

Electronic Signatures – Keeping them secure

Electronic documents and signatures

The use of electronic documents and signatures has become common and popular practice with the use of emails, digital word-processing, document digitisation and electronic signature tools. This should only grow with the advent of mobile computing devices and applications and the various online and cloud-based document management and collaboration software tools. However, while these tools offer convenience, usability and efficiency, as well as ways to connect with new groups and individuals, such benefits have to be balanced against security concerns and the need to uphold the legitimacy of the document and the decision-making/approval process so as to ensure the document or decision is legally effective.

An electronic signature (or e-signature) is any electronic indication (e.g. sound, image, process) attached to (or logically associated with) something as an intent to sign or approve it.

A digital signature is an advanced type of electronic signature using software technology intended to deliver reliability, authenticity and integrity through a coded message unique to the signer and document. Once signed, the document cannot be altered without invalidating the digital signature.

Under Australian Federal and State laws, a transaction will not be considered invalid simply because it was completed electronically. An electronic or digital signature can be treated just the same as an ink signature on paper.

Contract formation and decision-making

Most ordinary contracts and decisions do not have to be in writing or signed by a hand-written or “wet” signature to be legally effective. To form a contract, you need an agreement (offer and acceptance), the intention to create binding legal relations, transfer of consideration (money or value) between the parties in exchange for an undertaking by the other party to do or not do something, and certainty of what the terms are. For other documents, you may need to comply with the required decision-making procedures. Decisions on behalf of organisations or government bodies generally require a decision to have been made by an authorised decision-maker exercising a delegated decision-making authority within the scope of their office/authority, having turned their minds to the relevant facts and criteria to form that decision. There may also be stipulated procedures or conditions to comply with.

As long as these conditions are satisfied, generally (subject to certain exceptions where legislation or policy imposes requirements of written or physical evidence) it will not matter whether the agreement or decision is evidenced in a physical or virtual form for it to be legally valid. The need for formal documentation and some form of signature or authentication is more a question of being able to provide evidence to prove and enforce what was agreed or decided. This will obviously be more difficult if you cannot provide documentary evidence of what was ultimately agreed or decided, or put in place sufficient security protections to prevent the document from being subsequently changed or falsified (or accessed by unauthorised parties).

Validity

Whatever form of signature is chosen, it must be adequate to establish that the person(s) purporting to enter the agreement or make the decision means to do so and to authenticate that that person was the person who actually did so.

It is also important that the integrity of the document can be established from the time it was created, so it can be proved that the document reflects what was agreed.

It is therefore essential to keep good records to authenticate what was agreed, by whom and when, what changes or amendments have been made, when and why, and the relevant parties' acceptance or approval of the final authoritative document. Once 'signed', the document should be stored securely in a manner which would prevent anyone from accessing and making subsequent changes to the document which haven't been agreed or otherwise falsifying the document.

Security of Electronic Signatures

An electronic or digital signature should only be used to sign a document by the person who the signature (or user ID) actually belongs to. Individuals should ensure that they do not make their electronic signature or their digital signature login credentials available to others for use. However, as long as authorised users of a digital signature don't share their login details, a digital signature software's access requirements, certifications and tracking of user logins and other activities can actually make the document more secure and easy to validate than using hand-written signatures or scanned electronic signatures, both of which can be falsified. Once an individual has signed a document electronically, it would also be good practice to convert the document to a PDF file and apply security or editing protections on the document to minimise the chance of unauthorised copying of the signature or editing of the document, and to upload the document, and any other relevant evidence, to some form of records management software tool (with similar access/editing protections) to protect against lost records or unauthorised access.

Advice for Website

We suggest using the following plain language summary of our advice on your website.

Electronic signatures are a valid form of signature. Generally speaking, it does not matter whether an agreement or decision is evidenced in a physical or virtual form for it to be legally valid. When signing a contract or document electronically, you could use:

- **Electronic Signature:** an electronic indication (e.g. sound, image, process) attached to (or logically associate with) something as an intent to sign or approve it; or
- **Digital Signature:** an advanced type of electronic signature using software technology intended to deliver reliability, authenticity and integrity through a coded message unique to the signer and document. Once signed, the document cannot be altered without invalidating the digital signature.

If signing electronically, it is still important that you can provide evidence of what was agreed or decided, and that you can prove the integrity of the document or contract from the time it was created (e.g. that the document was stored securely and hasn't been changed).

You must also be able to establish that the person who is entering the agreement or making the decision actually means to do so and to authenticate that that person was the person who actually did so. Once 'signed', the document should be stored securely in a manner which would prevent anyone from accessing and making subsequent changes to the document which haven't been agreed or otherwise falsifying the document.

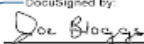
An electronic or digital signature should only be used to sign a document by the person who the signature (or user ID) actually belongs to. Individuals should ensure that they do not make their electronic signature or their digital signature login credentials available to others for use.

Here is an example of digital signatures:

Execution page

Executed as an agreement

Signed for Joe Bloggs Inc. by its authorised representative:

DocuSigned by:


Signature of authorised representative

Joe Bloggs

Name of authorised representative (please print)

04-May-2016

Date:

Signed for Jane Doe Ltd. by its authorised representative:

DocuSigned by:


Signature of authorised representative

Jane Doe

Name of authorised representative (please print)

04-May-2016

Date:

Applicable Legislation

- [Electronic Transactions Act 1999 \(Cth\)](#)
- [Electronic Transactions Act 2001 \(ACT\)](#)
- [Electronic Transactions \(Northern Territory\) Act 2000 \(NT\)](#)
- [Electronic Transactions Act 2000 \(NSW\)](#)
- [Electronic Transactions \(Queensland\) Act 2001 \(Qld\)](#)
- [Electronic Transactions Act 2000 \(SA\)](#)
- [Electronic Transactions Act 2000 \(Tas\)](#)
- [Electronic Transactions \(Victoria\) Act 2000 \(Vic\)](#)
- [Electronic Transactions Act 2011 \(WA\)](#)

The above links were accessible on 14 June 2016, if broken go to the relevant parliamentary website.

NCOSS thanks Hewlett Packard Enterprise's in-house legal team for the above information, developed pro bono for the NSW Community Sector.