GDPR AND DATA PROTECTION POLICY

SMART AWARDS
Awarding Platform for Smart Qualifications

Version Number	Date	Purpose of Change	Classification	Sign Off
V4.1	10/11/2025	Merge of NOPs, EPA and Awarding policies - new content and formatting	Public	Kerry Ore

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. SCOPE

1.1 Smart Awards needs to collect, store, and process personal information about individuals, centres, employers, training providers, learners, apprentices, assessors, and staff to carry out its functions effectively across qualifications, apprenticeship assessments, End-Point Assessments (EPAs), and Network Operator Programmes (NOPs).

1.2 This policy ensures compliance with the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) and applies to all personal data handled by Smart Awards in any format (digital, written, photographic, or recorded).

1.3 It covers all staff, contractors, centres, employers, training providers, apprentices, learners, and third parties who access or process data on behalf of Smart Awards.

2. POLICY STATEMENT

2.1 Smart Awards is committed to ensuring the lawful, fair, and transparent processing of all personal data.

2.2 Smart Awards complies with all relevant UK and EU data protection laws, safeguarding the "rights and freedoms" of individuals whose data we collect and process.

2.3 This policy applies to all Smart Awards operations, including qualifications, apprenticeship assessments, EPAs, and NOPs.

2.4 The Data Protection Officer (DPO) oversees compliance, ensuring that processing activities are reviewed annually and that the organisation maintains a Record of Processing Activities (ROPA) for inspection by the Information Commissioner's Office (ICO) upon request.

2.5 Smart Awards has established objectives for data protection and privacy that are:

- Consistent with this policy;
- Measurable and reviewed annually;
- Communicated to all employees and delivery partners; and
- Integrated into risk management and compliance processes.

2.6 Partners, centres, employers, and any third parties who process or have access to Smart Awards' data must comply with this policy and enter into a data processing or confidentiality agreement.

2.7 All Smart Awards staff and associates receive data protection training and are contractually bound by this policy. Breaches are treated as disciplinary matters and may also be reported to the ICO where appropriate.

3. DATA CONTROLLER AND PROCESSOR

3.1 Smart Awards acts as both a Data Controller and Data Processor under the Data Protection Act 2018 and GDPR.

3.2 As the Data Controller, Smart Awards determines how and why personal data is processed. As the Data Processor, Smart Awards handles data on behalf of approved centres, employers, and training providers.

3.3 Smart Awards is registered with the Information Commissioner's Office (ICO) and maintains accurate records of all data processing activities.

3.4 A Data Protection Impact Assessment (DPIA) will be completed where new technology, activities, or systems present potential risks to individuals' rights or privacy.

3.5 DPIAs will also be undertaken when new qualifications, apprenticeship standards, EPAs, or NOPs are developed or delivered.

4. DISCLOSURE

4.1 Smart Awards may share data with third parties such as regulators, funding bodies, employers, or industry partners where legally required or operationally necessary.

4.2 Data will only be disclosed when:

- Required by law;
- The data subject has consented;
- Disclosure is necessary to protect vital interests;
- It is part of a regulatory investigation or quality assurance activity.

4.3 All disclosures are controlled, recorded, and subject to review.

5. RESPONSIBILITIES

5.1 Smart Awards' Board of Directors has overall accountability for compliance with data protection legislation.

5.2 The Data Protection Officer (DPO) ensures operational compliance and provides guidance to staff and partners.

5.3 All staff, centres, employers, training providers, and contractors must:

- Follow this policy and associated procedures;
- Keep data accurate, relevant, and up to date;
- Report any breaches immediately.

5.4 Line managers are responsible for promoting good information-handling practices in their teams.

6. DATA SUBJECT RIGHTS

6.1 Smart Awards recognises and upholds the rights of all individuals (data subjects) as defined by the GDPR:

- Right to be informed: Clear information about how data is collected and used.
- Right of access: Individuals can request copies of data held about them.
- Right to rectification: Incorrect or incomplete data will be corrected promptly.
- Right to erasure ("right to be forgotten"): Individuals can request deletion of their personal data.
- Right to restrict processing: Processing may be limited while accuracy or legality is verified.
- Right to data portability: Individuals may request a copy of their data in a usable format.
- Right to object: Individuals can object to certain types of processing (e.g., direct marketing).
- Rights related to automated decision-making and profiling: Individuals can request human review of decisions made solely by automated means.

7. DATA PROTECTION PRINCIPLES

7.1 Smart Awards adheres to the seven key GDPR principles:

1. Lawfulness, fairness, and transparency
2. Purpose limitation – Data is collected for specific, legitimate purposes only.

3. Data minimisation – Data collected is adequate, relevant, and limited.
4. Accuracy – Data must be accurate and updated regularly.
5. Storage limitation – Data is kept only as long as necessary.
6. Integrity and confidentiality (security) – Data must be kept secure at all times.
7. Accountability – Smart Awards must demonstrate compliance at all times.

8. GENERAL GUIDELINES

8.1 All Smart Awards personnel and delivery partners must ensure that:

- Personal data is only accessed by authorised individuals.
- Strong passwords are used and changed regularly.
- Personal data is never shared informally or without authority.
- Printed documents are stored securely and disposed of confidentially.
- Data is processed only for lawful and stated purposes.
- Email and IT systems are protected by encryption, antivirus software, and firewalls.
- Data processing risks are logged on the organisation's Risk Register.

9. DATA PROTECTION OFFICER (DPO)

9.1 The DPO is responsible for:

- Ensuring policy compliance across all areas of Smart Awards.
- Responding to data subject requests.
- Maintaining the Record of Processing Activities (ROPA).
- Reviewing and reporting any data breaches.
- Liaising with the ICO and other regulatory bodies.
- Providing staff training and auditing internal data practices.

10. DATA COLLECTION AND INFORMED CONSENT

10.1 Smart Awards will obtain informed consent where required and ensure that individuals:

- Understand why their data is needed and how it will be used.
- Provide consent freely and voluntarily.
- Are informed of their right to withdraw consent at any time.
- For children under 16, parental or guardian consent will be obtained before any personal data is processed.

11. DATA SHARING

11.1 Data is shared only where necessary for delivery, certification, or quality assurance purposes. Before sharing data, Smart Awards will verify that the recipient has equivalent data protection safeguards in place. All data sharing is approved by the DPO and logged for accountability.

12. HANDLING DATA AND DATA SECURITY

12.1 All Smart Awards staff and approved partners must:

- Keep all personal and company data secure.
- Lock computers when unattended.
- Use encrypted systems for data storage and transfer.
- Never share passwords or access credentials.
- Dispose of physical and electronic data securely after retention periods expire.

13. DATA STORAGE

13.1 Smart Awards will ensure:

- Electronic data is stored on secure servers protected by encryption and access control.
- Paper files are kept in locked, fireproof cabinets.

- Backup systems are maintained and tested regularly.
- Passwords meet organisational security standards.
- Data is regularly reviewed, updated, and archived appropriately.

14. DATA ACCESS AND ACCURACY

14.1 Individuals may request access to data held about them through a Subject Access Request (SAR). Smart Awards will verify the requester's identity before disclosure and respond within one month. Data found to be inaccurate will be corrected promptly and third parties notified.

15. SUBJECT ACCESS REQUESTS (SARs)

15.1 Requests must be submitted in writing (including email).

15.2 Responses will include:

- Confirmation that data is held.
- Details of the processing purpose.
- Categories of data.
- Recipients or categories of recipients.
- Data retention period.
- Details of the individual's rights and complaint routes.

15.3 SARs are managed by the DPO in accordance with GDPR Article 15.

16. DESTROYING PERSONAL DATA

16.1 Data will be retained only as long as necessary for business or legal reasons and securely deleted when no longer required. Secure disposal methods include shredding, data wiping, and destruction of hard drives.

17. DATA BREACHES AND RISKS

17.1 All suspected breaches must be reported immediately to the DPO. Breaches will be investigated and, where necessary, reported to the ICO within 72 hours. Records of all incidents, outcomes, and corrective actions will be maintained.

18. DATA PROTECTION AND THE LAW

18.1 This policy complies with the Data Protection Act 2018, UK GDPR, and other related legislation. It also supports compliance with Ofqual, Qualifications Scotland Accreditation regulations requiring secure and ethical management of learner, apprentice, and assessment data.

19. ARCHIVING AND RETENTION

19.1 Smart Awards maintains an Information Asset Register and Records Retention Schedule to ensure that data is archived, retained, and disposed of appropriately. Retention periods are set according to regulatory, financial, and contractual requirements.

20. INFORMATION ASSET REGISTER / DATA INVENTORY

20.1 Smart Awards maintains a live Data Inventory identifying:

- Types and sources of personal data.
- Purpose of processing.
- Data owners and access levels.
- Retention and disposal requirements.

21. REVIEW OF THIS POLICY

21.1 This policy is reviewed annually, or sooner if required, in response to feedback, legislative updates, or regulatory guidance from Ofqual, SQA Accreditation, or other relevant authorities.

22. OFQUAL GENERAL CONDITIONS

22.1 Condition A1.2 An awarding organisation must ensure that its governance arrangements are appropriate to its activities and include effective arrangements to maintain compliance with its Conditions of Recognition.

22.2 Condition A8.1 An awarding organisation must take all reasonable steps to prevent the occurrence of any malpractice or maladministration in the development, delivery and award of qualifications which it makes available or proposes to make available.

22.3 Condition B3.2 – Such events include where there has been a loss or theft of, or a breach of confidentiality in, any assessment materials, or an incident of malpractice or maladministration that could invalidate an award or affect another awarding organisation.

22.4 Condition G4.1 – An awarding organisation must take all reasonable steps to ensure the confidentiality of assessment materials and ensure secure storage, controlled access, and appropriate transmission.

22.5 Condition H5.1 – An awarding organisation must retain evidence of assessment and decisions for a period that enables effective monitoring, appeals, and regulatory review.

23. OFQUAL APPRENTICESHIP CONDITIONS

23.1 Condition EPA6.1 – An end-point assessment organisation must take all reasonable steps to ensure that any assessment materials, information, or data are kept secure and confidential at all times and are not disclosed to unauthorised persons.

23.2 Condition EPA6.2 – An end-point assessment organisation must establish, maintain, and comply with up-to-date written procedures relating to the secure handling, transmission, and storage of all data and information relating to apprentices and assessment outcomes.

24. QUALIFICATIONS SCOTLAND ACCREDITATION PRINCIPLES

24.1 Principle 4 – Identification and Management of Risk. The awarding body must demonstrate an effective approach to the identification and management of risk.

24.2 Principle 6 – Internal Review and Audit. The awarding body must have effective arrangements for internal review and audit of its systems, policies, and procedures.

24.3 Principle 12 – Malpractice and Maladministration. The awarding body and its providers must ensure that they have the necessary arrangements and resources to prevent, investigate, and manage cases of malpractice and maladministration.

24.4 Principle 18 – Data Protection and Record Keeping. The awarding body and its providers must ensure that personal data is processed, stored, and disposed of securely and in accordance with the Data Protection Act 2018 and the UK GDPR requirements.