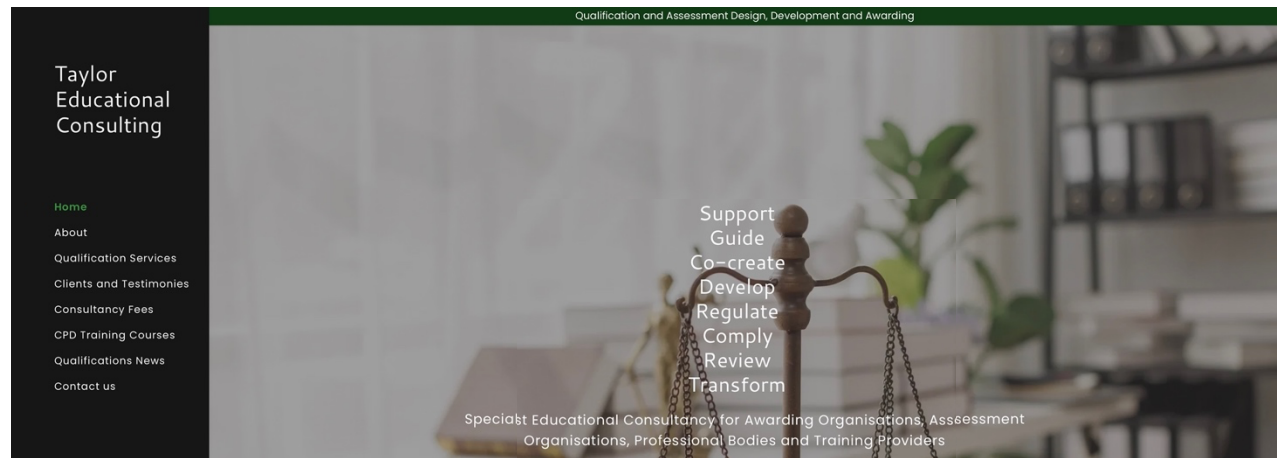




# Responsible Use of AI in Awarding and Assessment

## A Practical Guide for the Design, Development and Assessment of Qualifications

Ethical Practice, Human Accountability and Organisational Governance

## **Copyright, Use and Disclaimer**

This document is provided as a general information and professional guidance resource for awarding organisations, assessment organisations, professional bodies and related education and assessment providers. It must not be copied, reproduced, adapted, sold, republished, distributed or incorporated into another organisation's materials without prior written permission from Taylor Educational Consulting.

The content is intended to support discussion, reflection and good practice. It does not constitute legal advice, regulatory advice or data protection advice, and organisations remain responsible for ensuring that their own use of AI complies with applicable law, regulatory requirements, contractual obligations, information security requirements, intellectual property rights and internal governance arrangements.

No responsibility is accepted for any reliance placed on this document without appropriate professional review and organisation-specific consideration.

## **Sharing and Citation Statement**

This resource may be shared with colleagues, teams and professional networks for information, discussion and internal training purposes, provided that it is shared in full, unamended, and with clear acknowledgement of the author and source.

This document must not be copied, adapted, rebranded, sold, incorporated into paid training materials, or presented as another organisation's own work without prior written permission from Taylor Educational Consulting.

## Table of Contents

|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| Executive summary.....                                                      | 5  |
| Introduction .....                                                          | 6  |
| Ethical and responsible AI use .....                                        | 7  |
| GDPR, confidentiality and embedded content .....                            | 8  |
| Ways to retain confidentiality.....                                         | 10 |
| 1. Use anonymised scenarios .....                                           | 10 |
| 2. Use representative examples rather than real documents .....             | 10 |
| 3. Remove identifiers and unnecessary detail .....                          | 10 |
| 4. Summarise the issue instead of uploading the document .....              | 11 |
| 5. Use placeholders .....                                                   | 11 |
| 6. Ask for frameworks, not direct handling of confidential content .....    | 11 |
| 7. Use redacted extracts .....                                              | 12 |
| 8. Separate sensitive data from the drafting task.....                      | 12 |
| 9. Use approved methods where sensitive information is unavoidable .....    | 12 |
| 10. Keep human accountability .....                                         | 13 |
| 11. AI does not replace expertise .....                                     | 13 |
| Practical ways AI can be used in awarding and assessment organisations..... | 14 |
| 1. Qualification development.....                                           | 14 |
| 2. Assessment design.....                                                   | 14 |
| 3. Assessment banks and item writing .....                                  | 15 |
| 4. Mark schemes and grading descriptors .....                               | 15 |
| 5. Policy generation and policy review .....                                | 15 |
| 6. Governance frameworks.....                                               | 16 |
| 7. Regulatory mapping and evidence checks.....                              | 16 |
| 8. Centre approval and centre monitoring.....                               | 17 |
| 9. CASS and quality assurance activity.....                                 | 17 |
| 10. Staff training, induction and workforce documentation.....              | 17 |
| 11. Standardisation and training.....                                       | 18 |
| 12. Malpractice and authenticity controls .....                             | 18 |
| 13. Data analysis and risk monitoring .....                                 | 19 |
| 14. Operational documentation and communications.....                       | 19 |
| AI memory, organisational learning and consistency .....                    | 20 |
| Governance and responsible use .....                                        | 21 |
| Practical principles for ethical AI use .....                               | 22 |
| Summary of unacceptable use .....                                           | 23 |

|                                                                |    |
|----------------------------------------------------------------|----|
| Example content for a Generative AI Policy (staff facing)..... | 24 |
| AI Governance Self-Audit Checklist for Organisations.....      | 25 |
| Emerging considerations.....                                   | 26 |
| Further reading and resources .....                            | 26 |
| Conclusion .....                                               | 27 |
| About Taylor Educational Consulting.....                       | 28 |

Copyright (c)

## Executive summary

This guidance sets out how awarding organisations, end-point assessment organisations and professional bodies can use generative AI safely, ethically and effectively during their lifecycles of design, development and assessment. It emphasises that AI is a powerful support tool, not a replacement for professional judgement, subject expertise or accountable human decision-making.

Key messages:

- AI can improve efficiency, consistency and quality across qualification development, assessment design, policy, governance, quality assurance and operations but only when used with appropriate controls
- Confidentiality, GDPR, intellectual property and assessment security must be protected. Organisations should minimise sensitive data shared with AI tools and prefer anonymised scenarios, placeholders, frameworks and approved enterprise platforms
- Human accountability is non-negotiable. Any AI-assisted output that supports regulated activity must be reviewed by competent subject and assessment experts before use.
- Clear organisational governance is essential: approved tools, documented processes, staff training, risk registers and periodic review
- The strongest organisations will neither ignore AI nor adopt it uncritically. They will build controlled, transparent and defensible practices that strengthen rather than weaken validity, fairness and public confidence.

This document addresses a current gap in sector guidance. While Ofqual and JCQ provide important high-level and centre-focused material, there is limited explicit operational detail on the practical boundaries, safeguards and processes awarding organisations should apply when using generative AI in their own internal activities (qualification development, item writing, policy, quality assurance and governance).

This document provides practical methods for using AI to produce efficiency in the Design, Development and Assessment of Qualifications.

# Introduction

Artificial intelligence is now part of the qualifications and assessment landscape, and its use and capability are moving at pace. For awarding organisations, end-point assessment organisations, professional bodies and other assessment organisations, the question is no longer whether AI should be acknowledged. It is how it can be used safely, ethically and intelligently across qualification development, assessment design, item banking, policy development, quality assurance, governance, centre support, workforce development and operational delivery without weakening validity, fairness, security or public confidence.

Evolving frameworks such as the EU AI Act classify certain education and assessment systems as high-risk, while global reports and professional standards emphasise the need for robust oversight in assessment redesign.

While Ofqual has published its high-level approach to regulating AI use by awarding organisations and JCQ has issued detailed guidance for centres on managing learner use of AI in non-exam assessment, neither currently sets out explicit operational detail on the practical boundaries, safeguards and processes that awarding organisations themselves should apply when using generative AI in their internal activities (such as qualification development, item writing, policy drafting, mark scheme development, quality assurance and governance).

This document seeks to help fill that gap by providing sector-specific, practical guidance on responsible use within awarding and assessment organisations.

There is understandable caution across the sector. AI can create risks around regulatory compliance, authenticity, over-reliance, intellectual property, confidentiality, GDPR, embedded data, bias and poor-quality outputs. However, it can also support better assessment design, stronger quality assurance, more consistent operational processes and improved centre and learner support.

The key is to use AI as a controlled support tool, not as an unchecked decision-maker.

Just as importantly, AI is only as useful as the person directing it. Poor prompts, weak source material and limited subject understanding will usually produce poor or misleading outputs. In assessment and awarding contexts, the person using generative AI needs to understand the qualification, the subject area, the assessment methodology, the regulatory context and the purpose of the task.

Without that expertise, they may not ask the right questions, may accept inaccurate outputs, or may fail to notice that the content is not valid, proportionate, level-appropriate or fit for purpose.

In short, quality input is a prerequisite to production of quality output.

## Ethical and responsible AI use

Before considering how AI can support awarding and assessment activity, organisations need to be clear about how it should be used ethically.

This includes protecting confidential information, intellectual property, assessment security, personal data and the rights of organisations, centres, employers, learners, authors and assessment writers.

Staff and consultants should not upload entire specifications, live assessment materials, item banks, mark schemes, learner submissions, centre reports, branded documents, business plans, board papers, contracts, commercial proposals or internal governance documents into public AI tools unless the organisation has formally approved the platform and is satisfied that data, confidentiality, intellectual property and contractual requirements are protected.

This is particularly important where documents contain:

- Confidential assessment content
- Live or secure questions
- Unpublished specifications
- Centre or learner data
- Commercial information
- Business plans or financial assumptions
- Client names or client-specific information
- Third-party intellectual property
- Logos, branding or copyright material
- Author-created content
- Assessment materials owned by another organisation
- Sensitive quality assurance findings
- Board papers or governance records
- Contracts, tenders, commercial proposals
- Staff information or role-specific employment data.

Sharing business information with an AI tool simply to achieve a faster output is not acceptable unless the organisation has considered whether the information can lawfully and safely be shared. Efficiency does not override confidentiality, GDPR, assessment security, intellectual property rights or contractual obligations.

A safer approach is to minimise and anonymise the information entered into AI tools. For example, instead of uploading an entire branded qualification specification, a user might extract a small, non-confidential section, remove branding and identifiers, summarise the context, and ask AI to comment on wording clarity or level demand.

Instead of uploading a live assessment paper, they might provide a fictional example or a short representative extract that does not compromise assessment security.

Ethical AI use should be based on necessity, proportionality and control.

The organisation should ask whether:

- AI is needed for the task
- What the minimum necessary information is
- Whether the material is confidential, secure, copyrighted or commercially sensitive
- Whether it contains personal or embedded personal data
- Whether it has been anonymised or de-identified
- Whether the organisation is permitted to use the material in this way
- Whether the platform stores or reuses the content entered
- Who will check the output
- How human review and final approval will be documented.

AI should not become a route for casually exposing and unwittingly harvesting intellectual property, learner data, business information or secure assessment material.

## GDPR, confidentiality and embedded content

GDPR and confidentiality need specific attention. Awarding and assessment organisations routinely handle personal data, special category data, learner records, centre information, employer details, staff information, complaints, appeals, malpractice evidence and assessment records. This information must not be entered into public AI tools without a lawful basis, appropriate safeguards and organisational approval.

Even where a document appears to have been anonymised, it may still contain hidden or embedded information. This can include metadata, tracked changes, comments, author names, file properties, version history, email trails, embedded spreadsheets, hidden tabs, image data, previous edits or copied content from another source.

This means that simply deleting a name from the visible text is not always enough. Before any material is used with AI, organisations should consider whether the document contains hidden identifiers, embedded content or residual information that could disclose personal, confidential or commercially sensitive data.

Documents should be checked carefully before use. Where possible, users should work from clean extracts rather than uploading original files. They should remove names, centre details, learner numbers, employer references, logos, watermarks, comments, tracked changes and any unnecessary contextual information. Where tables or spreadsheets are used, hidden rows, hidden columns, hidden tabs and formulas should also be checked.

Confidentiality obligations may also arise from contractual agreements such as:

- Centre agreements
- Associate agreements
- Employment contracts
- Non-disclosure agreements
- Regulator correspondence
- Client instructions

An organisation should not share confidential information with an AI system even where the content does not contain personal data. Confidentiality is wider than GDPR.

The same applies to commercially sensitive information. Business plans, pricing models, tenders, financial forecasts, pipeline data, staffing models, client lists, market strategies and board papers should not be uploaded to public AI tools simply because doing so would make drafting easier.

A useful working principle is:

*If the organisation would not send the information to an unknown third party by email, it should not be entered into an uncontrolled AI tool.*

Organisations should distinguish between general public/consumer AI tools (such as the standard versions of ChatGPT, Claude or Gemini) and approved enterprise or private instances.

Enterprise platforms frequently offer stronger contractual safeguards, including no-training clauses (data is not used to improve the model), specified data residency, detailed audit logs, and easier deletion of conversation history. Where any sensitive, confidential, personal or regulated information must be processed with AI, only approved enterprise platforms with appropriate legal, data protection and information security review should be used.

Confidentiality does not mean AI cannot be used. It means AI must be used carefully, with only the information needed to achieve the task and without exposing sensitive, secure, personal or commercially confidential material.

A useful principle is:

*Share the context needed for the task, not the confidential content itself.*

For example, an organisation may need help drafting a centre monitoring checklist. The AI tool does not need the names of actual centres, previous EQA findings, learner records or confidential performance data. It only needs to know the type of organisation, the purpose of the checklist, the intended audience, the broad assessment model and the areas that should be covered.

Similarly, if an organisation wants support with writing job descriptions, the AI tool does not need salary negotiations, internal staffing issues, named employees, board discussions or commercially sensitive restructuring plans.

The role title, broad responsibilities, reporting line, competence requirements and organisational context are all that is required.

# Ways to retain confidentiality

There are several practical ways to retain confidentiality while still using AI effectively.

## 1. Use anonymised scenarios

Instead of sharing real centre, learner, employer or client information, convert the issue into an anonymised scenario.

For example, instead of writing:

*Centre X has failed two EQA visits and has poor assessment records for the Level 3 Diploma in X.*

Use:

*A centre has repeated quality assurance actions relating to incomplete assessment records and weak internal quality assurance. Draft a proportionate escalation plan for an awarding organisation.*

This provides enough context for AI to assist without exposing the identity of the centre, the qualification, the learners or the commercial relationship.

## 2. Use representative examples rather than real documents

Where possible, create a fictional or representative example rather than uploading an original document.

For example, instead of uploading a live assessment task, provide a simplified mock task that reflects what you want to assess. Provide a short, non-confidential extract that shows the level and structure you want reviewed.

This allows AI to support review, drafting or challenge without compromising secure or proprietary material.

## 3. Remove identifiers and unnecessary detail

Before using AI, remove information that is not essential to the task. This may include learner names, learner numbers, centre names, employer names, staff names, assessor names, client names, qualification numbers, contract values, commercial rates, financial data, internal email trails, logos and branding, document reference numbers, board or committee names where unnecessary, and geographical details where they could identify the organisation.

The aim is to provide enough information for AI to understand the task, but not enough information to identify the organisation, learner, centre, client or confidential matter.

## 4. Summarise the issue instead of uploading the document

In many cases, it is safer to summarise the issue in your own words rather than upload the source document.

For example:

*I need to draft a policy section explaining how an assessment organisation manages conflicts of interest. The organisation uses freelance assessors, requires annual declarations, records conflicts on a register and escalates high-risk conflicts to the Responsible Officer. Draft a concise section for a policy.*

This is ethically safer than uploading the actual conflicts policy, staff declarations, board papers or client-specific governance records and asking for AI to review it and produce a new version.

## 5. Use placeholders

Placeholders allow the AI tool to work with the structure of the content without receiving the sensitive information.

For example:

*Draft a centre action plan letter using the following placeholders: [CENTRE NAME], [QUALIFICATION TITLE], [ACTION REQUIRED], [DEADLINE], [EQA NAME].*

This allows the user to insert the sensitive or specific information afterwards, outside the AI tool.

## 6. Ask for frameworks, not direct handling of confidential content

AI can often help by producing a framework, checklist, structure or set of questions rather than needing access to confidential information.

For example, instead of uploading a confidential investigation report, ask:

*Create a malpractice investigation report template for an awarding organisation, including sections for allegation, evidence reviewed, learner response, centre response, findings, decision, rationale, sanctions and appeal rights.*

This gives the organisation a usable structure without exposing the actual case.

## 7. Use redacted extracts

Where some original wording is needed, use short, redacted extracts rather than whole documents.

For example, a user might provide one anonymised assessment criterion or a short, redacted policy paragraph and ask for a clarity review. This is safer than uploading the full specification, policy suite or assessment material.

Redaction should be meaningful. It should remove visible identifiers, but users should also check for comments, tracked changes, file metadata, embedded tables, hidden tabs and document properties.

## 8. Separate sensitive data from the drafting task

AI can help draft the general wording, but the sensitive details should be added manually afterwards.

For example, AI can draft a generic centre monitoring report structure. The SME or quality lead can then complete the actual findings, centre name, qualification details, learner evidence and actions within the organisation's own secure system.

This approach keeps confidential data inside the organisation while still using AI to improve structure, clarity and consistency.

## 9. Use approved methods where sensitive information is unavoidable

If there is a genuine need to use sensitive or confidential information with AI, this should only be done through an approved system with appropriate contractual, technical and data protection safeguards.

The organisation should be clear about whether the tool stores prompts or uploaded documents, whether data is used to train the model, where data is processed and stored, who can access the content, how long information is retained, whether information can be deleted, whether the tool meets the organisation's GDPR and information security requirements, and whether use is covered by privacy notices, contracts and internal policies.

Public AI tools should not be treated as secure repositories for business, learner, centre, staff or assessment information.

## 10. Keep human accountability

Even where confidentiality has been protected, AI outputs must still be checked. The user remains responsible for ensuring the final document is accurate, appropriate, lawful, fair and aligned to the organisation's actual procedures.

AI can help with structure, wording, challenge and consistency. It should not become a substitute for secure systems, professional judgement, regulatory understanding or information governance.

The safest approach is to give AI the minimum context needed to support the task, keep sensitive information out of the tool wherever possible, and complete the final organisation-specific detail within approved internal systems.

A generative AI agent is a sophisticated tool that can improve process efficiency, free up resources and support development, but it is not your own personal assistant that you rely on to do your work for you.

## 11. AI does not replace expertise

One of the biggest risks in using generative AI is the assumption that because an output is fluent, it is correct.

AI can produce confident but inaccurate, shallow or inappropriate content. It may misunderstand the level of demand, misuse command verbs, create unrealistic scenarios, miss regulatory implications, invent requirements, weaken assessment validity or produce wording that appears polished but is not technically sound.

This is why AI should be used by, or under the direction of, people with relevant expertise who can make sound judgement calls.

In awarding and assessment organisations, this may include qualification developers, assessment designers, subject specialists, responsible officers, quality assurance leads, moderators, EQAs, psychometricians, regulatory specialists or experienced operational leads.

The person using AI needs to know whether the output makes sense. They need to recognise when the language is too generic, when the task does not assess the intended outcome, when the grading descriptor lacks progression, or when a suggested control would be impractical or disproportionate.

AI can assist professional judgement. It must not be used to replace it.

A useful principle is:

*AI may help generate, organise, challenge or refine content, but a competent human must remain accountable for the final judgement.*

# Practical ways AI can be used in awarding and assessment organisations

AI can support a wide range of activities across awarding organisations and assessment organisations, provided it is used ethically, securely and with appropriate expert oversight.

## 1. Qualification development

AI can support the drafting, review and refinement of learning outcomes, assessment criteria, indicative content, qualification rationales, unit structures and qualification review documents. It can help identify duplication, unclear wording, weak progression, inappropriate command verbs or gaps between the qualification purpose and assessment model.

It can also support early stage thinking around qualification structure, guided learning hours, total qualification time, optional routes, unit sequencing, level alignment and progression pathways.

However, final qualification design must remain the responsibility of competent subject and assessment specialists. Organisations should avoid uploading entire specifications, branded materials or unpublished qualification documents into public AI tools. Where AI is used, information should be minimised, anonymised and checked before use.

### Example prompt

*As an experienced qualification developer and assessment specialist - draft three learning outcomes and associated assessment criteria at Level 3 for a unit on [TOPIC]. The outcomes should be clear, measurable, use appropriate command verbs, show progression from knowledge to application/evaluation, to suit a qualification with both knowledge and practical skills assessment. Provide a short rationale for level and demand. Output in clean, ready-to-edit format.*

## 2. Assessment design

AI can assist with the development of assessment briefs, scenarios, case studies, professional discussion prompts, viva questions, observation records, practical tasks, controlled assessment materials and learner-facing instructions. It can help test whether tasks are clear, level-appropriate and sufficiently applied.

AI can also be used to stress-test whether an assessment is overly vulnerable to generic AI-generated responses. This is particularly useful for essays, portfolios, reflective accounts, research tasks and unsupervised written evidence.

However, AI should not be used to produce final assessment materials without expert lifecycle management, such as review, mapping, quality assurance, version control, approval and sign off.

### 3. Assessment banks and item writing

AI can support the creation and review of question banks, scenario banks, viva banks, professional discussion banks, MCQ items, short-answer questions and resit variations.

It can also help identify weak distractors, cueing, ambiguity, overlapping answers, construct-irrelevant complexity, excessive reading load, negative phrasing, poor alignment to learning outcomes or KSs, and items that test recall when application is required.

However, secure item banks, answer keys and live assessment materials should not be uploaded into public AI tools. AI-generated items should never be treated as assessment-ready. They require technical review, subject review, bias and sensitivity review, mapping, trialling where appropriate, and post-assessment performance analysis.

### 4. Mark schemes and grading descriptors

AI can help review mark schemes, rubrics and grading descriptors for clarity, progression and consistency. It can support the drafting of assessor guidance, standardisation examples and feedback wording.

This is particularly useful where assessment relies on professional judgement rather than single correct answers. AI can help teams consider whether assessors have enough information to make consistent decisions.

However, the person reviewing the output must understand the assessment model. AI may suggest language that sounds better but actually changes the standard, reduces demand or creates criteria that are harder to assess. It may also produce descriptors that are too generic to support reliable judgement.

AI should support the development and review of mark schemes,  
not make final assessment or awarding decisions.

#### Example prompt

*Review the following draft grading descriptor [insert draft descriptor]. Comment on clarity, consistency, whether it supports reliable judgements, level appropriateness, and any risks of construct-irrelevant variance. Provide a revised version.*

### 5. Policy generation and policy review

AI can help draft, review and cross-check policies, procedures and templates, including malpractice, appeals, reasonable adjustments, special consideration, centre approval, centre monitoring, conflicts of interest, assessment design, CASS, qualification review, data protection and risk management documents.

It can help identify duplication, inconsistency, missing procedural steps, unclear responsibilities and weak audit trails.

However, policy content must be checked against the organisation's actual operating model and regulatory obligations. A well-written policy is not necessarily a compliant or operationally effective policy.

Organisations should also avoid uploading whole policy suites, board papers, confidential regulatory submissions or client-specific documents into public AI tools without approval and safeguards.

### Example prompt

*As a governance specialist for a UK awarding organisation - draft a concise section for a Conflicts of Interest Policy covering definition, annual declarations, recording, escalation to the Responsible Officer, and record-keeping. Use neutral, procedural language.*

## 6. Governance frameworks

AI can support the development and review of governance frameworks, committee terms of reference, board reporting templates, risk registers, decision logs, annual self-assessment templates, audit schedules, escalation routes and accountability maps.

It can help organisations consider whether responsibilities, reporting lines, decision-making authority and evidence trails are clear.

However, governance content must still be approved by accountable leaders and must reflect how the organisation actually operates. AI should not create a governance framework that looks strong on paper but is disconnected from real practice, capacity or accountability.

## 7. Regulatory mapping and evidence checks

AI can help map policies, procedures, qualification documents and quality assurance records against regulatory conditions, recognition criteria, apprenticeship requirements or internal quality standards. It can assist in identifying where evidence is strong, weak, duplicated or missing.

This is particularly helpful when preparing for recognition, audit, external review, regulatory monitoring or internal governance review.

However, regulatory mapping must be checked by someone who understands the relevant framework. AI may misinterpret conditions, overstate compliance, invent requirements or miss the significance of operational evidence.

## 8. Centre approval and centre monitoring

AI can support the creation of centre approval forms, centre risk profiles, monitoring checklists, action plans, report templates and centre guidance. It can help identify themes across centre reports or recurring risks.

However, centre judgements must remain evidence-based and human-led. Centre reports and risk records often contain sensitive or commercially sensitive information and should not be uploaded to public AI tools without approval, anonymisation and appropriate safeguards.

### Example prompt

*Create a risk-based centre monitoring checklist for vocational qualifications at Levels 2–3 covering assessment planning, IQA, record-keeping, staff competence, learner support and malpractice prevention. Include a simple Low/Medium/High risk rating and space for notes.*

## 9. CASS and quality assurance activity

AI can support CASS planning, sampling rationale, moderation themes, EQA report analysis, assessor feedback review, action tracking and quality assurance trend analysis. It can help identify patterns that may require further investigation.

For example, AI could help quality teams look for inconsistent assessor feedback, overly generic feedback, missing evidence references, repeated wording across learner submissions, gaps in sampling rationale or recurring centre action points.

However, AI should not make quality assurance decisions. It should help focus human review, not replace it.

## 10. Staff training, induction and workforce documentation

AI can support the development of staff training slides, training agendas, induction plans, job descriptions, person specifications, role profiles, assessor handbooks, IQA and EQA handbooks, centre handbooks, learner guidance and standardisation materials.

This can be particularly helpful where organisations are developing a new function, onboarding new staff or associates, preparing for external review, refreshing governance arrangements or trying to create a more consistent operating model.

For example, AI can help turn a policy into a training session, a procedure into an induction plan, a role description into a person specification, or a quality assurance process into a practical checklist. It can also help ensure that terminology is used consistently across documents, that responsibilities are clear, and that documents are written in a style appropriate for the audience.

However, these materials still require expert review. A job description may look professional but fail to reflect the actual accountabilities of the role. An assessor handbook may be well written but not accurately reflect the assessment model. A training slide deck may be engaging but

omit key regulatory or operational controls. An induction plan may be structured but not sufficient to evidence competence, standardisation or readiness to practise.

AI is most effective when it is given good-quality source information and clear direction. The user needs to explain the purpose of the document, the intended audience, the organisation's operating model, the regulatory context, the required tone and any specific processes that must be reflected. Without that context, AI is likely to produce generic content.

## 11. Standardisation and training

AI can help create training materials, assessor standardisation exercises, sample responses, borderline judgement activities, scenarios, webinar scripts and guidance notes.

This can improve consistency across staff and associates. It can also help new assessors understand the difference between evidence that is merely descriptive and evidence that demonstrates secure competence, application, evaluation or professional judgement.

However, standardisation materials should not be created from real learner work unless consent, anonymisation and data protection requirements have been addressed. Even anonymised learner work should be handled carefully, particularly where the evidence includes workplace examples, personal reflections or employer information.

AI-generated examples should be checked carefully before use, particularly where they relate to occupational competence, safeguarding, clinical judgement, legal compliance or regulated practice.

## 12. Malpractice and authenticity controls

AI has created new challenges around authenticity. Learners may use AI tools to produce written work, reflective accounts, portfolio narratives, presentations or research tasks. In some cases, AI use may be permitted for learning support. In others, it may undermine the validity of the assessment.

Awarding organisations and assessment organisations can use AI to help review and strengthen malpractice controls. This may include drafting clearer learner guidance, centre guidance, declaration wording, assessor prompts and investigation checklists.

AI can also help organisations think through risk scenarios, such as use of AI in coursework or portfolio evidence, AI-generated reflective accounts, over-polished written submissions inconsistent with observed performance, use of AI during remote assessment, inappropriate use of translation or paraphrasing tools, centre staff over-supporting learners through AI-generated templates, and difficulty distinguishing legitimate support from malpractice.

However, organisations should be careful about relying on AI detection tools as definitive evidence. Detection tools can be unreliable and may produce false positives or false negatives.

A stronger approach is usually based on assessment design, authentication, professional questioning, version history, declarations, assessor judgement and a clear investigation process.

Ethical practice also means being transparent with learners and centres. Learners should know what is allowed, what is not allowed, what must be declared, and what may happen if AI is used inappropriately.

### 13. Data analysis and risk monitoring

AI can help organisations make better use of assessment and quality assurance data. This might include identifying patterns in achievement rates, facility values, centre performance, assessor decisions, appeals, complaints, malpractice cases, late submissions or EQA findings.

For example, AI-supported analysis could help identify centres with unusual achievement profiles, assessment forms with unexpected pass rates, items with poor facility or discrimination, assessors whose decisions are frequently adjusted, qualifications with recurring centre support issues, increases in malpractice or authenticity concerns, gaps in portfolio review activity, and risks associated with ageing qualifications.

This can support a more proactive approach to governance. Instead of waiting for problems to escalate, organisations can use data to identify early warning signs and target their quality assurance activity more effectively.

However, data analysis must be handled ethically and securely. Learner data, centre performance data and commercially sensitive information should only be processed through approved systems. Outputs should be interpreted carefully and should not be used to make unfair assumptions about centres, assessors or learners without further investigation.

The key requirement is that AI-supported analysis must be explainable and subject to human interpretation. Data patterns are prompts for investigation, not automatic conclusions.

### 14. Operational documentation and communications

AI can also support everyday operational activity. It can help draft agendas, minutes, action logs, report summaries, audit checklists, learner communications, centre letters, internal briefings, FAQs, website content and report summaries.

For busy awarding and assessment teams, this can save time and improve consistency.

Organisations should remain alert to confidentiality, data protection and information security. Sensitive learner data, assessment materials, live items, centre performance data or commercially confidential information should not be entered into public AI tools unless there is a clear, approved and secure arrangement in place.

Operational AI use should therefore be covered by internal rules, staff training and data governance.

There should also be a clear expectation that AI-generated content is reviewed before use. A letter, report, checklist, meeting summary or website article may look professional, but it still needs to be checked for accuracy, tone, completeness and organisational context.

## AI memory, organisational learning and consistency

Where AI is used regularly within an organisation, it can develop understanding of your business needs and become more useful over time. It can learn from approved templates, preferred terminology, house style, previous examples and clear instructions.

In that sense, it can help build consistency across documentation and communications.

For example, an approved AI workspace, prompt library or controlled internal tool may help an organisation maintain a consistent approach to policy structure, report writing, board papers, centre communications, training slides, assessor guidance, qualification review reports, risk summaries, governance papers and standardisation materials.

Organisations must be careful about how this is managed. AI should not be allowed to develop uncontrolled organisational memory from confidential, secure, personal, commercially sensitive or copyrighted information.

If a tool stores previous prompts, uploaded documents, templates or organisational preferences, this must be governed. The organisation should know what is being stored, who can access it, how long it is retained, whether it can be used to train the model, and how information can be deleted.

Safer alternatives include approved internal or enterprise tools that offer appropriate data residency, encryption, and no-training guarantees.

AI memory can support consistency, but it can also embed outdated information, reproduce errors, retain confidential context or apply old assumptions to new situations.

Any use of AI memory, custom instructions, shared workspaces or reusable prompt libraries should therefore be approved, maintained and periodically reviewed.

## Governance and responsible use

The most important point is that AI use must be governed. Awarding organisations and assessment organisations should not allow uncontrolled experimentation across teams without clear parameters.

A responsible AI framework should address:

- Where AI may and may not be used
- Who can approve AI-assisted processes
- What data can be entered into AI tools
- How confidential and secure material is protected
- How GDPR requirements are met
- How embedded content and metadata are checked
- How intellectual property and branding are safeguarded
- How AI outputs are checked
- How human oversight is retained
- How conflicts, bias and errors are managed
- How AI use is documented
- How AI memory or reusable prompt libraries are controlled
- How risks are reviewed by governance groups
- How staff and associates are trained
- How learners and centres are informed where relevant

AI should be included in risk registers, policy review cycles, malpractice monitoring, assessment design review, qualification review and governance reporting.

Organisations should also consider whether AI use needs to be included in staff handbooks, associate agreements, centre agreements, confidentiality clauses, privacy notices, data protection procedures and information security policies.

*Used well, AI can support better processes.*

*Used poorly, it can create hidden risks, undermine confidence and weaken the defensibility of assessment decisions.*

The following checklist deliberately consolidates the key safeguards set out above into practical principles that can be used for policy, training and governance purposes.

## Practical principles for ethical AI use

- Develop a Use of Generative AI Policy
- Use the minimum necessary information
- Do not upload secure, live or confidential assessment material into public AI tools
- Do not upload business plans, board papers, tenders, commercial proposals, contracts or financial information into public AI tools without approval
- Remove branding, names, centre details, learner details and commercially sensitive information where possible
- Check for embedded content, metadata, comments, tracked changes, hidden tabs and file properties before using documents with AI
- Check copyright and intellectual property ownership before using source material
- Use clean extracts rather than whole documents wherever possible
- Use anonymised scenarios, placeholders and frameworks instead of identifiable information
- Use AI to support, not replace, professional judgement
- Ensure competent subject experts review the input and output
- Keep a record of how AI has been used where it supports regulated activity
- Do not rely on AI outputs without control methods
- Do not use AI-generated content directly in assessment materials without review, mapping and sign-off
- Ensure AI use aligns with GDPR, confidentiality, data protection, information security and assessment security requirements
- Monitor AI memory, prompt libraries and reusable organisational context
- Review AI-assisted materials regularly to ensure they remain accurate and current.

These principles are not intended to prevent innovation.  
They are intended to make innovation safer, more transparent and more defensible.

## Summary of unacceptable use

- Uploading of secure, live or confidential assessment materials into public AI tools. This includes live papers, item banks, answer keys, mark schemes, examiner materials, unseen scenarios, controlled assessment tasks or any content that could compromise assessment security
- Uploading of entire qualification specifications, branded documents, unpublished materials, commercially sensitive documents or third-party intellectual property without permission and appropriate controls
- Uploading of learner work, learner data, centre reports, employer information, complaints, malpractice evidence, EQA reports or quality assurance records into AI tools unless the platform is approved, the data is protected, and there is a lawful and proportionate reason for doing so
- Uploading of business plans, board papers, financial forecasts, pricing models, tenders, contracts, client lists, pipeline information, staffing models, commercial strategies or internal governance papers into public AI tools simply to achieve a quicker output
- Sharing of identifiable, confidential or commercially sensitive business information with AI simply because it helps achieve the task more quickly
- Sharing of confidential business information with AI tools unless the organisation has approved the tool, checked the data implications, considered contractual duties and confirmed that the information can be shared lawfully and safely
- Uploading of documents without checking for embedded content, metadata, comments, tracked changes, hidden tabs, previous edits, author names or file properties that may disclose confidential, personal or commercially sensitive information
- Inserting of AI-generated content directly into assessment materials without expert review, mapping, technical checking, version control and formal approval
- Relying on someone without the right subject, assessment or regulatory expertise to rely on AI outputs without knowing whether they are accurate, level-appropriate, fair, valid or fit for purpose
- Allowing AI to make assessment, moderation, malpractice, appeal, reasonable adjustment, centre approval, quality assurance or awarding decisions without accountable human judgement
- Using AI in a way that is hidden, uncontrolled or undocumented where it affects regulated activity, assessment design, quality assurance, governance, business decisions or learner outcomes
- Assuming that AI detection tools provide definitive evidence of malpractice. Any concern about AI misuse should be considered through a fair, evidence-based investigation process
- Allowing AI-generated staff training, induction materials, role descriptions, assessor handbooks or operational guidance to be used without checking that they accurately reflect the organisation's actual structure, responsibilities, assessment model, regulatory obligations and approved procedures
- Allowing AI to develop an uncontrolled organisational memory using confidential, secure, personal, commercially sensitive or copyrighted information
- Using AI as a shortcut for weak assessment design, poor quality assurance, insufficient standardisation, poor data governance, weak information security or inadequate governance

## Example content for a Generative AI Policy (staff facing)

The following headings and brief descriptions can be used as a starting point for an organisation-specific policy. Adapt the detail to reflect your approved tools, risk appetite and regulatory context. Each section will need full contextual population of organisational content.

### **Purpose and scope**

Sets out the principles and responsibilities for the use of generative AI in activities supporting regulated qualifications and assessments.

### **Approved tools**

Only tools and platforms formally approved by the organisation may be used. A register of approved tools and permitted use cases is maintained and detailed here as appropriate.

### **Prohibited uses**

Lists activities that are not permitted without specific written authorisation (e.g. uploading live assessment materials, making final awarding decisions).

### **Data handling and confidentiality**

Explains to staff about applying minimisation and anonymisation principles. How sensitive information may only be processed on approved enterprise platforms with appropriate safeguards.

### **Human review and accountability**

Details how AI-generated content used in regulated activity must be reviewed by a competent expert as part of lifecycle development. The reviewer remains fully accountable for the final output. Process and procedure flow.

### **Training**

Staff and associates must complete the organisation's responsible AI use training before using tools in regulated work. Insert details of training, updating and escalation requirements.

### **Governance and review**

Explains how AI use is monitored through existing risk management processes. The policy is reviewed at least annually.

### **Regulatory references**

Reference relevant Ofqual conditions, JCQ guidance, data protection requirements and the organisation's own malpractice and quality assurance policies.

### **Version control and owner**

Detail version, storage and accountable sign off.

# AI Governance Self-Audit Checklist for Organisations

Use this checklist to assess your organisation's current maturity.  
Rate each item: Yes / Partial / No.

## Policy & governance

- We have a documented Use of Generative AI Policy approved at senior level
- AI use is included in the organisational risk register and reviewed periodically
- Clear approval routes exist for new AI tools and use cases
- Roles and responsibilities for AI oversight are clearly assigned

## Data protection, confidentiality & security

- We distinguish between public/consumer AI tools and approved enterprise platforms with contractual safeguards
- Staff know how to minimise, anonymise and redact information before using AI tools
- We check for embedded metadata, tracked changes and hidden content before uploading documents
- Where sensitive information must be used, we only use approved platforms with no-training clauses and appropriate data residency

## Human oversight & competence

- All AI outputs used in regulated activity are reviewed by competent subject or assessment experts before final use
- We have clear guidance on when AI may and may not be used in assessment design, marking, quality assurance and decision-making
- Staff and associates receive training on responsible AI use, limitations of AI, and organisational policy
- We maintain records of AI use where it supports regulated activity

## Risk management & continuous improvement

- We monitor AI-related risks (malpractice, bias, over-reliance, IP leakage, regulatory non-compliance)
- We have processes to investigate and respond to incidents involving inappropriate AI use
- We periodically review AI-assisted materials and processes to ensure they remain accurate and current
- We stay informed of regulatory developments (Ofqual, JCQ, EU AI Act, ICO) and update our approach accordingly

Ultimately – AI should never be used in a way that weakens validity, fairness, confidentiality, GDPR compliance, assessment security, intellectual property protection, organisational accountability or public confidence.

If your organisation is unable to explain, justify and evidence how AI was used, what information was shared, what controls were in place, who reviewed the output, and why the final decision remained valid, secure and fair, then the use of AI is not sufficiently controlled.

The boundary is clear.

AI should:

- Support good professional judgement, not replace it
- Strengthen assessment practice, not weaken it
- Protect public confidence, not put it at risk.

## Emerging considerations

Organisations should also consider the implications of more advanced AI capabilities.

Multimodal models that can analyse images of handwritten scripts, portfolios or practical evidence raise new questions about data protection, consent and authenticity.

AI agents with persistent memory across sessions can improve consistency but increase the risk of embedding outdated or sensitive organisational context.

Predictive analytics for centre or learner risk monitoring can support proactive quality assurance but must be used transparently, with clear human oversight and safeguards against bias or unfair profiling.

Any such uses should be subject to the same rigorous governance and human accountability requirements as other AI applications.

## Further reading and resources

- Ofqual – Approach to regulating AI in the qualifications sector and principles for AI use in marking: <https://www.gov.uk/government/publications/ofquals-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector>
- JCQ – AI Use in Assessments guidance (updated): [https://www.jcq.org.uk/wp-content/uploads/sites/2/2025/09/AI-Use-in-Assessments\\_Apr25\\_FINAL.pdf](https://www.jcq.org.uk/wp-content/uploads/sites/2/2025/09/AI-Use-in-Assessments_Apr25_FINAL.pdf)
- ICO – Guidance on AI and data protection: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/>
- EU AI Act – High-Risk AI Systems (Annex III – Education): <https://artificialintelligenceact.eu/>

## Conclusion

AI has the potential to support awarding organisations and assessment organisations in many valuable ways. It can assist with qualification development, assessment design, item development, assessment banks, standardisation, quality assurance, policy review, governance frameworks, regulatory mapping, centre support, workforce documentation, training materials, risk monitoring and operational efficiency.

But AI should not be treated as a shortcut around professional judgement. It should not replace subject specialists, assessors, moderators, EQAs, governance boards or responsible officers. Nor should it be used in ways that make assessment decisions less transparent, less explainable or less fair.

The strongest organisations will be those that neither ignore AI nor adopt it uncritically.

They will be the organisations that build clear governance, use AI to strengthen assessment practice, retain human accountability and ensure that validity, fairness and public confidence remain at the centre of every decision.

AI can be a useful tool in awarding and assessment organisations. But it must be used with control, competence and care.

What matters?

- Quality inputs
- Expert prompts
- Human review
- Ethical controls
- GDPR considerations
- Confidentiality controls
- Intellectual property protection
- Business information protection

Without those safeguards, AI may simply help organisations produce poor-quality work more quickly while creating hidden risks. With those safeguards, it can help organisations improve the quality, consistency and defensibility of their assessment and awarding practice.

## About Taylor Educational Consulting

Sam Taylor is founder of Taylor Educational Consulting, a specialist in qualification and assessment design, regulation, compliance and training, with over 30 years of senior leadership experience in the education and skills sector.

As a Fellow of the Chartered Institute of Educational Assessors (FCIEA) and a Member of the Society of Authors, Sam's professional standing reflects both assessment expertise and a commitment to the publishing, training and awarding sectors.

If you want a chat to discuss any potential projects or training you think you may need help with - even if you aren't certain what you need or whether we can help, just tell us a little more by message or email and we will get back to you as soon as possible to set up a no-obligation chat over Zoom or Teams.

For details and to arrange a chat, contact us at:

Web: <https://qualificationdevelopment.co.uk>

Email: [hello@qualificationdevelopment.co.uk](mailto:hello@qualificationdevelopment.co.uk)

LinkedIn: <http://linkedin.com/in/sam-taylor-75178b2b>