# Durham College Policy and Procedure

| | |
|---|---|
| **TYPE:** | Administrative |
| **TITLE:** | Digital and Electronic Signatures |
| **NO.:** | ADMIN-281 |
| **RESPONSIBILITY:** | Chief Administrative Officer |
| **APPROVED BY:** | Durham College Leadership Team |
| **EFFECTIVE DATE:** | October 2020 |
| **REVISED DATE(S):** | |
| **REVIEW DATE:** | October 2024 |

## 1. Introduction

The use of digital and electronic signatures helps the College promote administrative efficiencies, improve customer service, and support the College's information management practices. Governance concerning the use of digital and electronic signatures is important as digital signatures can help authenticate signatures, collect data, and provide an audit trail.

This policy governs the usage of acceptable digital and electronic signatures when conducting business on behalf of Durham College (DC).

## 2. Purpose

The purpose of this policy and procedure is to provide a framework for the proper use of digital or electronic signatures.

## 3. Definitions

Refer to Durham College's Standard Definitions.

## 4. Policy statements

4.1. For security and authentication reasons, the College encourages the use of digital signatures when possible. The use of an electronic signature is permissible only when it is not possible to use a digital signature, or when the document being signed is for internal use only (e.g., letters, memos, reports, minutes).

4.2. Digital signatures shall be used to conduct College business to the fullest extent possible except:

- In instances in which the other contracting party will not accept a digital signature; or
- Where applicable law, regulation, or a College policy or procedure requires a handwritten signature.

4.3. A digital signature must satisfy the following criteria to be valid:

- The certificate associated with the digital signature is current (not expired).
- The signing person or organization, known as the publisher, is trusted.
- The certificate associated with the digital signature is issued to the signing publisher by a reputable certificate authority.

4.4. Digital signatures and associated data to validate the digital signature are an integral part of the record. Digitally signed documents must follow the same record retention as those using other methods of signing (e.g., electronic or handwritten signatures). The signature and means to verify it needs to be maintained for the full records life cycle. For more information, please see ADMIN-242 Information Management policy and procedure.

4.5. All digital signatures must be created using a DC-approved authentication method at the time of signature.

4.6. The presence of a digital signature does not mean that the signatory was authorized to sign or approve the document on behalf of the College. The signatory must have the proper authority as described in the Signing Authority policy.

4.7. It is a violation of this policy:

- For an individual to affix a signature of another individual, unless he or she has been granted specific, written authority by that individual; or
- To falsify a digital signature.

4.8. Employees are expected to report any actual or suspected fraudulent activities related to the use of digital or electronic signatures immediately to a manager in the appropriate department.

4.9. DC reserves the right to request a handwritten signature for any reason.

4.10. DC reserves the right to request photo identification in order to validate a signature.

## 5. Procedure

This section is not applicable.

## 6. Roles and responsibilities

6.1. It is the responsibility of the Chief Administrative Officer to ensure this policy and procedure is fully implemented.

6.2. It is the responsibility of the AVP, IT Services to approve digital signature authentication methods and for delegating responsibility for reviewing and approving the controls required for security and risk management related to the use of digital signatures.

6.3. It is the responsibility of a manager who has an incidence of actual or suspected fraud reported to them to investigate and respond accordingly.

6.4. All employees are responsible for understanding and complying with this policy and procedure to ensure all transactions are properly reviewed and executed.

## 7. Accessibility for Ontarians with Disabilities Act considerations

Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this policy and procedure, and it adheres to the principles outlined in the College's commitment to accessibility, as demonstrated by the Accessibility Plan (ADMIN-203).

## 8. Non-compliance implications

8.1. Confirmed violations of this policy will result in consequences commensurate with the offense, up to and including termination of employment, appointment, student status, or other relationships with the DC. Individuals may also be subject to criminal prosecution under applicable federal and provincial laws.

## 9. Communications plan

- A message will be posted on ICE alerting employees when new or revised policies and procedures are added to ICE.

## 10. Related forms, legislation or external resources

- None.