New College Durham

Policy on

Use of Electronic Signatures

DOCUMENT HISTORY

Issue No.	Consultation Detail	Date of Consultation	Approved by	Date Approved	Details of Amendment/ Review
1	SEG ICT Dept.	November 2012-January 2013			

NEW COLLEGE DURHAM

POLICY ON THE USE OF ELECTRONIC SIGNATURES

1. Introduction

In order to increase the speed and efficiency of its business processes the College requires that where feasible electronic signatures should be used in place of written signatures. For these electronic signatures to be effective it is important that they fulfil the same functions as written signatures and provide the appropriate level of authentication to a document.

This policy sets out the functional requirements for electronic signatures and defines the ways acceptable to the College for signing documents electronically.

2. Scope and Definitions

An **electronic signature** is data in electronic form which are attached to or logically associated with other electronic data and which serves as a method of authentication. This may include a process using email or a business system where a user is authenticated by their network login. It could also be a handwritten signature captured digitally as part of a College process (e.g. enrolment).

An **advanced electronic signature** is an electronic signature that –
(a) is uniquely linked to the signatory,
(b) is capable of identifying the signatory,
(c) is created using means that the signatory can maintain under his or her sole control, and
(d) is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable[1].

The College will not normally consider using advanced electronic signatures except where these are specifically required by a statutory or funding body as evidence of the College's internal processes.

3. Responsibilities

The Senior Information Risk Owner (SIRO) is responsible for ensuring compliance with this policy. The Deputy Chief Executive and Principal is designated in this role.

The ICT Department is responsible for reviewing this policy.

All staff are responsible for ensuring they act in compliance with this policy. In particular in ensuring the security of their user account for which they are held responsible under the Information Security Policy.

A member of staff who fails to comply with this policy may be subjected to action under the College Disciplinary Policy. It is the responsibility of Heads of

[1] Definitions are taken from the Electronic Signatures Regulations 2002 SI 2002/318. 'Advanced' signatures may include a signature created using certification by a trust service provider and public key cryptography.

Departments/School and their Directors/Assistant Principals to ensure that their staff are made aware of the existence of this Policy and its content.

4. Existing Policies

This policy relates to the following College policies:

Records Management Policy
Information Security Policy

5. Requirements

a. Functional requirements

A signature is only as good as the business process and technology used to create it. Staff must ensure that any electronic signature used must meet the functional requirements needed from a signature in the business process.

The functional requirements of a signature include:

- confirming originality and authenticity of a document;
- demonstrating a document has not been altered;
- indicating a signer's understanding and/or approval;
- indicating a signer's authorisation;
- identifying the signatory and ensuring non-repudiation of a document.

b. Cases where an electronic signature is not acceptable

Electronic signatures should not be used in transactions where there is a legal requirement for a written signature, for example in the signing of a deed or other document where the signature is required to be witnessed.

c. Electronic forms

An electronic form can be used to prove the authenticity of an authorisation when the system holding the form collects and stores an audit trail showing clearly the authorisation by an individual user.

The audit trail recording that the form has been signed and establishing the signatory's identity must be accessible for the length of the retention period required for the form, as set out in the College's Records Retention Schedule.

The system should fix the form once 'signed' so that the contents of the form cannot be changed without the signature being invalidated.

The person signing the form should be able to access a copy of the submitted signed form for as long as it is required for business purposes.

d. Scanned image of signature

A scanned image of a handwritten signature can be used as an equivalent to a written signature for purposes where it meets the appropriate functional requirements.

Scanned images of signatures must only be used where permission has been granted by the author and they must be kept securely to prevent unauthorised access and use. An example is in the preparation of transcripts.

Responsibility for the use of a scanned signature remains with the individual whose signature it is unless the person using the signature is acting maliciously, fraudulently or negligently.

e. Authorisation by email

An email from an individual user's newdur.ac.uk email address can be used as an equivalent to a written signature for internal purposes where it meets the appropriate functional requirements.

Where a member of staff allows a proxy to have write access to email it is important that the proxy is informed of the limits of his/her authority in the sending of emails on behalf of the member of staff.

Responsibility for authorisations made by email remains with the email account holder unless the proxy is acting maliciously, fraudulently or negligently.

6. Evaluation and Review

The performance of this Policy will be reported on annually and it will be formally reviewed every five years by the appropriate Corporation committee.

In addition, the effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.

Review Due: January 2018