External Parties Information Security Policy

V1.0 29/06/2020

Date approved	29 June 2020
Approved by	Chief Finance Officer
Review date	28 June 2021
Responsible Manager	Procurement Manager
Executive Lead	CISO, CFO
Accessible to	All External Parties

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Document Version
26/05/2020	N/A	Document Creation	v0.1
28/06/2020	26/05/2020	Feedback amends	v0.2
29/06/2020	28/06/2020	Approved	v1.0

1. Applicability of Policy

This Policy applies to all external parties such as suppliers and contractors which process, access, hold or transmit NCFE Data.

2. Scope and Purpose of Policy

2.1. The NCFE Group (NCFE) uses a number of external parties who provide services and goods. The effective management of these external parties is essential in the provision of onward services to the NCFE's clients and ensuring the security of the NCFE's systems and data. This policy describes control requirements for external parties who manage NCFE data.

3. Policy Statement

NCFE is committed to the highest standards of data integrity and security, underpinning all NCFE strategic objectives.

This Policy forms part of the NCFE Information Security Management System (ISMS) and aims to:

- Increase reliability and security of systems and information
- Increase business resilience, through documented processes and procedures
- Improve information management processes and integration with corporate risk strategies

- Demonstrate that NCFE has defined and put in place, best-practice information security processes

3.1. Access to NCFE systems and information is provided to external parties to promote partnership working, information sharing, service provisions and support arrangements. We rely on the confidentiality, integrity and accuracy of our information therefore it is essential that when working with external parties information is secured in line with professional best practice.

3.2. In order to achieve this, all contracts and relationships with external parties will ensure that acceptable levels of information security are in place to protect NCFE information. Expectations will differ depending on the nature of information being shared and any known risks to that information.

Consideration will be given to any associated risks in line with the NCFE's Risk Management Framework and our agreed risk appetite position.

3.3. Where appropriate, access to NCFE systems may be granted to external parties in support of collaborative working. The degree to which access will be granted may vary based on specific needs but where possible access will be provided via authenticated access, on an individually assessed and request based approach. See Appendix 1 for security control considerations and how external parties are categorised.

3.4. Access controls will be suitably restricted meaning that external parties only have access to the information they need to fulfil their role for the time required.

3.5. Contracts shall be in place for all key external parties, contain suitable obligations for sub-contractors and shall contain appropriate non-disclosure clauses and incident management considerations. Specific confidentiality and non-disclosure agreements shall be used where confidential and/or sensitive information will be shared with the external party.

3.6. At the point that a relationship with an external party is being or has been terminated, access to NCFE systems and data shall be restricted or revoked as appropriate. The return of any physical assets and the management of any data held by that party will be managed by the Contract Manager and the Information Asset Manager responsible for the information assets.

4. Location and access to Policy

The External Information Security Policy is located as follows:

- NCFE Website: Public

5. Persons responsible for the Policy

- The Procurement Manager will maintain the Information Security standards described in this Policy.

6. Validity and Document Management

This document is valid as of 29 June 2020

The owner of this document is the Procurement Manager who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number and significance of incidents arising from external party activities
- Whether valid contracts and confidentiality agreements are in place for all key external party relationships with defined owners.

Appendix 1

External party security categorisation:

Cat 0 – full access to NCFE systems with administrative privileges. Reserved for the most strategic partnerships and only then with full audit and contractual controls.

Cat 1 – controlled access to NCFE IT systems but without administrative privileges. Typically for key, business relationships and software systems such as Microsoft.

Cat 2 – controlled access to NCFE business systems, without administrative privileges and usually restricted to a particular system such as an API with supplier system. Can also include the sharing of personal data.

Cat 3 – restricted access to NCFE materials or data only and for a specific purpose.

Information Security considerations for external parties

Acceptable levels of information security will differ depending on the nature of information being shared and any known risks to that information. Controls shall include, but not limited to, the following:

1. Malware Protection
2. Secure Configuration
3. Network Security
4. Removable Media Controls
5. User Access
6. Password Policy/Complexity