselves familiar with and adhere to this policy. Failure to comply may result in disciplinary action being taken.
- Bring to their line manager's or the Trust SLT's attention areas of concern regarding any issues associated with the use of electronic signatures.
- Where signatories are to be inserted 'on behalf of', authorisation should be obtained in writing, in advance, from the main signatory. This may be in the form of a general delegation of authority or a specific delegation covering a single instance. Verbal approval should be followed up by written approval as soon as possible. In exceptional circumstances, where time is of the essence, (including annual leave), per procurationem (p.p.) signatures may be added without explicit permission. As a minimum, the main signatory must be copied into the document, who should acknowledge receipt.

5. Types of Electronic Signatures

5.1 Electronic signatures can be captured by various types of equipment including scanners, photocopiers and mobile phones. Once acquired, signatures can be transmitted electronically and copied between files, as well as being printed on paper documents. An electronic document, such as an email or word file, containing a digitised signature is nowadays considered to be no different from a paper one which has been signed manually. It is therefore important that individuals use image of their own signature with care and that there are controls over the use of other people's digitised signatures.

From a legal perspective there is usually no need to include an image of a signature in a document. The (typed) text at the end of an email acts as a signature. This applies to standard FFT emails.

5.2 Electronic signatures can be divided into three groups:

1. **Simple electronic signatures** examples are a stylus or finger drawn signature, a typed name, a tick box and declaration, a unique representation of characters, scanned image of a signature and an automatic e-mail signature.

2. **Advanced electronic signatures -** these are uniquely linked to the signatory, are capable of identifying the signatory, allow the signatory to retain control, and are linked to data within the signature that can detect any changes made.

3. **Qualified electronic signatures** - an advanced electronic signature, uniquely linked to the signatory, that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

The use of 'advanced' or 'qualified' electronic signatures provides:

a. Authentication - the signatory can be linked to the information
b. Integrity - changes to the information can be detected more easily.
c. Non-repudiation - legal assurance regarding where the electronic signature has come from.

6. Requirements

6.1. Authorisation by email

An email from an individual user's FFT e-mail address can be used as an equivalent to a written signature for internal purposes where it meets the appropriate functional requirements. Responsibility for authorisations made by email remains with the email account holder unless the proxy is acting maliciously, fraudulently or negligently or unauthorised access to the account has been obtained in breach of the Computer Misuse Act 1990.

6.2. Scanned image of a handwritten signature

Scanned images of handwritten signatures should not generally be required for internal authorisations. However, a scanned image of a handwritten signature can be used as an equivalent to a written signature where it meets appropriate functional requirements.

Scanned images must only be used directly by the author, or where express permission has been granted by the author for such use. This could include e.g. adding a signature to an external letter or contract, or for high volume processing such as mass mailings.

Documents containing the image of another person's signature must not be sent without the express agreement of the person concerned, unless prior delegation and clearance procedures have been agreed. Responsibility of authorisation made by scanned signature remains with the signature's author, however the author will not be held responsible for any malicious, fraudulent or negligent activity carried out by the proxy. The proxy should therefore retain their own records of agreement for use of a signature in this way. In addition:

- Such agreement, including the list of recipients, must be obtained in advance for each document.
- The content of the document must not be changed after authorisation to issue it has been obtained.
- Once such a document has been sent, it must not be sent again (or to additional recipients) without further explicit authorisation.
- Scanned images of signatures must be kept securely to prevent unauthorised access and fraudulent use.
- Images of signatures should be used only when essential. Though it is only a small deterrent to copying images of signatures, they should be sent outside the Trust in pdf files rather than emails, word documents or spreadsheets. The pdf files should be created with the highest levels of protection.

6.3. Advance or qualified electronic signatures

Advance or qualified signatures may be required by third parties when greater assurance is required particularly for contractual signatures.

7. Other electronic transactions

Electronic transactions in a workflow or other software system, or authorised by other electronic means, have a validity equivalent to a signature in virtually all circumstances.

Staff should ensure that they are adopting appropriate security and reporting measures for these types of transactions.

8. Legal Impact of Electronic Signatures

It is possible to commit to contracts using electronic signatures

An electronic signature could be used in court as evidence of the Authenticity of the communication or document if it is separately confirmed that the signature is a means of authenticating the communication or document. (Section 7 of the Electronic Communications Act 2000).

9. Precautionary Measures

It should be noted that it is possible for e-mails to be "spoofed" of "high jacked" i.e. appear to be sent by someone other than the true sender, and for this reason a degree of caution needs to be exercised when accepting e-mails from third parties. Check the actual email address of the sender to help identify whether it is correct. If there is any doubt as to the authenticity of an electronic communication, it should in the first instance be reported to the Data Protection Officer and IT support (Computeam).

10. Adoption of the policy

This policy has been adopted by the board of directors of the First Federation Trust. It will be reviewed at least every three years.