

NOCN Job Cards CPCS Fraud Prevention Policy

NOCN Job Cards Fraud Prevention Policy

Contents

1.	Part 1 Fraud Prevention Policy	2
2.	Part 2 Internal Processes and Procedures	4
3.	Part 3 External Procedures and Processes	6
4.	Part 4 Verification of Qualifications.....	7
5.	Part 5 Action Taken when fraud identified	7

1. Part 1 Fraud Prevention Policy

1.1. Introduction:

NOCN Job Cards is committed to maintaining the highest standards of integrity and accountability. This policy outlines our approach to preventing fraud within the product and business area relating to the Construction Plant Competence Scheme (CPCS), ensuring that Certification and Cards are issued based on genuine, verifiable credentials.

The Boards of Trustees wishes to encourage anyone having reasonable suspicions of fraud to report them. All stakeholders may be confident that they will not suffer in any way as a result of reporting such suspicions. For these purposes, “reasonably held suspicions” means any suspicions other than those which are raised maliciously and are found to be groundless. This document sets out how cases of suspected fraud should be reported and dealt with.

1.2. Objectives:

- Promote a culture of honesty and transparency.
- Ensure all stakeholders understand their roles in fraud prevention.
- Establish clear procedures for reporting, investigating, and addressing fraud.
- Provide confidence to the wider Construction and related Industries that the holder of a CPCS, CSCS Logoed card is eligible to hold the card having demonstrated the required level of identification, knowledge & understanding and practical ability.

1.3. Definitions:

Blacklist(ing)	Blacklisting is the action of a group or authority compiling a blacklist of people, groups, countries or other entities to be avoided or distrusted as being deemed unacceptable to those making the list due to behaviour or activities deemed unacceptable.
Fraud	wrongful or criminal deception intended to result in financial or personal gain, a person or thing intended to deceive others, typically by unjustifiably claiming or being credited with accomplishments or qualities:
Staff	In the main relates to employees of the NOCN Group and its subsidiaries, NOCN job Cards being one. Also relates to any employed person connected to the delivery of CPCS
Stakeholders	Any individual or group with an interest or is affected by an organisation, strategy or project, both internal and external to the organisation

1.4. What is Fraud?

- 1.4.1. There are two main ways in which fraud may be committed - either by using deceit to obtain an advantage to which the fraudster is not properly entitled, or to avoid delivering on an obligation which is properly owed.
- 1.4.2. The most obvious asset open to fraud is money but many other “valuables” may be exposed to fraud such as award of contracts, appointment to positions of authority or influence, issue of permissions or licences, commercially valuable information or intellectual property as well as fraudulent qualifications and apprenticeship assessment results. Examples of fraud include:
 - False or inflated invoices for goods, services or expenses;
 - Fraudulent claims for grants, loans or compensation;
 - Failure to notify breaches of conditions of grants or assistance that would trigger repayment or breaches of contract that might result in penalty payments or termination of contract;

NOCN Job Cards Fraud Prevention Policy

- Misrepresentation to change official records and redirect genuine payments from a legitimate recipient to another account;
- Individuals seeking access to personal or financial data such as payroll records (possibly through gaining employment in a suitable post) for the purposes of direct fraud or for resale to others for exploitation;
- Collusion, bribery to influence the award and or pricing of contracts;
- Misrepresentation to obtain commercially sensitive information or access to intellectual property; and
- Incorrectly and deliberately changing results for an individual's achievements for personal or another's gain or providing examination and test answers to an individual to allow them to gain and achievement for which they do not have the required knowledge and skills.

1.5. Who might try to defraud us?

- 1.5.1. Pretty much anyone who is able to contact us may present a risk of fraud – though the vast majority will not. In reviewing the risk of fraud the possibility that staff, contractors, suppliers, training providers, applicants, testers, assessors or professional advisors, members of the public or professional criminals may try to defraud us – either individually or in collusion – is a point that has to be considered.
- 1.5.2. Staff are asked to remain vigilant at all times and report anything which seems unusual or irregular so that it can be looked into. I know that we never like to be suspicious or think the worst, but in many cases it is very simple things which highlight fraud - for example consistently avoiding complying with procedures or reporting deadlines.

1.6. Scope:

This policy applies to all employees, contractors, applicants, vendors, and partners involved with the delivery of the CPCS Card Scheme.

1.7. Reporting Fraud

- 1.7.1. All members of staff have a duty to report suspicions of fraud and raise concerns where areas of weakness in procedures are identified to the Head of Card Schemes. However, if staff have reasons for not wishing to raise concerns in this way then they may instead follow the guidance set out in the NOCN's Whistleblowing Policy. The matter will be dealt with in confidence and in accordance with the Public Interest Disclosure Act 1998. Prompt and vigorous investigations will be carried out into all cases of actual or suspected fraud discovered or reported.
- 1.7.2. Fraud conducted by Accredited Test Centres delivering CPCS is covered by the Centre Agreements, however, this does not cover the fraud of NOCN Group staff working in collaboration with centres to give them an advantage over other centres or to circumvent CPCS controls. Any activity conducted by NOCN staff that gives a centre an undue advantage over other centres or provides confidential information to a centre inappropriately for personal gain, either immediate or delayed, would be considered as fraud and gross misconduct.
- 1.7.3. The NOCN Group's whistleblowing policy also covers any flagging by outside parties of suspected fraud in relation to learners and centres.

1.8. Accountability:

- **Group CEO:** responsible to the Job Cards Board of Trustees for maintaining a sound system of internal control
- **Group Director of Finance and Governance** (Refer to NOCN Group Fraud Policy)
- **Director of Skills:** Supporting fraud prevention and managing incidents reported to them, liaising with the Assurance Committee providing updates on known or suspected fraud Ensuring that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively, ensuring compliance with systems of internal control
- **Management:** Implement and maintain robust internal controls, promote fraud awareness, and ensure compliance with this policy, reviewing when required. Ensuring that decisions made regarding new or changed business take into account the opportunities, and likelihood, of fraud. Identifying and evaluating significant risks of fraud arising out of the introduction of new or changed processes and ensuring that appropriate counter-measures are put in place; and Seeking advice from the Director of Skills where the potential for fraud is significant with regard to managing the risks.
- **Employees/Contractors:** Adhere to internal controls and report any suspicions of fraud immediately.
- **Audit Team:** Oversee the fraud prevention policy and monitor its effectiveness.

1.9. Associated documents and policies:

- NOCN Group Fraud Policy
- NOCN Group's Whistleblowing Policy
- NOCN job Cards Investigation Policy
- Accredited Centre Terms
- Accredited Centre Agreement
- CPCS Scheme Booklet for Accredited Centres
- CPCS Scheme Booklet for Testers and Trainers
- CPCS Approved Code of Delivery
- CPCS Learning Outcomes and Syllabus
- CPCS Category Specific Theory Test
- CPCS Category Specific Standard Practical Test
- CPCS Category Specific Advanced Practical Test
- CPCS Category Specific On Site Assessment
- CPCS Category Specific Advanced on Site Assessment
- CPCS Renewal CPD

1.10. Review

- 1.10.1. A formal review will take place normally annually but at least every 2 years. Any proposed changes will be considered by the CPCS Management Team liaising with the Director of Skills and the NOCN Group Audit and Risk Committee.

2. Part 2 Internal Processes and Procedures

2.1. Accredited Centre Process:

- 2.1.1. **Management System:** A CPCS Accredited Centre must implement a management system (ISO9001 or centre's own equivalent) that provides reliable means of complying with the conditions set out in the Scheme Booklets, including the following:
- Counter Fraud and Bribery
 - Whistle Blowing
 - Malpractice and Maladministration
 - Data protection requirements
 - A documented process for quality assurance to ensure staff and facilities are compliant.
- 2.1.2. **Internal Quality Assurance:** A CPCS Accredited Centre must have a named person (IQA) responsible for the Internal Quality Assurance of CPCS activities undertaken by the centre. The centre is responsible and accountable for ensuring that they have a documented internal quality assurance strategy and sample plan.
- 2.1.3. **CPCS Technical Test Delivery:** A CPCS Accredited Centre must ensure that the candidate has a valid CPCS registration number which includes the requirement to bring one form of identification.

2.2. Application Process Red to Blue Upgrade:

- **Standardised Procedures:** Application processing for all card types must follow the work instructions available within the CPCS SharePoint area.
- **Document Verification:** All submitted documents, including qualifications and identity proofs, must be thoroughly verified. Examples of previously received fraudulent and authentic documents (proof of achievement certificates Etc.) can be found in the "Suspected Fraud Log" within the CPCS SharePoint Area for reference and training purposes.
- **Application Tracking:** Maintain the Job Cards payment Log used to track applications for card from receipt to printing including invoicing.

2.3. Verification of Qualifications:

- **Accredited Institutions:** Only accept qualifications from accredited awarding bodies governed by Ofqual.
- **Direct Verification:** Conduct direct verification of qualifications with issuing awarding bodies where possible.
- **Third-Party Services:** Utilise third-party verification services to authenticate qualifications and credentials.

2.4. Collaboration with Partners:

- **Partnership Agreements:** Only share data with parties with whom we have a signed Data Sharing Agreement using means of secure transfer of data only required to undertake any investigatory work in line with the agreement.
- **Information Sharing:** Information data requests, only share data in line with any signed data agreements or authentic requests for information using secure means, no information is to be passed to any third party without first ensuring that a data agreement is in place or that the Information Manager has been informed and confirmation to provide information has been confirmed and the detail clarified as to the detail of information to be passed.
- **Regular Audits:** Conduct regular audits of delivery partners' compliance with fraud prevention measures.

2.5. Training and Awareness:

- **Fraud Awareness Training:** Provide regular training for all employees and contractors on fraud prevention, detection, and reporting.
- **Educational Materials:** Distribute materials that outline common fraud schemes and prevention techniques.
- **Updates and Reminders:** Regularly update staff on new fraud risks and remind them of their responsibilities utilising the suspected Fraud Log to provide examples of the types of suspected fraud.

2.6. Continuous Monitoring and Evaluation:

- **Monitoring Systems:** Utilise and review the various CPCS card application recordings processes to continuously monitor interactions, applications and transactions for signs of fraud.
- **Data Analytics:** Use data analytics to identify unusual patterns and potential fraudulent activities.
- **Performance Metrics:** Utilise the quality assurance Team to evaluate the effectiveness of fraud prevention measures.
- **(Insert flow diagram feed back loop)**

2.7. Action Taken When Fraud Identified:

- **Immediate Response:** Take immediate action to investigate and address suspected fraud.
- **Investigation Procedures:** Follow established procedures for conducting thorough and impartial investigations as outlined in the NOCN Job Cards Investigation Policy.
- **Disciplinary Actions:** Implement appropriate actions, including termination of card and potential legal action, against individuals involved in fraud.
- **Loss Recovery:** Seek to recover any losses incurred due to fraudulent activities.

2.8. Regular Updates and Compliance Checks:

- **Policy Reviews:** Review and update the fraud prevention policy Bi annually or following an investigation feedback loop where improvements have been identified.
- **Compliance Audits:** Conduct regular compliance audits to ensure adherence to the policy.
- **Feedback Mechanism (Lessons learned):** Following any internal investigation use the feedback loop to identify any opportunities to improve process and procedures which are then to be included to standardisation meetings (EQA) and training session for the application processors (Customer Services Team).

2.9. Whistleblowing:

- **Confidential Reporting:** Provide a confidential whistleblowing channel for reporting suspected fraud.
- **Protection for Whistleblowers:** Ensure that whistleblowers are protected and that their reports are taken seriously.
- **Investigation Follow-Up:** Ensure that all whistleblowing reports are thoroughly investigated and appropriate actions are taken

3. Part 3 External Procedures and Processes

3.1. Accredited Centre Technical Test Delivery

3.1.1. Pre Technical Test Delivery:

- All candidates are to verify the ID of the candidates undertaking the CPCS Activity
- All candidates are to complete the Data Protection from prior to undertaking any CPCS Activity.
- CPCS can make a request of the Accredited Test Centre, that any ID used to confirming the identity of the candidate undertaking the CPCS Activity must be photocopied or a photo is to be taken of the ID used and stored with the candidates Technical Test Documentation.

3.1.2. Technical Test Delivery:

- The Theory Test Induction: The induction must include core elements that cover the following points:
 - Confirmation of the details relating to tester, candidate, venue, test, and date details.
 - Identification check using documentation that includes a photograph and signature
 - Theory Test Script (To be recorded) for quality assurance purposes: Read out by the Tester – Identification Check – I am now checking the candidate's identity documentation and I have been shown their (list contained within the Scheme Booklet and Approved Code of Delivery) and can confirm that the photograph is a true likeness.
- Quality Assurance: A CPCS Accredited Centre and including their Testers must allow unrestricted access for NOCN Job Cards Quality Assurance Personnel (EQA) to all facilities and sites where CPCS activities are being conducted or where there are related documents.

3.2. Application Review Red Card to Blue Upgrade

3.2.1. Application Submission:

- **Application Forms:** Ensure all applications are submitted through:
 - CWA (cards without application) – submitted through NOCN Hub uploaded into SharePoint (CPCS Test Centre Team).
 - CPCS email inbox – DPA checks completed by Ops Team verified via quartz.
 - Postal applications signed by applicant

3.3. Data Collection and Verification:

3.3.1. Identity Verification:

- Identification checked prior to commencement of CPCS Health, Safety and Environment Test
- Identification checked by Accredited Centre prior to commencement of Technical Testing
- DPA checks completed by Ops Team verified via quartz
- Document Uploads: Require scans of identity documents (passport, driver's license) if Vocational Qualification name does not match quartz record
- Validation Checks: Manually validate the format and details of submitted documents

3.4. Fraud Detection Tools:

- **Fraud Scoring:** Assign a fraud risk score to each application based on criteria like geographical location, address, and historical fraud data.
- **Cross-Referencing:** Cross-check applicant details against databases of known fraudsters.

3.5. Manual Review:

- **High-Risk Applications:** Flag high-risk applications for manual review by nominated personnel. Classification to be added to Quartz to highlight individuals associated with high risk Accredited Centres.
- **Expert Analysts:** Ensure team members are trained to detect signs of fraudulent behaviour and document manipulation.
- **Additional Verification:** Contact applicants directly to verify details if necessary.

3.6. Data Analytics and Monitoring:

- **Behavioural Analysis:** Monitor application behaviour for unusual patterns (e.g., multiple applications from the same address etc.).

NOCN Job Cards Fraud Prevention Policy

- **Real-Time Alerts:** Set up real-time alerts for suspicious activities. Classifications added to Quartz to highlight individuals and accredited centres.

3.7. Security Measures:

- **Secure Data Storage:** Store applicant data in password protected databases with access controls.

3.8. Compliance and Auditing:

- **Regulatory Compliance:** Ensure the procedure complies with regulations, including GDPR.
- **Regular Audits:** Conduct regular audits of the application review process and fraud detection systems.

3.9. Applicant Communication:

- **Clear Instructions:** Provide clear instructions on the application process and required documents.
- **Status Updates:** Keep applicants informed of their application status.

3.10. Continuous Improvement:

- **Feedback Loop:** Gather feedback from fraud analysts and improve the fraud detection based on new fraud trends.
- **Training Programs:** Regularly update training programs for fraud detection personnel.

4. Part 4 Verification of Qualifications

4.1. Accredited Institutions:

- Only accept qualifications from accredited awarding bodies recognised by relevant authorities.

4.2. Direct Verification:

- Conduct direct verification of qualifications with issuing awarding bodies where possible:
 - NOCN (National Open College Network)
 - SQA (Scottish Qualifications Authority)
 - ProQual (ProQual Awarding Body)
 - AIM Qualifications and Assessment Group
 - City and Guilds
 - ECITB (Engineering Construction Industry Training Board)
 - Pearson / Edexcel
 - GQA Qualifications
 - Lantra
 - MPQC (Mineral Products Qualifications Council)
 - Apprenticeship awarding body *ifate*

4.3. Third-Party Services:

- Utilise third-party verification services to authenticate qualifications and credentials.
 - CITB Card Checker
 - CITB Fraud Manager
 - CISRS (Construction Industry Scaffolders Record Scheme)

5. Part 5 Action Taken when fraud identified

5.1. Immediate Response:

- Take immediate action to investigate and address suspected fraud.
 - Application received
 - Fraudulent activity determined
 - Team leader informed
 - Investigation procedure started

NOCN Job Cards Fraud Prevention Policy

- Whistle Blowing

5.2. Investigation Procedures:

- Follow established procedures for conducting thorough and impartial investigations.
 - Fraudulent activity determined
 - Information passed to Investigation (CPCS Product and Services Management Team) team
 - Application verified through accredited awarding bodies
 - Certification deemed genuine or not genuine
 - Genuine – no further action required
 - Not Genuine – log information on database
 - Application suspended
 - Any further action determined by the Investigation Team following the CPCS Investigation guidance and Policy Document.

5.3. Disciplinary Actions:

- Implement appropriate actions, including termination of card and potential legal action, against individuals involved in fraud.

5.4. Loss Recovery:

- Seek to recover any losses incurred due to fraudulent activities.