# Helpsheet: Electronic signatures

**Issued:** January 2021

**Last issued:** July 2024

**Last reviewed:** July 2024

## Introduction

The increased use of electronic communication, whether it be email or dedicated portals or cloud storage, coupled with an increasingly mobile workforce, flexible working arrangements and client relationships which are geographically agnostic presents logistical challenges for obtaining signed documents for both the accountant and client.

As a result obtaining handwritten ‘wet’ signatures can be inconvenient and time consuming and electronic signatures may be more convenient.

There has been some uncertainty around the legal status of electronic signatures and whether they are permitted to be used in relation to the signing of accounts, reports and other documents typically found in an accountancy practice. This helpsheet provides information on the legal status of electronic signatures, explains the different types of electronic signatures and considers aspects relating to the use of electronic signature platforms.

This helpsheet should be read in conjunction with the helpsheet on signing off accounts, reports and other documents which provides information on specific signing requirements as well as more general matters for consideration in relation to signing (see [Useful links](#_Useful_links)).

## The legal status of electronic signatures

There are two issues which require consideration:

1. which documents are capable of electronic signature.
2. where electronic signatures are permitted what are the characteristics of the electronic signature for it to be valid.

Historically there has been some considerable doubt about which documents require a ‘wet signature’ and whether an electronic signature is capable of being used in certain circumstances. Within the UK, this has further been complicated by the different legal jurisdictions which make up the UK.

In Scots law, the [Requirements of Writing (Scotland) Act 1995](https://www.legislation.gov.uk/ukpga/1995/7/section/1) (the 1995 Act) requires certain documents that must be signed on paper such as wills and other testamentary documents. As a result these can only be signed using a ‘wet signature’.

The 1995 Act also requires certain other documents to be made ‘in writing’ such as documents dealing with interests in land and some trusts and guarantees. If these documents are signed electronically then they must be signed via advanced methods or, for property documents, qualified electronic signatures. It is therefore not possible to electronically sign those types of agreements using a simple electronic signature.

Where a document type is not covered by the 1995 Act, the general position is that documents can be validly signed using either a ‘wet signature’ or an electronic signature.

In England and Wales, a [Law Commission report](https://www.lawcom.gov.uk/electronic-signatures-are-valid-confirms-law-commission/) into electronic signatures, issued in September 2019, has provided some clarity and comfort into the use of electronic signatures. The report took into account EU law, UK legislation and case law and confirmed that electronic signatures can be used as an alternative to handwritten ones, including where there is a statutory requirement for a signature.

“Electronic signatures can offer quicker and easier transactions for businesses and consumers. Our report aims to provide an accessible statement of the law which makes it clear that an electronic signature can generally be used in place of a handwritten signature as long as the usual rules on signatures are met.” Commercial and Common Law Commissioner, Stephen Lewis.

An electronic signature is therefore capable in law of being used to execute a document, provided that the signatory intends to authenticate the document. The UK government acknowledged the Law Commission’s report in [its announcement on 3 March 2020](https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2020-03-03/HCWS143/) and agreed that electronic signatures have a legal basis.

### Other legal considerations

Further legal provisions concerning the use of electronic signatures within the UK are contained in the [Electronic Communications Act 2000](https://www.legislation.gov.uk/ukpga/2000/7/contents) and the UK eIDAS Regulations. The legislation provides that an e-signature has the same legal standing as a handwritten signature in most situations.

The UK eIDAS Regulations sets out rules for UK trust services and establishes a legal framework for the provision and effect of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

Whilst electronic signatures are recognised as signatures under the law, they cannot all necessarily be relied upon, particularly in business transactions as there may be times that it is necessary to determine whether there is an ‘intention to authenticate’.

### Regulatory requirements

UK legislation and regulation can specify further requirements regarding signatures. for example, HMRC, Companies House and the Land Registry expressly require handwritten signatures for certain forms and other documents.

## Types of electronic signatures

An electronic signature is using some form of electronic data to sign, or otherwise signify agreement or consent, as an equivalent to a signature. However, not all electronic signatures are equal, with different types of signatures having different effects.

There are three types of electronic signature, recognised by eIDAS, as follows:

### Simple

The most commonly encountered e-signatures will be ‘simple’. These include scanned manuscript signatures, using a finger or stylus to sign on a screen, clicking an onscreen button such as ‘I agree’ or ‘submit’ and by using a PIN with your bank card for example. Simple electronic signatures are the easiest to use, but the least secure as there is no clear evidence of who the signatory was.

Other sophisticated types of electronic signature include Adobe Sign or DocuSign, that use a signing platform, which provide greater reliability but still lack an ability to link them to the actual signatory. The use of these are becoming more prevalent particularly where the need to be ‘self-proving’ is not strictly necessary.

### Advanced

These are uniquely linked to the signatory, and are encrypted and time stamped, so you can identify them by the individual ID. This helps ensure that the signatory can only have been the individual from whom the signature was requested. They offer a higher level of security but are more costly as they require use of a third-party digital signing software platform.

### Qualified

These offer the most security but are the most complex. To be authenticated, the electronic signature requires a ‘qualified certificate’ which contains verification information and be provided by a trusted provider in order to fulfil various requirements as set out in EU regulation. There is little evidence of these being used in practice currently due to their impracticability.

Advanced and qualified electronic signatures therefore have an advantage as their digital audit trails provide better evidence of the intention to authenticate the document than simple electronic signatures, since only the named individual is able to use them.

What is important to note is that there is no equivalent to ‘witnessing’ when it comes to electronic signatures. So, if someone were to apply an electronic signature in the presence of another person, who also applies an electronic signature, as a ‘witness’, it would not confer self-proving status to that document or be legally valid. Only a qualified signature can confer self-proving status in Scotland, since rather than a witness providing the assurance it comes from the authentication in the qualified signature.

This would be crucial in the case of a contract being used in court proceedings as only a qualified electronic signature will be presumed to have been signed by the requested signatory whereas a simple or advanced electronic signature may require further evidence to prove that the signatory did in fact sign the electronic document.

## Electronic signature platforms

Many electronic signature platforms are now able to establish enough evidence to prove intention, should someone later dispute the validity of the contract. These platforms allow you to upload and set-up a document for signing via a secure cloud-based environment, bypassing the problems associated with manual signing of documents. They assist in verification of you or a third party’s signature by allowing the download of a certificate from the platform provider.

Usually, access is granted to the document via a link sent between parties which may also be PIN protected, for added security. Once signed, the platform captures information such as the signatories email address, IP address and the date and time of access. Once complete, the document is then circulated as a read-only PDF, highlighting if any alterations have been made.

The benefit of using such platforms is that they offer a greater degree of control and collate evidence of an ‘intention’ to sign the document when compared to other simple electronic signatures. Electronic signature platforms typically use language that indicates to the signatory that by applying their signature they are agreeing to the terms. Therefore, the electronic platform and associated email narrative that would usually surround legal completion can produce sufficient evidence to demonstration an intention, on the part of the signatory, to enter into the contract.

## Practical considerations

Before deciding to use electronic signatures, it might be useful to think about a number of further practical considerations as follows:

* Which form of signature is accepted by any regulator (if applicable)? It may be advisable to check with the regulator to ascertain whether electronic signatures are accepted.
* Which form of signature is the most practical for your firm? It may be that signing the accounts by hand and coordinating by post is a perfectly acceptable option if there is less time pressure, and these are processes that everyone is used to. If there are quality management procedures over ‘wet ink’ signing that are established, then you may wish to continue in this way. Sometimes, adopting a more complex solution may just take more time and add complexity to the process.
* If advanced or qualified electronic signatures are considered, cost will have to be weighed up against the benefits of higher levels of security and greater expedience. Which level of security is right for the cost? Is a qualified electronic signature really needed, or will an advanced electronic signature suffice where a higher level of security is deemed necessary?
* Simple electronic signatures may be lower in cost than handwritten signatures, given potential savings on paper, ink and postage, and savings on physical storage, so might it be worth changing the process?
* If an advanced or qualified signature platform is being adopted, will training need to be arranged for the partners or other Responsible Individuals who will be using it?
* What would be acceptable to your insurers? Are there any clauses in your professional indemnity cover which specify that handwritten signatures are required, for example?
* What would be your client’s preference? Some electronic solutions may require clients to adopt the same software as the firm so the cost, and who will be incurring it, might then need to be considered.
* If there is a reluctance to use electronic signatures, is this based on preconceptions that electronic signatures may be more susceptible to fraud than handwritten signatures? Those who are intent on committing fraud, may still find a way - even with wet ink signatures. In some respects, even a simple electronic signature can be more secure than handwritten signatures with an appropriate audit trail.
* Using handwritten signatures via the post may also give rise to further risks. These might include postal service or courier delays affecting the timely delivery of the signed annual report and financial statements (and management representation letter), and the need for partners to provide details of their home address, which in itself gives greater security and data protection risks.
* If a simple electronic signature is being used for the first time but the individual has no access to a scanner at home, a digital photo of their signature may be considered instead.

## Risk Management

If electronic signatures are used then policies and procedures should be established to mitigate some of the risks associated with their use. This will include for example:

* Controls to ensure that only authorised persons have access to electronic signatures and their application, particularly where simple electronic signatures are being used
* Controls to ensure that the electronic signature is only applied to the final version of any document
* If simple electronic signatures are to be used and the signature is likely to be available publicly, consideration should be given to the use of a ‘professional signature’. This would be a distinct signature of a person which is only used in connection with public documents which may mitigate against the risk of an individuals signature being copied and used for fraudulent purposes.

## Use of electronic signatures with accounts and audit reports

Requirements for the annual report and financial statements may vary according to the regulatory environment of the entity, but usually the directors’ report/strategic report and the balance sheet must be signed by a director, and the auditor’s report by the senior statutory auditor.

The Companies Act 2006 does not specifically make reference to ‘electronic signatures’ but rather states that the auditor’s report must be ‘signed’. Since UK law has generally recognised the validity of a wide range of electronic signatures, and the kind of signature is not specifically stipulated in the Companies Act 2006, it does leave it open to interpretation.

What is important is that the ‘intention to authenticate’ should be evidenced to give a robust audit trail. For example, the auditor may consider including wording in an email to the client, with the signed auditor’s report attached, to ask them to confirm that they have signed the report and consider including that on the audit file.

[ISA 700 (UK)](https://www.frc.org.uk/getattachment/a08b0906-f40c-4735-bbc7-45908bee2b32/ISA-%28UK%29-700_Revised-June-2016.pdf) also refers to Section 503(3) of the Companies Act 2006 which states that the senior statutory auditor must sign the auditor’s report so another audit partner or responsible individual cannot sign for and on behalf of the senior statutory auditor. The standard does acknowledge that there may be circumstances where the senior statutory auditor is absent but is still able to take responsibility for the direction, supervision and performance of the audit. In this instance, ISA 700 (UK) states that the senior statutory auditor may sign the auditor’s report using electronic means such as e-mail or fax.

In addition to the practical considerations noted above, if electronic signatures are adopted for the first time, it might be beneficial to update the quality management procedures by considering the following:

* Controls should be in place to ensure that only the audit partner holds their simple electronic signature so no one else can use it on their behalf. If a simple electronic signature is held by another person to be applied under the audit partner’s specific authority, are there controls in place to ensure the signature is not used without this authority?
* Where a simple electronic signature is being used to sign the auditor’s report, intention to authenticate may be better demonstrated if the audit partner confirms their intention to sign when responding to their client with the signed auditor’s report (with the annual report and financial statements). This will provide a clear evidence trail of the intentions to authenticate if authenticity of electronic signatures is subsequently challenged and may also help protect against fraudulent use of signatures.
* If the entity’s constitutional documents do not specify how the annual report and financial statements must be signed, electronic signatures are presumed to be valid, unless the contrary can be proven. If the directors, or equivalent, of the audited entity are choosing to sign the annual report and financial statements with a simple electronic signature, the auditor may wish to obtain evidence directly by email that those directors provided the signatures themselves, as evidence to authenticate. As with ‘wet ink’ signing, the auditor should still check that the directors, have signed the annual report and financial statements prior to the auditor signing the auditor’s report, and that the directors were able to do so. The directors may sign using a different mode of signature to the auditor, for example one by ‘wet ink’ signature and one by simple electronic signature. However, if either is signing using an advanced or qualified electronic signature, it is likely the other will also have to as it will be enforced by the software platform.
* Many firms maintain electronic audit files, and archive audit files electronically. Are there procedures in place to ensure the client and the audit file have copies of the ‘original’ annual report and financial statements?
* It is not just fraud, but also error, that should be considered – is there a risk that an electronic signature is released too early? What procedures are in place to ensure a signature is only used on the final version that would have been signed by hand?

To conclude, the use of electronic signatures on audit reports appears to be acceptable provided provisions are in place in accordance with legislation and that audit partners meet the guidance in [ISA (UK) 700](https://www.frc.org.uk/getattachment/a08b0906-f40c-4735-bbc7-45908bee2b32/ISA-%28UK%29-700_Revised-June-2016.pdf).

## Useful links

[Helpsheet: Signing off accounts, returns and other documents](https://www.icas.com/__data/assets/pdf_file/0016/2185/Signing-off-accounts-returns-and-other-documents-helpsheet.pdf)

[ICO: Guide to eIDAS](https://ico.org.uk/for-organisations/guide-to-eidas/)

## Further information and assistance

Further assistance and information can be obtained from the Practice Support team. You can contact them through the Practice Support section of the [ICAS Technical helpdesk](https://www.icas.com/contact-us/icas-technical-helpdesk).

Disclaimer:

This document has been published by ICAS for information purposes only and ICAS cannot accept responsibility for any person acting or refraining to act as a result of any material contained within this guidance. Recipients should make their own independent evaluation of this information and no action should be taken, solely relying on it. The document is intended to assist members in the general application of the subject, it is not intended to cover all aspects.

Whilst this information is believed to be reliable, ICAS, its employees and others involved in the production of this information do not provide any representation or warranty (express or implied) of any kind as regards the accuracy or completeness of this information, nor do they accept any responsibility or liability for loss or damage arising in any way from any use made of or reliance placed on this information.

All information is believed to be correct at the time of publication.