



NOPS CERTIFICATE SAMPLING PLAN POLICY



Version Number	Date	Purpose of Change	Classification	Sign Off
1.0		New Document	Public	Tony Ryde
1.1	05/03/2026	Reformat and new template	Public	Marc Henson
1.2	25/03/2026	Content updated	Public	Lesley Barr

Copyright © 2026 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
W: www.smartawards.co.uk

Company Number 9079735 | VAT Number 216 7632

1. OVERVIEW

1.1 NOPS is a central register of operatives' identities, qualifications, accreditations, and job roles within the telecommunications and utilities sectors.

1.2 The scheme provides a mechanism to demonstrate competence, promote safety, and support compliance with industry and legislative requirements.

1.3 Smart Awards is the sole owner, operator, and administrator of NOPS and is responsible for setting standards, maintaining the register, and issuing NOPS cards and digital records.

1.4 NOPS includes both physical cards and digital access via the NOPS App, which enables operatives and authorised organisations to view and verify competency records.

2. OBJECTIVE

2.1 To maintain accurate records of individuals working within utilities trades or occupations who have achieved, or can demonstrate prior achievement of, accredited qualifications or training.

2.2 Additionally, to provide these individuals with appropriate identification and to promote the engagement and use of suitably accredited and qualified personnel across the industry.

3. DEFINITIONS

3.1 For the purposes of this policy:

(a) "Operative" means an individual whose qualifications, accreditations, or job roles are recorded on the NOPS register.

(b) "Employer Organisation" means any company or entity submitting certification on behalf of operatives.

(c) "Certification" means any document or evidence submitted to demonstrate achievement of a qualification, accreditation, or training.

(d) "Fraud" means any deliberate act to falsify, alter, or misrepresent certification or information.

(e) "Maladministration" means any unintentional error, omission, or failure to follow required processes.

(f) "Sampling Period" means a calendar month during which assurance checks are conducted.

(g) "Verification" means the process of confirming the authenticity and validity of submitted certification.

4. SAMPLING PLAN SCOPE

4.1 In order to maintain the accuracy and integrity of the NOPS register, assurance checks shall be conducted throughout each sampling period to verify compliance with this policy. For the purposes of this policy, the "sampling period" shall be defined as a calendar month.

4.2 Certificate submissions may be received from the following sources:

- email requests.
- operative update and/or card update requests.
- training update requests.
- bulk upload requests.

4.3 Smart Awards shall undertake assurance checks on a representative sample of certificate submissions received from all sources.

4.4 The volume of certificate submissions may vary. Accordingly, assurance checks shall be applied using a risk-based and proportionate sampling approach, designed to ensure the ongoing accuracy, reliability, and integrity of the NOPS register.

5. RISK CATEGORIES

5.1 Risk shall be classified into two categories:

- Fraud; and
- Maladministration.

5.2 Non-compliance may arise either through deliberate and planned actions or as a consequence of inadequate, ineffective, or unenforced controls.

5.3 Operatives and employer organisations shall ordinarily be classified as Low Risk when submitting certification to the NOPS register. However, Smart Awards reserves the right to assign a Medium Risk or High-Risk classification where concerns are identified through assurance or verification activities.

5.4 Risk classifications may be determined having regard to, but not limited to, the following indicators:

- Administrative errors within certificate submissions
- Repeated submission of incorrect or incomplete documentation
- Certificates that cannot be verified with the awarding body or training provider
- Evidence of altered, forged or fraudulent certification
- Patterns of non-compliance identified through sampling checks

5.5 Where a risk classification has been applied, Smart Awards may increase the level and frequency of assurance sampling applied to submissions from the relevant operative or employer organisation.

5.6 Risk classifications shall ordinarily be applied as follows:

Risk	Description
Low	Applied to operatives and employer organisations where no concerns are identified through routine sampling or verification checks.
Medium	Applied to operatives and employer organisations where repeated administrative errors or documentation issues are identified. Submissions may be subject to increased sampling or 100% verification.
High	Applied to operatives and employer organisations where fraudulent certification, suspected falsification, or deliberate attempts to misrepresent qualifications are identified. Submissions will be subject to 100% verification and may be escalated for formal investigation.

5.7 Risk classifications shall normally remain in effect for a minimum monitoring period of six (6) months. Where no further issues are identified during this period, the classification may be reduced. Where additional concerns arise, the monitoring period may be extended and further assurance measures implemented.

6. SAMPLING METHODOLOGY AND VOLUMES

6.1 Assurance checks will be carried out as follows:

- All certificate submissions received through operative uploads or email requests will be subject to assurance checks.
- Certificate submissions received through other submission methods will be subject to assurance sampling.
- A sample of 10% of certificate submissions will normally be selected for assurance checks.
- Where total submission volumes fall below one hundred certificates within the sampling period, 100% of certificates will be assurance checked.
- The sample size will not usually exceed one thousand certificates within the sampling period.

6.2 The sampling methodology used within this policy is designed to ensure an appropriate level of assurance that submitted certification is valid and compliant. The approach aligns with generally accepted industry sampling principles and supports the identification of potential fraud or maladministration.

6.3 Should fraud or maladministration be identified, Smart Awards reserves the right to investigate further.

7. SAMPLING ACTIVITY AND VERIFICATION

7.1 Smart Awards shall undertake planned sampling in accordance with its prescribed sampling volumes. Assurance checks shall be conducted using either random or targeted methodologies, as determined by the nature and level of risk identified.

(a) **Random Sampling:** Random sampling shall be undertaken as part of the core assurance programme and shall consist of due diligence checks distributed proportionately across all submission sources.

(b) **Targeted Sampling:** Targeted sampling shall be applied where indicators suggest that fraud or maladministration may have occurred. Such sampling shall adopt a focused approach and may include, but shall not be limited to, increased sampling rates within specific areas and retrospective review of historical submissions.

(c) **Outcomes and Actions:** Actions arising from sampling activities shall include, but shall not be limited to:

- acceptance of certification deemed compliant;
- rejection of certification where maladministration is identified, with a requirement for corrective action; and
- escalation and reporting of suspected or confirmed fraud to the Smart Awards Responsible Officer for investigation, guidance, and appropriate corrective action.

7.2 Where operatives or employer organisations are classified as Medium Risk or High Risk, Smart Awards shall apply targeted sampling measures. Such measures may include increased sampling volumes, retrospective verification of historical submissions, and/or direct validation with awarding organisations or training providers.

7.3 Verification checks shall include, but shall not be limited to, the following:

- confirming that the certificate constitutes valid and acceptable evidence of the relevant qualification or accreditation.
- verifying that the name stated on the certificate corresponds with the operative associated with the submission.
- checking issue dates and expiry dates to ensure the qualification or accreditation remains valid.

- verifying the authenticity of the certificate using available verification methods, including but not limited to QR codes, awarding body databases, or confirmation from the training provider.
- where applicable, confirming that assessor or trainer details correspond with recognised or authorised personnel.
- reviewing the certificate for any indication of alteration, falsification, or inconsistency with known templates or standard formats.

8. ESCALATION AND SANCTIONS

8.1 Where fraud or serious non-compliance is identified, Smart Awards shall escalate the matter in accordance with its malpractice and maladministration procedures.

8.2 Actions may include:

- suspension of submissions
- removal or withholding of certification records
- referral to awarding organisations or regulatory bodies
- formal investigation.

8.3 Smart Awards reserves the right to apply additional controls or restrictions where necessary to protect the integrity of the NOPS register.

9. RESPONSIBILITY

9.1 **Smart Awards** - Smart Awards shall be responsible for:

- maintaining appropriate systems and controls to support the integrity and accuracy of the NOPS register.
- implementing assurance, verification, and sampling processes in accordance with this policy.
- taking appropriate action where non-compliance, maladministration, or fraud is identified.

9.2 **Employer/organisations responsibility** – Employers/organisations submitting certification to the NOPS register shall be responsible for ensuring that:

- all certificates submitted are genuine, accurate, complete, and relate to the individual named within the submission.
- appropriate due diligence is undertaken prior to submission, including but not limited to verifying that the relevant training or assessment has been completed with an approved or recognised training provider.
- ensuring that all submitted documentation is authentic and has not been altered, falsified, or otherwise misrepresented.

9.3 **Operative responsibility** - Operatives submitting certification to the NOPS register shall be responsible for ensuring that:

- all certificates submitted are genuine, accurate, complete, and relate to themselves.
- they undertake appropriate due diligence prior to submission confirming that the training or assessment has been completed with an approved or recognised training provider.
- ensuring that any documentation provided has not been altered, falsified, or otherwise misrepresented.

10. RECORD KEEPING AND AUDIT

10.1 Smart Awards shall maintain records of all sampling activities, outcomes, and actions taken.

10.2 Records shall be retained in accordance with data retention and audit requirements.

10.3 Sampling records shall be made available for audit and regulatory review where required.

11. APPEALS

11.1 Employers, organisations and operatives shall have the right to challenge decisions made under this policy.

11.2 Appeals shall be submitted in accordance with Smart Awards' appeals procedure and within defined timeframes.

12. MONITORING AND REVIEW

12.1 This policy shall be reviewed annually, or sooner where required due to changes in legislation, industry requirements, or identified risks.

12.2 Smart Awards shall monitor the effectiveness of this policy through ongoing assurance and audit activities.

13. DATA PROTECTION

13.1 All personal data processed under this policy shall be handled in accordance with applicable data protection legislation, including the UK GDPR and Data Protection Act 2018.