



---

# FRAUD POLICY



Version Number	Date	Purpose of Change	Classification	Sign Off
V4.1	13/11/2025	Merging of EPA, NOPS and Qualifications Policies and new content and formatting	Public	Kerry Ore

Copyright © 2025 Smart Awards Ltd

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means whatsoever without prior written permission from the copyright holder.

Unit F8A | Holly Farm Business Park | Honiley Road | Kenilworth | CV8 1NP  
T: 02476 421125  
E: [info@smartawards.co.uk](mailto:info@smartawards.co.uk)  
W: [www.smartawards.co.uk](http://www.smartawards.co.uk)

Company Number 9079735 | VAT Number 216 7632 0

# 1. POLICY STATEMENT

1.1 Smart Awards is committed to maintaining the highest standards of honesty, integrity, transparency, and accountability across all activities related to Qualifications, Apprenticeship Assessments, End-Point Assessments (EPA) and the Network Operative Passport Scheme (NOPS).

1.2 Smart Awards has zero tolerance for:

- Fraud
- Dishonesty
- Theft
- Deception
- Falsification of records or evidence
- Misuse of systems, credentials, data or certification
- Any action intended to obtain an unauthorised benefit

Fraud undermines:

- The integrity of assessments
- Public confidence
- Qualification and EPA validity
- The safety and compliance of NOPS
- The credibility of Smart Awards as an awarding and EPA organisation

Smart Awards is committed to:

- Preventing fraud
- Detecting fraud quickly
- Investigating all allegations thoroughly
- Taking proportionate action and applying sanctions
- Reporting concerns to external authorities where required
- Ensuring that learners, apprentices, employers, centres, contractors and staff act ethically
- Maintaining compliance with all regulatory and legislative requirements

1.3 Smart Awards will support anyone who raises a genuine concern about possible fraud in good faith. Retaliation or victimisation of whistleblowers will not be tolerated.

## 2. PURPOSE AND SCOPE

### 2.1 Purpose

The purpose of this policy is to:

- Ensure Smart Awards has a clear, systematic framework for preventing, detecting, reporting, and responding to fraud.
- Protect the integrity of Qualifications, Apprenticeship Assessments, End-Point Assessments (EPA) and the Network Operative Passport Scheme (NOPS).
- Promote a culture of honesty, transparency, accountability, and good governance.
- Set out clear responsibilities for staff, Centres, Employers, Training Providers, contractors and NOPS users.
- Prevent false certification, false identification, data manipulation, assessment fraud, and misuse of credentials.
- Ensure compliance with:
  - Ofqual General Conditions
  - Ofqual EPA Qualification Level Conditions
  - Qualifications Scotland Accreditation Principles
  - Industry and legal requirements (including the Fraud Act 2006 and UK GDPR)

Smart Awards will act promptly and proportionately to all allegations or suspicions of fraud.

## 2.2 Scope

This policy applies across the entire Smart Awards provision and covers all types of fraud associated with:

- Qualifications
- Apprenticeship Assessments
- End-Point Assessment (EPA)
- NOPS (Network Operative Passport Scheme)

It applies to:

- Smart Awards employees
- Board members
- Independent contractors
- Assessors and Internal Quality Assurers (IQAs)
- Independent End-Point Assessors (IEPAs)
- External Quality Assurers (EQAs)
- Centres, Employers and Training Providers
- Apprentices and learners
- NOPS users, cardholders and organisations with NOPS access
- Partners and third parties acting on behalf of Smart Awards

## 2.3 Types of Fraud Covered by This Policy

This policy covers all forms of fraud including, but not limited to:

- False certification
- Forged signatures or documents
- Identity fraud
- Manipulation of learner or apprentice records
- Misuse of EPA assessment materials
- Gateway fraud
- Portfolio or evidence falsification
- Maladministration that results in fraudulent outcomes
- NOPS card misuse or falsification
- Misuse of systems or access privileges
- Falsification or destruction of official records
- Dishonest or deceptive behaviour to secure an unfair advantage
- Theft, financial fraud or misappropriation of assets

## 2.4 Relationship with Other Policies

This policy should be read in conjunction with:

- Malpractice and Maladministration Policy
- Conflicts of Interest Policy
- Data Protection Policy
- Complaints Policy
- Whistleblowing Policy

Where fraud is suspected, this Fraud Policy takes precedence over internal complaints procedures.

# SECTION 3 – DEFINITIONS

## 3.1 Fraud (General Definition)

Fraud is defined as: *Any intentional act or omission intended to deceive, dishonestly gain an advantage, cause loss, or secure an unauthorised benefit for oneself or another.*

This includes (but is not limited to):

- Falsification of documents or assessments
- Dishonest representation of information

- Theft or misappropriation of assets
- Alteration, destruction, or concealment of records
- Misuse of systems, access or credentials
- Providing false information to gain an award, card or assessment outcome

### **3.2 False Certification**

False certification includes:

- Forging or altering Smart Awards certificates
- Issuing certificates without valid assessment
- Duplicate or fraudulent replacement certificates
- Using someone else's certification
- Creating false training or achievement records
- Misrepresenting NOPS status or expiry
- Producing falsified qualification evidence or records

### **3.3 Identity Fraud**

Identity fraud includes:

- Sitting an assessment or EPA on behalf of someone else
- Using another person's identity, NOPS card, or credentials
- Misrepresenting personal information or employment status
- Submitting evidence created by someone else
- Manipulating apprentice identity at Gateway

### **3.4 Assessment Fraud (Qualifications & Apprenticeship Assessments)**

Examples include:

- Fabrication or falsification of learner evidence
- IQA falsifying sampling records
- Assessors signing off work not completed
- Altering marks, logs, portfolios or witness testimonies
- Working with others to circumvent assessment controls

### **3.5 EPA Fraud (EPA-Specific)**

Examples include:

- IEPA submitting incorrect or manipulated assessment outcomes
- Failure to follow the Assessment Plan
- Manipulated Gateway information
- Collusion between IEPA, Employer or Training Provider
- Premature release or misuse of EPA materials
- Providing predetermined questions or model answers
- Non-independent assessment

### **3.6 Apprenticeship Assessment Fraud (On-Programme)**

Fraud relating to apprenticeship assessments includes:

- Employer-generated false workplace evidence
- Training Provider altering progress records
- Misrepresentation of KSB achievement
- Manipulated mock EPA outcomes
- False declarations at Gateway

### **3.7 NOPS Fraud (Card Scheme-Specific)**

Examples include:

- Use of fake or altered NOPS cards
- Fraudulent applications for NOPS access
- Misuse of system permissions to alter card data
- Shared logins or unauthorised system access

- Use of a card by an individual other than the cardholder
- Falsification of health and safety or training completion records
- Criminal misuse or attempted misuse of scheme data

### **3.8 Internal Fraud**

Includes:

- Staff falsifying records
- Improper use of information systems
- Manipulating qualifications or EPA outcomes
- Misuse of expenses, assets or funds
- Theft or financial irregularity

### **3.9 External Fraud**

Includes fraud carried out by:

- Centres
- Employers
- Training Providers
- Learners or apprentices
- Contractors
- NOPS users
- Third parties

Such fraud may involve any misrepresentation that undermines validity or integrity.

### **3.10 Suspected Fraud**

A suspicion of fraud exists when:

- There is evidence of unusual behaviour or anomalies
- Concerns are raised by staff, apprentices, learners, employers or third parties
- Assessment or NOPS data appears manipulated
- There is a pattern of inconsistencies
- Something "does not feel right"

Smart Awards will treat all suspected cases seriously, even if not yet proven.

## **SECTION 4 – PRINCIPLES**

Smart Awards is committed to adopting a proactive and systematic approach to preventing, detecting, and responding to fraud across Qualifications, Apprenticeship Assessments, EPA, and NOPS. These principles underpin all aspects of fraud prevention and investigation.

### **4.1 Zero Tolerance**

Smart Awards has zero tolerance for fraud, dishonesty or deception.

Any proven case of fraud will result in immediate and proportionate action, including:

- Suspension of access
- Removal of approval
- Invalidating results or certificates
- Disciplinary action
- Police or regulatory reporting
- Legal action

### **4.2 Integrity and Transparency**

All individuals must act with:

- Honesty
- Professional integrity
- Transparency in records and communications
- Accountability for actions and decisions

Smart Awards maintains transparent reporting mechanisms for handling fraud allegations.

### **4.3 Fairness and Impartiality**

All fraud investigations will be conducted:

- Objectively
- Free from conflicts of interest
- In a timely manner
- In accordance with regulatory expectations
- Proportionately, based on severity

Investigations must be evidence-based and documented.

### **4.4 Confidentiality**

Smart Awards will:

- Protect the identity of individuals reporting suspected fraud (where lawful)
- Keep investigation details confidential
- Share information only where necessary for investigation or regulatory/legal requirements

### **4.5 Protection for Whistleblowers**

Individuals raising concerns in good faith will:

- Be protected under Smart Awards' Whistleblowing Policy
- Not be victimised or disadvantaged
- Be supported throughout the process

False or malicious allegations will be treated as misconduct.

### **4.6 Compliance with Regulatory and Legal Requirements**

Smart Awards must comply with:

- Ofqual General Conditions of Recognition
- Ofqual EPA Qualification Level Conditions
- Qualifications Scotland Accreditation Principles
- Fraud Act 2006
- Bribery Act 2010
- Data Protection Act 2018 / UK GDPR
- Apprenticeship Assessment Plans
- Industry and scheme requirements (NOPS)

Where a fraud case meets the threshold of an Adverse Effect, Smart Awards will notify:

- Ofqual
- Qualifications Scotland Accreditation
- Qualifications Wales
- Police or ICO (if criminal or data breach implications exist)

### **4.7 Prevention First**

Smart Awards takes a preventive approach by:

- Establishing robust controls
- Ensuring staff training and awareness
- Maintaining clear processes and system safeguards
- Monitoring emerging risks
- Encouraging early reporting
- Maintaining multiple routes for disclosures

### **4.8 Proportionality and Consistency**

Sanctions and actions resulting from proven fraud will be:

- Proportionate to the seriousness of the offence
- Consistent across all departments
- Linked to risk to validity, safety or scheme integrity

- Applied fairly and transparently

#### 4.9 Record Keeping and Evidence Retention

Smart Awards will retain:

- Fraud reports
- Investigation notes
- Evidence
- Communications
- Corrective actions
- Board decisions

For 7 years, or longer where regulator or law requires.

#### 4.10 Continuous Improvement

Smart Awards uses fraud cases to:

- Identify systemic weaknesses
- Improve controls and processes
- Update training and guidance
- Strengthen monitoring and verification
- Enhance data security

## SECTION 5 – RESPONSIBILITIES

Fraud prevention and detection is a shared responsibility across Smart Awards, Centres, Employers, Training Providers, Assessors, IEPAs, NOPS users and all individuals involved in any aspect of qualifications, apprenticeship assessments, EPA or NOPS.

This section outlines **clear responsibilities by role**, ensuring transparency and accountability.

<p><b>Smart Awards Board and CEO</b></p>	<p>Responsible for:</p> <ul style="list-style-type: none"> <li>• Strategic oversight of fraud prevention and response</li> <li>• Ensuring an anti-fraud culture within the organisation</li> <li>• Reviewing serious fraud cases and deciding sanctions where required</li> <li>• Approving final decisions for high-risk or high-impact cases</li> <li>• Ensuring regulatory notifications are completed</li> <li>• Reviewing fraud trends and systemic risks quarterly</li> </ul>
<p><b>Responsible Officer</b></p>	<p>Responsible for:</p> <ul style="list-style-type: none"> <li>• Ensuring this policy is implemented effectively</li> <li>• Ensuring all allegations of fraud are treated seriously</li> <li>• Appointing independent investigators</li> <li>• Escalating cases to police, ICO, regulators or external authorities if required</li> <li>• Providing updates to the Board</li> <li>• Ensuring corrective actions are delivered</li> <li>• Ensuring risk implications are reviewed and mitigated</li> </ul>
<p><b>Quality Manager</b></p>	<p>Responsible for:</p> <ul style="list-style-type: none"> <li>• Day-to-day management of fraud prevention and detection</li> <li>• Logging and tracking cases through SAMS and the Risk Register</li> <li>• Coordinating and supporting investigations</li> <li>• Ensuring cases are handled within defined timescales</li> <li>• Ensuring investigators have correct access to evidence and records</li> <li>• Monitoring patterns, trends and emerging risk areas</li> <li>• Updating Smart Awards' processes and training as necessary</li> </ul>

	<ul style="list-style-type: none"> <li>• Maintaining the Fraud &amp; Malpractice Risk Assessment</li> </ul>
<b>Staff, Contractors, Assessors, IEPAs and EQAs</b>	<p>All individuals working with or for Smart Awards must:</p> <ul style="list-style-type: none"> <li>• Act with honesty and integrity</li> <li>• Follow all processes designed to prevent and detect fraud</li> <li>• Not engage in any form of dishonest behaviour</li> <li>• Report suspected fraud immediately</li> <li>• Cooperate fully with investigations</li> <li>• Maintain accurate records</li> <li>• Follow data protection and privacy requirements</li> <li>• Avoid conflicts of interest</li> <li>• Protect secure materials, including EPA materials, Centre files and NOPS data</li> </ul> <p>IEPAs have a specific duty to:</p> <ul style="list-style-type: none"> <li>• Maintain independence</li> <li>• Follow the Assessment Plan precisely</li> <li>• Report irregularities or concerns immediately</li> <li>• Support investigations by providing accurate information</li> </ul>
<b>Centres, Employers and Training Providers</b>	<p>Responsible for:</p> <ul style="list-style-type: none"> <li>• Preventing fraud at Centre or employer level</li> <li>• Maintaining secure processes for assessment, delivery and certification</li> <li>• Ensuring staff follow correct identity verification procedures</li> <li>• Ensuring accurate and honest record-keeping</li> <li>• Reporting any suspected fraud or irregularity to Smart Awards within 3 days</li> <li>• Supporting investigations by providing information, access and cooperation</li> <li>• Maintaining and reviewing their own malpractice controls</li> <li>• Ensuring appropriate supervision of learners and apprentices</li> </ul>
<b>Learners and Apprentices</b>	<p>Learners and apprentices must:</p> <ul style="list-style-type: none"> <li>• Provide accurate and truthful information at all times</li> <li>• Complete their own work</li> <li>• Not impersonate or allow impersonation</li> <li>• Not share assessment materials inappropriately</li> <li>• Not commit any act of dishonesty, falsification or deception</li> <li>• Report concerns or irregularities if noticed</li> </ul>
<b>NOPS Users, Employers and Organisations</b>	<p>Responsible for:</p> <ul style="list-style-type: none"> <li>• Maintaining secure access credentials</li> <li>• Ensuring login details are not shared</li> <li>• Preventing misuse of NOPS cards</li> <li>• Ensuring all NOPS-related information is accurate</li> <li>• Reporting any suspected misuse or fraudulent activity immediately</li> <li>• Supporting investigations into NOPS misuse or data manipulation</li> </ul> <p>Failure to comply may result in:</p> <ul style="list-style-type: none"> <li>• Access removal</li> <li>• Card invalidation</li> <li>• Contract termination</li> <li>• Reporting to authorities (if fraudulent or criminal behaviour is involved)</li> </ul>

## SECTION 6 – PREVENTION MEASURES

Smart Awards takes a preventative approach to fraud by ensuring that appropriate systems, controls, culture and oversight are in place across Qualifications, Apprenticeship Assessments, EPA and NOPS.

### 6.1 Control Environment

Smart Awards maintains an organisational culture where:

- Fraud is not tolerated
- Ethical behaviour is expected
- Controls are monitored
- Staff are trained
- Policies are clear and accessible
- Reporting concerns is encouraged

### 6.2 Segregation of Duties

Segregation of duties helps reduce fraud risk by ensuring:

- No single individual controls all stages of a process
- EPA decisions cannot be influenced by training providers
- NOPS data changes require appropriate authorisation
- Qualification certification requires dual verification
- Staff approval levels are limited and monitored
- System access aligns with job roles only

### 6.3 Access and System Controls

Smart Awards operates robust technical controls, including:

- User authentication and password protection
- Role-based permissions and access restrictions
- Monitoring of activity logs for unusual behaviour
- Secure storage of EPA materials
- Secure NOPS data architecture
- Multi-factor authentication where appropriate
- Immediate removal of access upon staff exit
- Periodic access audits

Systems monitored include:

- SAMS (qualification/EPA records)
- NOPS system
- IT infrastructure and email
- Assessment platforms and repositories

### 6.4 Staff Training and Awareness

Smart Awards ensures that:

- All staff receive fraud awareness training
- IEPAs are trained on EPA integrity and conflicts of interest
- Centre staff receive guidance on preventing assessment fraud
- NOPS users receive training on system security
- Risk-based training is delivered to areas of higher vulnerability
- Refresher training occurs annually

### 6.5 Centre and Provider Controls

Smart Awards requires Centres, Employers and Training Providers to:

- Verify learner and apprentice identity
- Maintain secure assessment environments
- Protect assessment materials
- Prevent staff from assisting learners inappropriately

- Maintain accurate records and evidence
- Report suspected fraud immediately

### **6.6 Preventing False Certification**

Smart Awards applies controls to prevent false or invalid certificates, including:

- Validation checks before issuing certificates
- Examination of assessment completion and verification logs
- Audit of records where anomalies arise
- Secure storage of certificate paper
- Controls over certificate printing and reprints
- Recording reasons for any reissue
- Scrutiny of suspicious or duplicate requests

### **6.7 Preventing EPA Fraud**

EPA-specific controls include:

- Strict identity verification at Gateway and EPA
- Clear separation of training and assessment
- EPA materials held securely and only accessed when required
- IEPA independence checks
- Spot checks and moderation of IEPAs
- Recording and logging of assessment interviews (where required by the Assessment Plan)
- Secure scheduling processes
- Continuous training on avoiding bias and undue influence

### **6.8 Preventing Apprenticeship Assessment Fraud**

On-programme controls include:

- Evidence authenticity checks
- Observation or verification logs
- Preventing employer over-involvement or falsification
- Moderation of portfolios and records

### **6.9 Preventing NOPS Fraud**

NOPS-specific prevention controls include:

- Unique NOPS card identifiers
- Real-time status checks
- System-based audit logs
- Photo and personal detail verification
- Employer verification processes
- Access control rules
- Monitoring for suspicious log-ins
- Immediate suspension procedures

### **6.10 Third-Party Controls**

Where contractors or partners are involved (e.g., IT providers, assessors, specialist consultants):

- Due diligence checks are performed
- Contracts include anti-fraud clauses
- Access to systems is restricted
- Activity is monitored
- Non-compliance results in removal of access

### **6.11 Risk-Based Monitoring**

Smart Awards undertakes regular monitoring to identify fraud risks, including:

- Performance data review

- EPA grade pattern analysis
- Centre risk profiling
- NOPS activity audits
- Assessor and IEPA performance monitoring
- Spot-checks and unannounced sampling

High-risk areas receive enhanced monitoring.

## SECTION 7 – DETECTION OF FRAUD

Smart Awards employs a range of proactive and reactive methods to detect potential or actual fraud across Qualifications, Apprenticeship Assessments, EPA, and NOPS. Detection relies on robust systems, careful monitoring, awareness and a culture where concerns can be raised safely.

### 7.1 Early Warning Signs of Fraud

Fraud indicators may include (but are not limited to):

- Inconsistent or irregular records
- Altered or suspicious documentation
- Unusual activity patterns in NOPS system logs
- Duplicate or inconsistent apprentice or learner details
- Missing signatures or frequent corrections
- Unmatched dates or implausible timelines
- Repeated complaints about a particular Centre, IEPA or employer
- Unusual grade patterns (EPA or qualification)
- Evidence that appears overly polished or identical
- Learner work that does not match known ability
- Connection between IEPA and employer/training provider
- Unexpected changes to certification or registration requests

Any concern, however small, must be taken seriously.

### 7.2 Internal Monitoring

Smart Awards uses several internal controls to identify fraud:

#### 7.2.1 Data Monitoring

Regular analysis of:

- Registration trends
- Certification anomalies
- EPA grade distributions
- High or unexpected pass rates
- NOPS access logs
- System login patterns
- Duplicate user activity

#### 7.2.2 Quality Assurance Activity

Includes:

- Internal audits
- External Quality Assurance (EQA) outputs
- Standardisation outcomes
- EPA moderation
- Monitoring of assessors and IEPAs
- Centre monitoring visits

#### 7.2.3 System Alerts

System-based flags may be triggered by:

- Multiple failed login attempts
- Repeated card scans (NOPS)
- Suspicious editing behaviour
- External IP access patterns

- Unusual EPA marking patterns
- Altered documents or data inconsistencies

### **7.3 External Detection Triggers**

Fraud may be identified by:

- Employers
- Training Providers
- Centres
- Apprentices or learners
- Professional bodies
- Members of the public
- External authorities (Police, ICO, ESFA)
- Other Awarding Organisations/EPAOs

All allegations must be reported immediately.

### **7.4 Centre and Provider-Level Detection**

Centres, Employers and Training Providers may detect:

- Identity mismatch at assessment
- Irregularities during portfolio submission
- Falsified work or signatures
- Inconsistent on-programme records
- EPA readiness disproportions
- NOPS misuse or card fraud
- Tampering with documentation
- Conflicting statements from staff or learners

They must notify Smart Awards within 3 days.

### **7.5 Detection in EPA**

EPA-specific detection includes:

- IEPA observing inconsistent performance
- Gateway record inconsistencies
- Evidence that does not match employer accounts
- Apprentice unable to explain portfolio content
- Prior knowledge of EPA tasks or questions
- IEPA concerns around independence or interference

EPA concerns are high-risk due to validity requirements and may trigger EPA3 regulatory notifications.

### **7.6 Detection in NOPS**

NOPS-specific fraud detection includes:

- Card scanning irregularities
- Use of expired or invalid cards
- Photo/image mismatch
- Repeated failed verification attempts
- Multiple users with identical information
- Access logs indicating suspicious system access
- Audit trails showing manipulation of data

### **7.7 Whistleblowing Route**

Fraud may be detected through the Smart Awards Whistleblowing Policy, allowing concerns to be raised anonymously or confidentially. Whistleblowers are protected under this policy.

### **7.8 Immediate Actions on Detection**

Where suspected fraud is identified:

- Smart Awards must immediately secure evidence

- Access to systems or records may be suspended
- EPA or qualification results may be withheld
- NOPS cards may be suspended
- Staff or IEPAs may be temporarily removed from duty
- CEO/MD must be informed
- Risk Register updated
- Relevant authorities may be notified

## SECTION 8 – REPORTING FRAUD

Smart Awards requires all staff, Centres, Employers, Training Providers, IEPAs, contractors, apprentices, learners and NOPS users to report any suspicion of fraud immediately. Reporting fraud early reduces the impact and prevents further harm.

### 8.1 How to Report Fraud

Concerns may be reported via:

- Email
- Phone
- Letter
- In person
- Through the Whistleblowing Policy (anonymous reporting permitted)

Reports should include:

- Details of the concern
- Names of individuals involved
- Relevant dates and evidence
- Whether the risk is ongoing

### 8.2 Immediate Escalation to Senior Leaders

Serious cases must be escalated immediately to the Responsible Officer.

Examples requiring immediate escalation include:

- False certification
- EPA fraud or Gateway fraud
- NOPS card misuse
- Identity fraud
- Criminal activity
- Data breaches
- Centre-wide malpractice
- Collusion

### 8.3 External Reporting Requirements

Smart Awards may be required to report suspected or confirmed fraud to external authorities:

Regulators

- Ofqual (Qualifications & EPA – EPA3 conditions)
- Qualifications Scotland Accreditation
- Qualifications Wales

Legal Authorities

- Police (fraud, impersonation, criminal activity)
- ICO (data breaches or unlawful processing)

### 8.4 Protection for Individuals Reporting Fraud

Smart Awards protects individuals who report fraud:

- No victimisation
- No detriment
- Confidential handling
- Anonymous reporting permitted

- Protection under the Whistleblowing Policy
- False accusations made maliciously will be treated as misconduct.

### **8.5 Failure to Report Fraud**

Failure to report known or suspected fraud may constitute:

- Misconduct
- Maladministration
- Breach of contract
- Professional misconduct

And may result in disciplinary, contractual or regulatory action.

## **9. FRAUD INVESTIGATION PROCESS**

Smart Awards conducts thorough, confidential, fair and impartial investigations into all reports of suspected or proven fraud.

### **9.1 Overview**

All investigations follow a universal Smart Awards process, with department-specific details detailed in Section 13.

The process ensures:

- Independence
- Procedural fairness
- Evidence-based decisions
- Regulatory compliance
- Documentation of all findings

### **9.2 Stages of Investigation**

#### **Stage 1 – Receipt & Logging**

- Logged on SAMS
- Risk Register updated
- Initial screening completed

#### **Stage 2 – Initial Assessment**

Responsible Officer or Quality Manager determines:

- Nature of allegation
- Severity
- Relevant department
- Whether suspension of activity is necessary
- Whether to notify external authorities

#### **Stage 3 – Appointment of Investigator**

An investigator is appointed who is:

- Independent
- Not connected to the allegation
- Trained and authorised

#### **Stage 4 – Evidence Gathering**

May include:

- Document review
- Interviews (staff, assessors, learners, IEPAs, employers)
- Witness statements
- Assessment or EPA evidence
- NOPS logs
- System audit trails
- Communications data
- Centre records

#### **Stage 5 – Investigation Report**

Investigator produces a report covering:

- Background
- Allegation details
- Evidence summary
- Findings
- Impact assessment
- Recommendations
- Risk level
- Regulatory implications

### **Stage 6 – Decision Making**

Decision approved by:

- Responsible Officer
- CEO
- Smart Awards Board (for serious/high-risk cases)

Decisions include:

- Complaint upheld / partially upheld / not upheld
- Appropriate sanctions
- Reporting to regulators
- Corrective actions

### **Stage 7 – Sanctions Applied**

In accordance with Section 10.

### **Stage 8 – Communication of Outcome**

Written outcome includes:

- Summary
- Findings
- Actions
- Rights to appeal

### **Stage 9 – Lessons Learned**

Added to:

- Improvement Plan
- Quality reports
- Risk assessments

## **9.3 Timeframes**

Smart Awards aims to:

- Complete investigations within **28 days**
- Complex fraud cases (EPA, NOPS, police involvement) may require **up to 60 days**

If timelines cannot be met:

- Complainant is notified
- Revised timeline is provided

## **9.4 Withholding Results or Certificates**

Smart Awards may withhold, Certification, EPA results or NOPS access until investigations are complete.

# **SECTION 10 – SANCTIONS AND CORRECTIVE ACTIONS**

## **10.1 Possible Sanctions**

### **For Individuals (Learners/Apprentices)**

- Invalidation of assessments or EPA results
- Certificate withdrawal
- Reassessment at own cost
- Removal from programme
- Notification to employer

### **For Centres, Employers, Training Providers**

- Action plans
- Mandatory training
- Increased monitoring or sanctions
- Suspension of approval
- Withdrawal of approval
- Contract termination
- Reporting to regulators

### **For Assessors, IQAs, IEPAs, Contractors**

- Removal from role
- Contract termination
- Reporting to professional bodies
- Referral to police or regulators

### **For NOPS Users**

- Suspension of access
- Card invalidation
- Account removal
- Employer notification
- Police notification (fraud or misuse)

## **10.2 Corrective Actions**

Smart Awards may apply:

- Reissue of accurate results
- Correction of records
- Update to systems or processes
- Strengthening of controls
- Centre intervention
- Additional quality assurance measures
- Amendments to training or documentation

## **10.3 Preventive Actions**

Preventive actions may include:

- Additional monitoring
- Staff or IEPA retraining
- Revising procedures
- Updating risk assessments
- Communications and awareness campaigns

# **11. REPORTING & RECORD KEEPING**

11.1 Smart Awards maintains full, accurate records of:

- Fraud allegations
- Investigations
- Evidence
- Outcomes
- Communications
- Regulatory notifications
- Sanctions
- Lessons learned

Records are kept for **7 years** or longer where required.

11.2 Smart Awards reports fraud to:

- Regulators
- Law enforcement
- ICO (data concerns)

- Industry bodies (where relevant)

## 12. REVIEW OF POLICY

This policy is reviewed:

- Annually
- After any significant fraud case
- When regulations change
- Following system or scheme changes
- After internal audit findings

## 13. DEPARTMENT-SPECIFIC FRAUD REQUIREMENTS

### 13.1 Qualifications

Unique Risks

- False certificates
- IQA falsification
- Portfolio manipulation
- Staff assisting learners
- Falsified signatures

Additional Controls

- Validation before certification
- IQA monitoring
- Dual verification of high-risk Centres

### 13.2 EPA

Unique Risks

- IEPA bias or undue influence
- Gateway fraud
- EPA materials misuse
- Collusion with Providers
- Incorrect or manipulated EPA grades

Additional Controls

- Independent investigations
- EPA moderation
- IEPA independence checks
- Adverse Effect evaluation (EPA3)

### 13.3 Apprenticeship Assessments

Unique Risks

- Employer-generated false evidence
- Portfolio falsification
- False workplace logs
- Manipulated progress records

Additional Controls

- Authenticity checks
- On-programme IQA sampling
- Verification of workplace logs

### 13.4 NOPS

Unique Risks

- Card misuse or fraud
- Data manipulation
- Identity fraud
- System access abuse

- Criminal misuse of card or data

#### Additional Controls

- Real-time status checks
- Audit logs
- Employer verification
- Access suspension procedures

## 14. OFQUAL GENERAL CONDITIONS

14.1 A1.2 An awarding organisation must ensure that it undertakes effective management of all risks relating to its activities, including the risk of fraud, and must take all reasonable steps to prevent any Adverse Effect.

14.2 B3.1 An awarding organisation must promptly notify Ofqual when it has cause to believe that any event has occurred, or is likely to occur, which could have an Adverse Effect.

14.3 A5.1 An awarding organisation must ensure the integrity and security of assessment materials, including taking all reasonable steps to prevent the loss, theft, or misuse of such materials.

## 15. OFQUAL APPRENTICESHIP CONDITIONS

15.1 EPA3.1 – EPA Notifications An awarding organisation must promptly notify Ofqual when it has cause to believe that any event has occurred, or is likely to occur, which could have an Adverse Effect.

15.2 EPA3.2(d) An Adverse Effect may include... any failure in assessment delivery which threatens assessors' ability to differentiate accurately and consistently between levels of attainment demonstrated by learners.

15.3 EPA6.3 An awarding organisation must comply with the EPA Qualification Level Conditions in respect of each End-Point Assessment it awards.

## 16. QUALIFICATIONS SCOTLAND ACCREDITATION PRINCIPLES

16.1 Principle 10 The awarding body must ensure the integrity and security of all assessment instruments and certification.

16.2 Principle 13 The awarding body and its providers must have systems and processes to ensure the effective identification and management of malpractice and maladministration.

# APPENDIX 1 – FRAUD & MALPRACTICE RISK ASSESSMENT

**RISK ASSESSMENT TABLE**

<b>Risk Area</b>	<b>Description</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Controls / Mitigation</b>	<b>Owner</b>
False certification	Certificates issued incorrectly or fraudulently	Low	High	Certificate validation, dual checks, system controls	Quality Manager
EPA fraud	IEPA bias, collusion or incorrect grading	Medium	High	Independence checks, moderation, EPA3 notification	EPA Manager
Identity fraud	Impersonation in assessment or EPA	Medium	High	ID checks, invigilation, NOPS verification	Centres / EPA team
NOPS misuse	Fraudulent card or data manipulation	Medium	High	Access controls, audit logs, employer verification	NOPS Manager
Portfolio falsification	Learner work falsification	Medium	Medium	IQA sampling, authentication checks	Centres
System access misuse	Unauthorised system changes	Low	High	Role-based access, monitoring, MFA	IT Manager
Data breaches	Fraud via misuse of data	Low	High	GDPR compliance, secure storage	Data Protection Officer
Centre malpractice	Staff falsification of records	Medium	High	Monitoring, sanctions, training	Quality Manager
External fraud	False claims by third parties	Low	Medium	Verification, employer checks	Smart Awards Teams