FUTURE CONNECT
TRAINING INSTITUTE

Produced by Abhishek Sharma, Head of IT and Marketing

Approved by Palwi Sood , Managing Director

Version date: 25/05/25 Version Number: FCT/AIP/25

Review schedule: 25/05/26 or in line with operating procedure requirements

Person/s responsible: SLT, all management and delivery staff

DPO : Umar Tariq

Signed Abhishek Sharma

Signed Palwi Sood

Policy owner: Abhishek Sharma

Future Connect Training & Recruitment AI Policy

1) Purpose & Scope

This policy sets out how FC Training (Future Connect Training & Recruitment Ltd) will procure, use, govern and monitor Artificial Intelligence (AI) across teaching, learning, assessment, recruitment, marketing and operations. It covers both **generative AI** (e.g., large language models, image/audio generators) and **non-generative AI** (e.g., predictive analytics, proctoring, recommendation systems).

The policy applies to:

- All programmes including **NCFE**, **AAT**, Functional Skills and short courses (online and on-campus).
- All AI use on FC Training devices, networks, platforms, and third-party systems used for FC Training purposes—even when accessed on personal devices.

Where awarding-body regulations (e.g., NCFE/AAT) or statutory requirements are stricter, **the stricter rule prevails**.

---

2) Principles

1. **Learner success & integrity:** AI should enhance learning and employability without undermining assessment integrity or qualification standards.
2. **Transparency:** Significant use of AI in content, assessment or decision-making must be explained to affected individuals in clear language.
3. **Human oversight:** AI outputs that affect people (grades, progression, hiring decisions, disciplinary outcomes, safeguarding signals) require accountable human review.
4. **Privacy & security by design:** Personal data is processed lawfully, fairly and securely with appropriate controls and retention limits.
5. **Accessibility & inclusion:** AI use should support equitable access and reasonable adjustments without creating new barriers or bias.
6. **Safety first:** AI must not expose learners or staff to harmful, discriminatory or illegal content or unsafe practices.

---

3) Roles & Responsibilities

- **Head of Centre / Managing Director:** Accountable for compliance and resources; approves this policy.
- **Policy Owner (Head of IT and Marketing):** Maintains the policy and guidance, conducts audits, and escalates risks.
- **Centre Manager / Exams Officer:** Applies awarding-body and exam rules in assessments and examinations.

- **IT & Security:** Approves tools, sets technical controls (e.g., MFA, allow/deny lists), and investigates incidents.
- **All Staff, Contractors & Learners:** Use AI responsibly, follow assessment rules, disclose permitted use, and report incidents.

4) Definitions (Plain English)

- **AI system:** Software that performs tasks requiring human-like intelligence (recognition, prediction, generation).
- **Generative AI:** Tools that create text, code, images, audio or video from prompts.
- **Automated decision-making:** A decision made by a system without meaningful human involvement.
- **High-risk use:** AI use that can materially impact learning outcomes, grades, access to services, employment or safety.

5) Governance & Approval

1. **AI Register:** IT maintains an up-to-date register of approved AI tools and models, with version numbers, data flows, licences and risk ratings.
2. **Change control:** New tools or significant updates require: (a) owner, (b) purpose, (c) data categories, (d) legal basis, (e) security review, and (f) **DPIA** if personal data or high-risk.
3. **Vendor management:** Third-party tools must meet FC Training's security, GDPR and accessibility requirements; contracts must include data processing and sub-processor transparency.

6) Acceptable Use: Summary Matrix

Role / Context	Allowed	Allowed with Conditions	Not Allowed
Learners – Study Support	Brainstorming ideas; explaining concepts; creating revision plans	Drafting outlines or example answers **only if** referenced/declared; accessibility aids (speech-to-text; translation)	Submitting AI-generated work as own; using AI that stores/exports assessment content without permission
Learners – Assessments (Coursework)	Using assistive tools for spelling/grammar	Generative support if explicitly permitted in the brief **and** fully disclosed; citations checked	Where the brief forbids AI; automated code/content generation that is uncredited or exceeds permission

Learners – Exams/Controlled Assessments	N/A	Use of approved accessibility tech only (with reasonable adjustments)	**Any** generative AI or internet-connected AI unless the awarding body permits
Tutors/Assessors	Creating teaching resources; personalised feedback exemplars	Using AI to draft feedback where the assessor verifies and personalises	Auto-marking summative tasks without human review; feeding unredacted learner personal data into public tools
IQA/Quality	Drafting checklists/rubrics	Using AI to suggest sampling comments (human-checked)	Relying on AI detectors as sole evidence of malpractice
Recruitment & Careers	CV review templates; vacancy summaries	Screening assistance with bias-mitigation and human review	Fully automated hiring decisions
Marketing & Comms	Drafting copy/images (rights-cleared)	Publish only after human fact-check; label AI-assisted imagery where material	Deepfakes; misrepresentation or undisclosed synthetic personas
Admin & Operations	Drafting emails, meeting notes, checklists, process maps; summarising non-sensitive documents	Data extraction from internal docs where tools are **approved**; human review before circulation; no auto-sending without approval	Entering confidential/personal data into public tools; using AI for binding decisions or policy changes without human sign-off
Admissions & Student Support	FAQs, appointment reminders/templates; triage scripts; signposting	Use chatbots for **general** info only with clear hand-off to humans; anonymise examples; follow consent/record-keeping rules	Storing or processing applicant data in public AI; automated admissions decisions; immigration/visa advice beyond approved guidance
Finance & Accounts	Drafting comms on fees; summarising policies; creating non-live models with dummy data	Handling live financial data only in **approved, compliant** tools; human approval for invoices/credit-control templates	Uploading bank/PCI data to public AI; autonomous payment decisions or changes to ledgers
HR (People Team)	Drafting job descriptions, interview questions, policy drafts	Screening assistance with bias-mitigation and **human** review; avoid protected characteristics; keep decision rationale	Fully automated hiring, disciplinary or performance decisions; processing special category data in public tools
Exams & Centre	Creating	Templates must **not**	Uploading exam

Admin	schedules/checklists; generic candidate communications	include live assessment content; devices used in exams must block AI/internet where prohibited; follow invigilation/device rules	papers or confidential materials to any AI; using AI during controlled assessments; tools that circumvent exam rules

7) Assessment Integrity (NCFE/AAT & Other Awarding Bodies)

1. **Brief-level rules:** Every assessment brief must state one of: **(A) AI Prohibited**, **(B) AI Limited Use** (state exactly what is allowed), or **(C) AI Permitted with Disclosure**.
2. **Learner declaration:** Where AI is permitted, learners must submit an **AI Use Statement** (template in Appendix B) detailing tools, prompts and how outputs were used.
3. **Evidence requirement:** Learners should retain drafts, prompt history and notes. Assessors may request these to verify authenticity.
4. **Detection:** AI-content detectors are **not reliable** as sole evidence. Suspected malpractice must be investigated using holistic evidence (drafts, interviews, version history, plagiarism checks, similarity analysis, metadata, and professional judgement).
5. **Exams/controlled conditions:** Generative AI is **not allowed** unless the awarding body states otherwise. Follow invigilation and device rules.
6. **Credit & citation:** If AI contributes ideas or text, cite the tool (name, version/date, prompt summary). Learners remain responsible for accuracy and originality.

8) Teaching & Learning

- Tutors may use AI to create lesson plans, examples, question banks and differentiated resources; all materials must be reviewed for accuracy, bias and appropriateness.
- Where AI creates images/audio/video, staff must ensure **IP rights** are respected and content is age-appropriate.
- Provide learners with guidance on effective, ethical AI use relevant to their programme (e.g., accountancy, data analysis, cyber security).

9) Data Protection & Privacy (GDPR)

1. **Lawful basis:** Identify and document the legal basis before processing personal data in AI tools (e.g., contract, legitimate interests, consent for optional services).
2. **Data minimisation:** Share the minimum required. **Do not paste** special category data (health, ethnicity, etc.) into public AI tools.
3. **Confidentiality:** Do not input exam content, unpublished assessments, or commercially sensitive data into public tools.

4. **DPIA required** for high-risk uses (profiling, monitoring, automated decisions, processing minors’ data, or large-scale personal data).
5. **International transfers:** Check where data is stored/processed and ensure appropriate safeguards.
6. **Retention:** AI training logs, prompts and outputs that include personal data must have defined retention and secure deletion.
7. **Rights:** Provide clear routes for access/erasure/objection requests. Automated decisions that have legal or similarly significant effects require the option for human review.

---

10) Security & Safety Controls

- Use only approved accounts and MFA where available.
- IT maintains allow/deny lists and URL filtering for high-risk tools.
- Content moderation must block abusive, discriminatory or harmful prompts/outputs in learning spaces.
- Never use AI to generate or advise on dangerous, illegal or unethical activities.

---

11) Accessibility, Inclusion & Safeguarding

- AI tools used for accessibility (e.g., text-to-speech, captioning, translation) are encouraged where compliant and effective.
- Staff must be alert to safeguarding concerns arising from AI-mediated interactions (e.g., harassment in chat spaces, deepfake abuse) and follow reporting procedures.
- Ensure AI does not disadvantage learners with limited digital access or those who opt out for privacy reasons—offer non-AI alternatives.

---

12) Procurement & Vendor Standards

Vendors must:

- Provide clear documentation of data collection, model behaviour, security controls and sub-processors.
- Offer admin controls for data retention, export and deletion.
- Support UK GDPR compliance, accessibility standards, and appropriate age-assurance where relevant.
- Disclose model updates that could affect results (model/version transparency).

---

13) Monitoring, Audit & Quality Assurance

- **Termly audits** of AI use in modules and assessments.
- Sampling of feedback generated with AI to ensure quality and personalisation.
- Review of prompt/output logs (where systems provide them) for compliance.
- Annual report to the Board covering incidents, benefits, risks and improvements.

14) Incident Management

Report AI-related incidents (privacy breach, harmful content, suspected malpractice, security issue) immediately to the Policy Owner via the usual incident form. The DPO will be engaged for data breaches. Lessons learned will inform updates to this policy and training.

15) Training & Awareness

- **Mandatory annual training** for all staff on ethical and compliant AI use.
- Induction briefings for learners on permitted use, disclosure, and academic integrity.
- Just-in-time guidance embedded in VLE/assessment briefs.

16) Non-Compliance & Sanctions

- Staff: managed under HR disciplinary procedures and, where relevant, contractual remedies.
- Learners: handled under Academic Misconduct procedures and awarding-body rules; penalties range from resubmission to disqualification depending on severity.

17) Review Cycle

This policy will be reviewed at least **annually** or sooner if there are significant legal, regulatory or awarding-body changes, or material incidents.

Appendix A – Quick Rules by Assessment Type

- **AI Prohibited:** Exams, controlled assessments, professional discussions under exam conditions.
- **AI Limited Use:** Coursework where specific tasks allow AI (e.g., idea generation, structure, code linting) with disclosure.
- **AI Permitted with Disclosure:** Reflective journals, research scoping, early drafts—must cite AI tool and verify facts.

Disclosure format: Tool name & version/date; prompts used (high-level); which parts of work were influenced; what checks you performed (citations, calculations, originality).

Appendix B – Learner AI Use Statement (Template)

I used [Tool name & version] on [date] to [purpose]. I entered prompts such as: [short description]. I edited and verified the output by [methods]. I confirm this submission is my own work and complies with the assessment brief and FC Training's AI Policy.

Signature: ____ Date: ____

Appendix C – Assignment Wording (Insert into Briefs)

- **AI Status:** [Prohibited / Limited Use / Permitted with Disclosure].
- **If Limited/Permitted:** You may use [specific tools/uses]. You **must** submit an AI Use Statement (Appendix B) and retain drafts/prompts. Failure to disclose may be treated as malpractice.

Appendix D – DPIA Trigger Checklist (Yes/No)

- Processes personal or special category data?
- Monitors behaviour or location?
- Uses profiling or automated decision-making with significant effects?
- Involves minors or vulnerable adults?
- Large-scale data, new tech, or international transfers?
- Supports or interacts with **JCQ-regulated assessments** in any way (teaching, authentication, marking, devices)?
- If any **Yes** → complete a DPIA before go-live and notify the HoC/Exams Officer where JCQ applies.

Appendix E – Prompt & Content Handling

- Avoid entering personal, confidential or assessment-sensitive data into public tools.
- Use neutral, non-biased prompts; test with diverse examples.
- Fact-check and reference authoritative sources; do not invent citations.
- Keep local copies of important prompts/outputs when needed for audit.

Appendix F – Glossary

- **DPIA:** Data Protection Impact Assessment.
- **GDPR:** UK General Data Protection Regulation.
- **IQA:** Internal Quality Assurance.
- **LLM:** Large Language Model.
- **VLE:** Virtual Learning Environment.