External Parties Information Security Policy

Document Control		
Document Number:	IS-052	**Effective from**: 11-11-2021
Linked Regulatory Requirements:	ISO27001	
Version Number and Date:	V2.5, 15-01-2025	**Review Date:** 15-01-2025
Date of Next Review:	14-01-2026	**Classification Level:** Public/General

Approved by: Senior Leadership team

Date version approved: 15-01-2025

Version Number	Date	Changes
V2.4	28/08/24	External document control sheet updated and contact information added
V2.5	15/01/25	Annual review – minor change to section 1.2 - word Group removed from scope

Table of Contents

1. Introduction **4**
1.1. Purpose 4
1.2. Scope 4
1.3. Responsibilities/Duties 4
1.4. Definitions 4
1.5. Location 4
2. Process **4**
3. Initial Equality Impact Assessment **5**
4. Implementation and Dissemination **5**
5. Monitoring Arrangements **5**
6. Data Retention **6**
7. Contact Information **6**
8. Appendices **7**
Appendix A – External Party Security Categorisation 7

1. Introduction

This policy ensures the highest standards of compliance and empowers users to make informed decisions on how to utilise IT (Information Technology) resources.

1.1. Purpose

NCFE use several 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.

1.2. Scope

This policy applies to NCFE and all subsidiaries/business units/trading names, including third-party contractors and any future business units or subsidiaries.

1.3. Responsibilities/Duties

The Head of Procurement and Supply will maintain the Information Security standards described in this Policy.

1.4. Definitions

Word/Acronym	Definition
API	Application Programming Interface

1.5. Location

Available on NCFE website

2. Process

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.

a) 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.

b) 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.

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

d) 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.

e) 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.

f) 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.

g) 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 and Supplier Relationship Manager and the Data Steward responsible for the information assets.

3. Initial Equality Impact Assessment

An Initial Equality Impact Assessment has been completed for this policy, and no concerns were raised.

4. Implementation and Dissemination

Available on the NCFE website.

5. Monitoring Arrangements

This document is valid as of 11 November 2021

The owner of this document is the Head of Procurement and Supply 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 (in scope) external party relationships with defined owners.

6. Data Retention

Following guidance in the NCFE Data Retention Policy the data retention requirements and timescales for deletion under this Policy are as follows:

Any financial related data - six years plus current from date of processing as outlined in HMRC Financial documentation guidance.

Unsuccessful Tender documents - one year from submission.

Successful - six years from submission as outlined in Legal and National Archives retention guidance.

7. Contact Information

If you have any queries about the contents of the policy, please contact the Customer Support team.

Email: customersupport@ncfe.org.uk

NCFE
Q6, Quorum Business Park
Benton Lane
Newcastle upon Tyne
NE12 8BT

8. Appendices

Appendix A – 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