

Electronic Signing Policy for Apprenticeships and Traineeships in Queensland

Approving Authority	Director, Queensland Apprenticeship and Traineeship Office (QATO)
Approval Date	26 July 2016
Effective Date	1 July 2019
Review Date	1 June 2024
Version Control	Version: 6 – July 2024



Policy

The [Electronic Transactions \(Queensland\) Act 2001](#) provides the regulatory framework to facilitate the use of electronic transactions and, where possible and appropriate, enable the giving of consent by electronic communication. This Act provides that, if a state law requires a person's signature, the signature when given by an electronic communication meets the requirement if the method of communicating is reliable and appropriate, the person consents to using the method, and the electronic communication identifies the person and their intention.

The Queensland Government Customer and Digital Group (QGCDG) encourages Queensland government departments to consider their requirements and assess circumstances where digital alternatives would be suitable and/or efficient.

The digitisation of services/processes and use of electronic signatures are supported by:

- an [Electronic signatures guideline](#) managed by the QGCDG
- the Department of Employment, Small Business and Training (the department), to improve productivity and process efficiencies.
 - The Queensland Apprenticeship and Traineeship Office (QATO) has developed this *Electronic Signing Policy for Apprenticeships and Traineeships in Queensland* (ESP) to guide stakeholders in the use of appropriate electronic or digital signatures (e-signatures) where document-signing or consent is required under the FET Act.

Traditional paper-based methods of document-signing and providing consent continue to be acceptable, however where these processes can be achieved more efficiently electronically, the ESP provides the guiding principles for using and accepting electronic means with regard to the processes under:

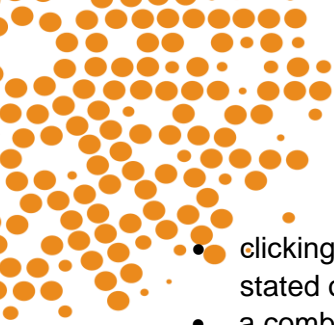
- the [Further Education and Training Act 2014](#) (FET Act),
- the [Further Education and Training Regulation 2014](#) (FET Regulation), and
- the department's [apprenticeship and traineeship operational policy and procedures](#).

Examples of electronic signatures (e-signatures)

An e-signature binds the signer to a document in a way that makes later repudiation difficult, however the validity of an e-signature depends on the type used and its purpose.

Examples of e-signatures include, but are not limited to, the following:

- typing a name into an electronic document such as an email and sending it from an email account which identifies it as originating from that particular business or person – such as an email from a business sent from the business's email account, or an email from an apprentice/trainee sent from their own email account
- signing by hand on a screen or digital pad, i.e. a scanned image of a handwritten signature applied to a document – such as signing on a courier's handheld device
- a digital signature which uses encryption and decryption technology alongside a Public Key Infrastructure (PKI) – recognised software is used to insert a digitised version of a signature into a document

- 
- clicking or ticking an 'I agree' or similar button or box on a website to provide consent as stated on screen
 - a combination of a username and a pin number or password.

Acceptable forms of e-signature

An e-signature is acceptable to the department provided the below principles are met:

- *Identity* – the document or electronic communication is signed by an identifiable person (authentication) and that person cannot credibly deny their identity (non-repudiation)
 - Where a person provides a document or consent by email, the origin of the email must identify clearly that it was sent by that person – i.e. the sender's email address identifies them.
 - For example, an apprentice or trainee providing their consent by email must send the email from their own email account, not from their employer's email account or a generic email address of their employer.
 - An apprentice/trainee's email account name need not necessarily incorporate the apprentice/trainee's name; however it must be identifiable as being their email account – e.g. tomdeb@hotmail.com.
 - The apprentice/trainee's email address can be verified, for example, by comparing it to their email address as stated on their training contract or in the DELTA database.
- *Consent or approval* – the person affixing the signature approves of the contents of the document or electronic communication and cannot later deny that they have given their approval (non-repudiation)

A party may provide their consent or approval by email in the following ways:

- by attaching a completed and signed departmental form or letter signed by hand, to the email, or
- by providing text in the email which is a clear declaration of their intent – if consenting to or approving something, the email states clearly what it is they are consenting to or approving (and includes any other required details, such as reason or date of effect).

Note that it is not sufficient for a party (say, the employer) to state in an email that the other party (say, the apprentice/trainee) agrees to a particular action. The apprentice/trainee's agreement must be given either on a completed and signed application submitted by themselves or their employer, or provided by the apprentice/trainee by email direct to the Apprentice Connect Australia Provider (Provider) or the department.

E-signature may also be used to withdraw consent.

- *Integrity* – the document or electronic communication has not been altered since it was signed. The communication method is reliable and appropriate for the purpose.
 - Note that an email that is on-forwarded (and therefore forms part of an email trail) is not considered an acceptable form of e-signature, as any email in an email trail may be altered when on-forwarded.

The department will accept e-signatures for all apprenticeship and traineeship transactions under the FET Act and FET Regulation.



Short Message Service (SMS):

- may be used to verify or seek to confirm a party's consent or approval to a stated transaction
- is limited to simple transactions that do not require extensive information
- should not be used when conveying sensitive or confidential information
- must be retained on file.

Roles and responsibilities

Department of Employment, Small Business and Training (DESBT)

- Ensure the requirements of the ESP have been met when a stakeholder provides their consent or approval by e-signature.
- If receiving an application form, follow-up on any missing signatures or information in accordance with the relevant DESBT Work Instructions.
- Maintain any records that include e-signatures in accordance with the requirements of the departmental retention and disposal schedule.
- Ensure contact details of all stakeholders are accurate and up-to-date to assist in verifying the validity of electronic communications.

Apprentice Connect Australia Providers (Providers)

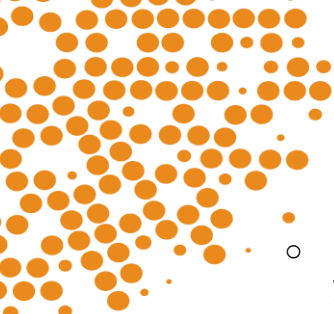
- Ensure the requirements of the ESP have been met when a stakeholder provides their consent or approval using an e-signature as an alternative to a handwritten signature.
- If receiving an application, follow-up on any missing signatures or information in accordance with the relevant Provider Work Instructions.
- Maintain any records that include e-signatures in accordance with the requirements of confidential information in the Services Agreement between the department and Providers.
- Ensure the contact details of all stakeholders are accurate and up-to-date to assist in verifying the validity of electronic communications.

Supervising Registered Training Organisation (SRTO)

- Ensure the requirements of the ESP have been met when using or/receiving electronic communications in relation to apprenticeship/traineeship transactions.
- Notify the Provider and/or the department of any changes to SRTO contact details that may be used in electronic communications and transactions under this policy.

Employer

- Ensure the requirements of the ESP have been met when providing consent or approval by e-signature as an alternative to a handwritten signature.
 - If providing consent or approval by email, ensure the email clearly identifies what it is you are consenting to or approving and that the email is sent from the relevant business email account.



- Note that, if on-forwarding an apprentice/trainee's consent or approval under cover of your email, the apprentice/trainee's consent must be sent as an attachment (not part of an email trail); the attachment may be either the relevant departmental form fully completed and signed, or an email from the apprentice/trainee stating clearly what it is they are consenting to and sent from the apprentice/trainee's personal email account.
- Notify the Provider and/or the department of any changes to employer contact details that may be used in electronic communications and transactions under this policy.

Apprentice/Trainee

- Ensure the requirements of the ESP have been met when providing consent or approval by e-signature as an alternative to a handwritten signature.
 - If providing consent or approval by email, ensure the email clearly identifies what it is you are consenting to or approving and is sent from your own email account (not a work email account).
- Notify the Provider and/or the department of any changes to contact details that may be used in electronic communications and transactions under this policy including parent/guardian details (if applicable).

Parent/Guardian (if applicable)

- Ensure the requirements of the ESP have been met when providing consent or approval by e-signature as an alternative to a handwritten signature.
 - If providing consent or an e-signature by email, ensure the email clearly identifies what it is you are consenting to and is sent from your own email account.
- Notify the Provider and/or the department of any changes to contact details that could be used in electronic communications and transactions under this policy

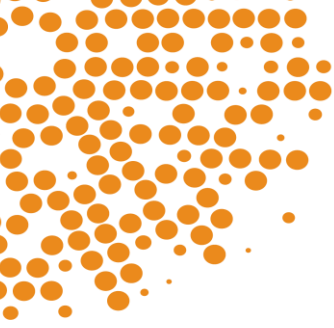
School

- Ensure the requirements of the ESP have been met when communicating consent or approval by e-signature as an alternative to a handwritten signature.
 - If providing consent or approval by email, ensure the email clearly identifies what it is you are consenting to and is sent from the school's email account.
- Notify the Provider and/or the department of any changes to contact details that could be used in electronic communications and transactions under this policy.

Process

When exercising a delegation under the FET Act, departmental officers and Providers must ensure the applicant/s have provided sufficient details and signatures to enable approval of a particular transaction, including:

- following up on any missing details or signature/s
- if the application or notification is missing a signature, that person's consent or approval may be obtained by e-signature as an alternative to a handwritten signature.



Verifying an e-signature

Each case is to be reviewed on its own merits and in the particular circumstances.

Where an officer has doubts about the authenticity of an e-signature or type of communication, they may take additional steps to verify authenticity, e.g.

- obtain documentary evidence from the party/ies, such as the certificate of authenticity, audit report from the sender, or contact the party/ies to verify the identity of the e-signature.
 - A digitised e-signature is identifiable by the automated notation that appears beside it. The visible appearance is subject to customisation, however typically consists of three components:
 - signature – which identifies the signer – e.g. a scanned handwritten ('wet') signature that has been transformed into a digital format that can be attached to an electronic document such as a PDF; or an encrypted digital code that authenticates the identity of the person affixing it to the document
 - signature details – data that appears to the right of the signature, such as the date and time the signature was affixed to the document
 - watermark or logo – an image that appears behind the signature.
- If there are still concerns about authenticity, email opra@desbt.qld.gov.au for advice before approving the transaction.

Definitions

In this policy the following definitions apply:

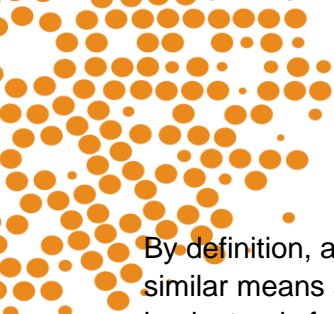
'Apprenticeship' means employment-based training declared by the chief executive under section 8 of the FET Act to be an apprenticeship.

'Certificate Authorities (CA)' are trusted companies or IT-provided services that issue and maintain digital identities. CAs confirm a signer's identity in advance, and then issue the digital ID, private PIN and/or hardware security (such as a USB token or smart card) used to create digital signatures.

'Consent or approval' – the person giving consent or approval must be in possession of all essential information so they may give valid consent or approval; and should be provided free of coercion or fraud. The Queensland Office of the Information Commissioner, in its information privacy guidelines, specifies the [key privacy concepts](#) required for valid agreement or consent. The consent must be voluntary, informed, specific and current.

'Digital signature' means an electronic signature that can be used to authenticate the identity of the signer as well as the integrity of the signed document through the use of a certificate-based digital ID. A digital signature demonstrates proof of signing by binding a signature to the document with encryption. Validation typically occurs through a Certificate Authority.

'Electronic signature (e-signature)' means a visible representation of a person's name or mark in digital form, that is attached to an electronically transmitted document, as verification of the sender's intent to sign the document.



By definition, an e-signature is ‘any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with an intent to authenticate a ‘writing’, or ‘data’ in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication’ (Blythe, 2005).

‘**DESBT**’ and ‘**the department**’ mean the Department of Employment, Small Business and Training.

‘**FET Act**’ means the [Further Education and Training Act 2014](#).

‘**Officer**’ is an appropriately qualified person to whom the chief executive has delegated functions and powers under the FET Act.

‘**Provider**’ means Apprentice Connect Australia Provider. Providers are contracted by the Department of Employment, Small Business and Training to provide targeted services which deliver tailored advice and support to employers, apprentices and trainees. The Provider is the first point of contact for the administration of all apprenticeship/traineeship training contracts.

‘**SRTO**’ means supervising registered training organisation as defined in the FET Act.

‘**Traineeship**’ means employment-based training declared by the chief executive under section 8 of the FET Act to be a traineeship.

‘**Transaction**’ includes any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, that the parties are required or choose to make in connection with the formation or performance of a contract, agreement or other arrangement.

A ‘**wet**’ signature is a handwritten signature used on a physical document, affixed with a pen or other writing device. It uses ‘wet ink’. If a traditional wet ink signature on a piece of paper is scanned into an electronic device (which identifies the signature as authentic), the scanned version is an electronic signature.

References

Blythe, S.E. (2005). Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security. Richmond Journal of Law and Technology, 11(12). Retrieved from <http://jolt.richmond.edu/jolt-archive/v11i2/article6.pdf> .

Resources

Frequently Asked Questions (FAQ) on the [Electronic signing policy](#) provide specific information on particular scenarios under the FET Act to assist officers to determine whether a transaction meets the ESP principles – refer to [Attachment 1](#) below.

Associated Documents

- [Departmental operational policies and procedures](#)
- [Electronic signatures guideline \(Queensland Government\)](#)
- [Queensland Government information privacy guidelines – Key privacy concepts \(agreement and consent\)](#)
- [DESBT Records Management policy](#)
- [Education and Training Sector retention and disposal schedule](#)
- [Electronic Transactions \(Queensland\) Act 2001](#)
- [Frequently Asked Questions \(below\)](#)
- [Further Education and Training Act 2014](#)
- *Further Education and Training Regulation 2014*



Attachment 1

Frequently Asked Questions – Electronic signing policy

Q. What is the Electronic Signing Policy (ESP) about?

A. The electronic signing policy provides guidance on considerations for accepting e-signatures as an alternative to a handwritten signature with respect to a specific transaction under:

- the [Further Education and Training Act 2014](#) (FET Act),
- the [Further Education and Training Regulation 2014](#) (FET Regulation), and
- the [department's operational policy and procedures](#) regarding apprenticeships and traineeships.

Q. What does an e-signature look like?

A. Two types of digitised e-signature are acceptable:

- A scanned signature is a digital image of a handwritten signature, obtained by scanning a paper document that has been signed by hand previously, and then converting it to a digital format – such as docx, pdf, etc. – which can then be attached to an electronic document such as an email.
- For a digitised signature, a specific type of encryption technology is used to produce secure, signed documents where their authenticity can be verified by means of a user identity and audit trail.


If in doubt about the authenticity of an e-signature, you may obtain evidence such as the certificate of authenticity or audit report from the sender, or verify the identity of the signer.

Q. What are the GUIDING PRINCIPLES for an e-signature that's acceptable to the department for emails?

A. The following principles apply.

- Note the exception where e-signature is not acceptable (in another question below).
- Any stakeholder may send an email attaching an application signed by hand by the parties. However—
- An employer providing approval/consent by email must send it from an email address that is clearly the employer's email account.
- An apprentice/trainee providing approval/consent by email must send it from an email address that is clearly their personal email account – not the employer's business email account.
- The email must state clearly that the person approves/consents, what it is that they are approving/consenting to and, if the FET Act requires the applicants provide a reason, each party must state the reason in their email.

Example 1: 'I agree to cancel training contract registration 2022xxxxx with effect from xx/xx/xxxx.' If the FET Act requires the party provide a reason for the transaction, the reason also should be stated.



Example 2: 'I agree to change my registered training organisation from x to y with effect from z.'

- The integrity of the email must be maintained. An email from one party stating that they and the other party approve/agree to a transaction isn't sufficient. Each party needs to provide an email from their identifiable email account, or one party may send the email from their account and attach, for example, an application completed and signed by the other party.

Q. Is consent provided in an email attachment acceptable for e-signature purposes?

A. Yes, provided the attached email has been sent from the sender's own recognisable email account and clearly states what it is they are, or are not, agreeing to (see the guiding principles above).

Q. Is consent provided in an email trail acceptable for e-signature purposes?

A. No, unless it is provided in the head email of the email trail. When an email is on-forwarded, the content of any email in the trail may be compromised. Therefore, only the email at the head of the trail would be acceptable for e-signature purposes.

Q. A party has sent an email from their own identifiable email address, consenting to a particular transaction. They have attached the relevant departmental form fully completed and signed except for the signature of the party sending the email. Is this acceptable as mutual consent?

A. Yes. The completed form signed by one party provides their consent to the transaction stated on the form, and the other party provides their consent by email ensuring it contains the same particulars of the transaction as identified in the form.

Q. A party has completed and signed a departmental form for a particular transaction, however the other party's signature is missing. What should I do?

A. You may obtain the consent of the party whose signature is missing from the form, by e-signature, such as by email. You would need to ensure, however, that the email they return complies with the guiding principles stated above (and obtain the parent/guardian's consent, where required).

Q. Can a party use email to withdraw from a training contract during the probationary period?

A. Yes, a party may provide an email from their own email account, stating the details of the transaction they require. The withdrawal email must be received within the applicable timeframe. A parent/guardian may also provide their consent by email.