Using electronic signatures

This factsheet provides information to help you understand how the Department expects you to electronically sign or obtain an electronic signature on a document, including a table to show common methods for obtaining electronic signatures and some practical example scenarios.

An electronic action equivalent to a signature

This means an electronic method of obtaining a person's agreement or endorsement of information as an alternative to making an ink-based signature on paper.

For an 'electronic action equivalent to a signature' to meet the requirements in the Contract, you must use a method that satisfies the following main principles:

- **identity –** clearly identify the person undertaking the action.
- **consent –** clearly indicate the person's agreement to the relevant information.
- **reliability –** be 'as reliable as appropriate in light of all the circumstances' so that the Department can rely on the action as demonstrating the person's agreement at audit or review.

What 'as reliable as appropriate in light of all the circumstances' means

To decide what is 'as reliable as appropriate in light of all the circumstances', we would look at a range of matters such as:

- the nature of the information being agreed to or endorsed.
- the level of risk if an electronic signature was found to be invalid or unenforceable.
- the nature and extent of data being collected and stored (for example, copies of documents, the relevant audit trail and personal information to identify signatories).
- whether the method enables adequate protection from security risks, including both from within and from outside the training provider (for example, ensuring a person's identity cannot be misused or a document altered after it was electronically signed).

When you are deciding to use an electronic signature, you need to choose a method where the level of detail and risk management is proportionate to the action required in the Contract.

In general, the higher the risk of an invalid or unenforceable signature, or potential security breaches, the more robust an electronic method of collecting signatures needs to be.

When to use 'an electronic action equivalent to a signature'

Electronic signatures are acceptable for most documents that need to be signed to meet a Contract requirement, including your own signature, signatures of your employees or signatures of third parties such as students.

For example:

- Practical Placement agreements
- the Evidence of Eligibility and Student Declaration form
- teacher endorsement of an attendance roll for Evidence of Participation.

Published 14 December 2021 (version 1.2) *This document is a guide only and subject to change*

The only exceptions where you can't use an electronic signature are where it isn't appropriate because of the degree of legal formality of the document or the decision that requires signed agreement. Specifically, you can't use an electronic signature if:

- it binds you or the person signing it to a contract with the Department or an amendment to such a contract (this means an agreement outside of the normal terms and conditions of the Contract itself)
- it is on a formal 'Notice' issued under the Contract
- there is another law or regulatory obligation you have to comply with that says you can't use an electronic signature.

You should be aware that additional requirements apply to the making and delivery of a communication identified in the Contract as a 'Notice'. The Notice must be in writing, signed by a Party to the Contract and be delivered by hand or by prepaid priority post.

Accepted methods for collecting an electronic signature

We don't prescribe the methods that can be used or endorse particular commercial products that enable collection of electronic signatures, given this is an emerging area of technology. You'll need to research and investigate what's available and decide what will work best for your business.

We expect you to develop a business process/rationale when you choose to use electronic signatures and use methods that are proportionate to the risk level of what is being agreed to or endorsed. You'll also need to think about how to demonstrate at any audit or review that the method you have chosen is robust and appropriate to the circumstances.

The table on the next page identifies common methods for obtaining electronic signatures, with a rating of how robust we think they are in meeting the requirements of the Contract.

- Any of the methods described in the green box are considered to be sufficient on their own.
- The methods identified in the orange box may need to be combined with an additional method to be sufficiently robust, or may need to be supported by further, separate evidence that meets the three main principles (Identity, Consent and Reliability).
- You should not use any of the 'least robust' methods identified in the red box for the purpose of meeting any requirement of the Contract.

Published 14 December 2021 (version 1.2) *This document is a guide only and subject to change*

Common electronic methods for obtaining agreement/ endorsement

MOST ROBUST

Method	Application to Contract
• Graphical representation of a signature (for example, using an electronic pen or finger to make a signature directly onto an electronic device). • Encrypted codes (issuing a unique code or encryption key to a user and then requiring the user to enter the code when signing the relevant document by ticking a box and/or entering their name). • Use of an electronic signature program (commercially available programs that operate by sending a request for signature to a user's email address. The programs then require the user to authenticate their identity using a range of methods such as provision of an access code, SMS authentication, phone authentication or identity checks against publicly available information. The programs also keep electronic records of the application of signatures and use encryption technology to protect signed documents from unauthorised alteration).	A single one of these methods is likely to be robust for most purposes where an electronic signature is accepted under the Contract.
• Ticking a box in an online form. • Sending or receiving an email if it’s from an email address that is verified to belong to a particular person. For example, an email address from an employee of your training provider where they log in with a unique ID and password to use it, or an email from a student that you’ve recorded in their student file as their primary contact address. • Typing one's name in an online form. • Completing a step in an electronic workflow. • An ink-based signature that is scanned into an electronic format and cut and pasted into a document.	A combination of one or more of these methods might be needed for a higher risk application. For example, a student signature on the Evidence of Eligibility and Student Declaration form. A single one of these methods may be sufficient for lower risk applications, or for actions occurring within a secure system (i.e. within an online platform that includes both **authentication** [secure login] and **authorisation** [restricts particular actions to authorised users]).
• Phone conversation. • Text message.	These methods are not appropriate or sufficiently robust for application to any contractual requirement.

LEAST ROBUST

Example scenarios

Example 1: Fully online enrolment process

A training provider has implemented a fully online enrolment process. This process includes completing the Evidence of Eligibility and Student Declaration form electronically.

The online process has two separate parts:

- an online form that the student completes, which includes information required for testing Skills First eligibility and other mandatory enrolment questions
- the 'back-end' administrative process used by the training provider, where eligibility information is assessed and processed through a workflow.

Obtaining the student's signature

Given that checking eligibility is a fundamental requirement of Skills First and involves making decisions about large amounts of taxpayer funds, the training provider opts to use a commercially available electronic signature product for getting the student's signature. This covers the requirements for identity, consent and reliability in one step and provides an electronic audit trail.

Obtaining the training provider's signature

The training provider's signature is obtained when an authorised delegate completes a step within a workflow.

The training provider can demonstrate that delegate 'sign-off' can only be achieved by an individual logging-in to the system with a unique ID and password **(identity).**

Only specific individuals are authorised within the system to review and approve student information and decide student eligibility **(consent and reliability)**.

The training provider has a clear business process in place that prevents anyone without the required authorisation from completing this step in the workflow.

Example 2: Electronic endorsement of an attendance roll

A training provider uses a classroom-based delivery model, but to improve efficiency they use an online administration system to collect information about student attendance.

The training provider uses this information as Evidence of Participation.

Obtaining the training provider's signature

To record student attendance, the Skills First teacher has to log-in to a secure administrative platform using a unique ID and password **(identity)**.

The training provider has a business process in place that shows this is a recognised method for collecting student attendance information. It makes sure the minimum information needed for Evidence of Participation is recorded in the one place (the student's name or student ID, the subject identifier and the date) and that any clustered delivery information is provided as needed.

When the Skills First teacher records attendance, they complete a 'tick box' process that shows who attended the class and that they have endorsed the information **(consent and reliability)**.

Further information

Please submit an enquiry via SVTS.

Fact sheet: Sighting and retaining evidence of eligibility

Fact sheet: Recordkeeping requirements