

## **ELECTRONIC SIGNATURES FOR INTERNAL PROCESSES POLICY**

### **1 PURPOSE OF THE POLICY**

- 1.1 In order to increase the speed and efficiency of its business processes the University requires electronic signatures which can be used in place of written signatures. For these electronic signatures to be effective it is important that they fulfill the same functions as written signatures and provide the appropriate levels of authentication, integrity and non-repudiation to a document.
- 1.2 This policy sets out the functional requirements for electronic signatures and defines the ways acceptable to the University for signing documents electronically as an equivalent to a hand written signature for internal processes.

### **2 DEFINITIONS**

- 2.1 “Electronic signature” means “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”<sup>1</sup>. This may include a scanned image of a handwritten signature, a typewritten signature in an email or a ticked box on an electronic form.
- 2.2 “Advanced electronic signature” means an electronic signature -
  - (a) which is uniquely linked to the signatory,
  - (b) which is capable of identifying the signatory,
  - (c) which is created using means that the signatory can maintain under his sole control, and
  - (d) which is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable”<sup>2</sup>. This may include a signature created using certification by a trust service provider and public key cryptography. The University shall not normally consider advanced electronic signatures for internal processes except where 3.2 applies.

### **3 SCOPE OF THE POLICY**

- 3.1 This policy sets out when electronic signatures will be acceptable for internal processes and the necessary supporting conditions.

---

<sup>1</sup> Electronic Signatures Regulations 2002 SI 2002/318

<sup>2</sup> *Ibid.*

- 3.2 The use of electronic signatures to make agreements with third parties is not covered by this policy. Where signatures are required by third parties as evidence of the University's internal processes, the validation requirements of the third party must be established and, where more stringent, will normally take precedence over this policy.

#### **4 RELATIONSHIP WITH EXISTING POLICIES**

- 4.1 This policy should be read in conjunction with the:

- IT Regulations;
- IT Security Policy;
- IT Systems Password Policy;
- Records Management Policy.

#### **5 THE FUNCTION OF A SIGNATURE**

- 5.1 A signature is only as good as the business process and technology used to create it<sup>3</sup>. Any electronic signatures used therefore must meet the functional requirements needed from a signature in the business process. Staff implementing electronic signatures must ensure that the appropriate form of electronic signature is used to meet the requirements. 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.

#### **6 CASES WHERE AN ELECTRONIC SIGNATURE IS NOT ACCEPTABLE**

- 6.1 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.

#### **7 FORMS OF ELECTRONIC SIGNATURE**

##### **7.1 Electronic Forms**

- 7.1.1 The selection of an 'I agree' option (e.g. tick box or button) on an electronic form can be used as an equivalent to a written signature for internal purposes where it meets the appropriate functional requirements and the technology used records that the form has been signed and clearly identifies (e.g. by recording the username) the person who has 'signed' the form in this manner. The audit trail recording that the form has been signed and the signatory's identity must be accessible for the length of the

---

<sup>3</sup> Department for Business Enterprise & Regulatory Reform *Electronic Signatures and Associated Legislation* (2009) p.1

retention period required for the form, as set out in the University's Records Retention Schedule.

- 7.1.2 The system should fix the form once 'signed' so that the contents of the form cannot be changed without the signature being invalidated.
- 7.1.3 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 reference purposes.
- 7.2 Scanned image of a handwritten signature
  - 7.2.1 As is current practice, a scanned image of a handwritten signature can be used as an equivalent to a written signature for internal purposes where it meets the appropriate functional requirements.
  - 7.2.2 Scanned images must only be used where express permission has been granted by the author and are therefore more likely to be acceptable for high volume processes such as mass mailings.
  - 7.2.3 Scanned images of signatures must be kept securely to prevent unauthorised access and use.
  - 7.2.4 Responsibility for authorisations made by scanned signature remains with the signature's author unless the person using the signature is acting maliciously, fraudulently or negligently.
- 7.3 Authorisation by Email
  - 7.3.1 A typewritten signature in a Cardiff University account email can be used as an equivalent to a written signature for internal purposes where it meets the appropriate functional requirements, however given the ease with which emails may be manipulated this is not recommended for anything more than low risk transactions.
  - 7.3.2 Care must be taken with generic email accounts that the person sending the email is the person authorised 'to sign'.
  - 7.3.3 Where a member of staff allows a proxy to have write access to email it is extremely 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.
  - 7.3.4 Responsibility for authorisations made by email remains with the email account holder unless the proxy is acting maliciously, fraudulently or negligently.

## **8 RESPONSIBILITIES AND COMPLIANCE**

- 8.1 All staff signing electronically must ensure that they are authorised to do so.
- 8.2 All staff using electronic signatures are responsible for the security of their user account and must follow the University's IT Systems Password Policy. Passwords must not be revealed to any other person. Computers which are logged-in, including computers used to access systems remotely, must be locked when left unattended.

- 8.3 All staff who allow a proxy to access their email account or scanned signature must ensure that the proxy is informed of the limits of their authority in the sending of emails or signing documents on behalf of the member of staff.
- 8.4 The senior officer responsible for the University's compliance with this policy is the Director of Registry, Governance and Students.
- 8.5 The Governance & Compliance Division are responsible for annually reviewing this policy.
- 8.6 A breach of this policy will be considered under the University's Disciplinary Procedure.

## **9 SOURCES OF ADVICE AND SUPPORT**

- 9.1 Guidance on the legal admissibility of electronic signatures is available from the University Records Manager.
- 9.2 Advice on the technology used for electronic signatures is available from Information Services.