



AI human avatars: opportunities and risks for UK businesses and services

Written by Dr Mathilde Pavis and Dr Dominic Lees
University of Reading, [Synthetic Media Research Network](#) and [Replique](#)



Executive summary

The problem

- UK businesses are rapidly adopting AI cloning tools to create digital avatars of workers, consumers or public figures for efficiency, accessibility, and engagement.
- But digital cloning raises legal, economic and safety risks from privacy violation, and misinformation to the exploitation of workers.
- Current UK law provides no unified protection individuals' likeness, ownership or misuse of AI avatars.
- Organisations lack guidance on procurement, compliance, and risk management, leaving them exposed to legal uncertainty and public mistrust.

Our solution: Four priority actions for government and industry

1. **Likeness protection** – Introduce a UK-wide statutory right over image and voice with accessible remedies. DSIT should lead this reform with IPO and ICO.
2. **Fair contracts** – Ban exploitative clauses transferring likeness or data rights without free informed consent or fair compensation. Alongside statutory limits, DSIT and DBT to publish best-practice guidance and support sectoral bargaining.
3. **Safe adoption guidance** – Develop procurement standards and risk management resources for AI avatar tools, with joint IP and data protection guidance, coordinated by DSIT.
4. **Sustainability** – Commission research into the environmental impact of AI avatars to inform future environmental standards.

These reforms will safeguard individuals while enabling UK businesses and public services to deploy AI avatars responsibly and competitively, advancing goals in the [AI Opportunities Action Plan](#) and [2025 Industrial Strategy](#).

Research funded by the University of Reading's Policy Fund and [Replique](#).

Introduction

Recent advances in Generative AI have made it possible to create life-like *human avatars* that replicate a person's voice, face and gestures with striking accuracy, through a process known as *digital cloning*.

Once experimental, these technologies are now commercially available and have been increasingly used by UK businesses and public services since 2022.

AI human avatars are increasingly used to enhance communication, training and customer interaction, driven by gains in efficiency, inclusivity and emotional resonance.

Yet this rapid uptake raises complex legal, ethical and economic risks, from consent and misinformation to cybersecurity or labour displacement.

As a high-reward, high-risk application of AI, the use of human avatars and digital cloning demands urgent and coordinated policy attention. This briefing maps emerging trends in AI human avatar use by UK businesses and services, describing key reported benefits and risks of the technology to support effective policy intervention.

This briefing makes 4 policy recommendations to support the government's objective for economic growth and leadership in AI, set out by the [AI Opportunities Action Plan](#) and [The UK's Modern Industrial Strategy 2025](#).

The briefing covers:

- a description of AI human avatars and the digital cloning process
- key benefits and risks in deploying AI human avatars across the UK economy
- examples of avatar use across UK sectors
- policy recommendations for the UK government to support the safe and effective use of digital cloning tools across economic sectors
- a glossary of terms



What is an AI human avatar?

An *AI human avatar* (or ‘avatar’) is a digital representation of a person reproducing their appearance, voice and mannerisms in audio or video form without requiring their direct physical participation.

The underlying process, known as *digital cloning*, involves recording and recreating an individual's likeness so that their avatar is visibly or audibly recognisable to others. An overview of the digital cloning process is provided on page 9 of this report.

There is no single definition or settled terminology for AI human avatars. In different contexts, human avatars are also called: *deepfakes*, *digital twins*, *digital clones*, *voice clones*, *digital doubles*, *digital replicas* or *synthetic performances*. In this briefing, we primarily use the phrase ‘AI human avatar’ or avatar.

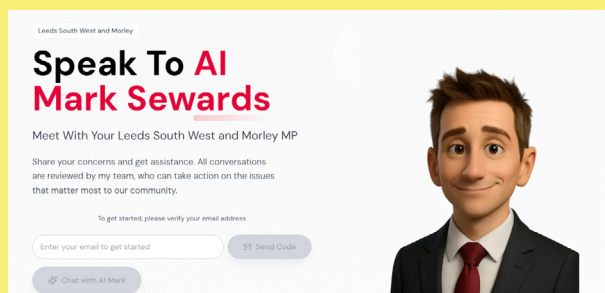
AI human avatars are typically deployed in two forms:

Pre-recorded content: scripted videos, sound recordings or presentations where the avatar delivers prepared material. For example, the BBC Maestro course where a [video avatar of Agatha Christie](#) teaches crime writing.



© BBC Maestro

Real-time interaction: avatars integrated into services such as chatbots, voice assistants or virtual presenters that engage dynamically with users. Westminster MP Mark Sewards has integrated a [voice avatar of himself into a chatbot](#) to answer simple policy questions.



© Neural Voice

Avatars can be used by organisations both internally and externally. Internally, they assist with staff training, knowledge-sharing and corporate communications. For example, Zoom's CEO Eric Yuan used [his avatar to present an earnings report](#). Externally, avatars provide customer service, translation and live announcements, as in the case of software company Jet BI which relies on [employee avatars to guide clients](#) through its services.

AI human avatars are not autonomous systems. They function as digital overlays on existing AI tools, such as chatbots or content generators; they cannot replicate human reasoning, critical assessment or self-reflection. Even when paired with advanced AI systems, their outputs require human oversight to ensure accuracy and relevance.

Opportunities of AI human avatars for businesses and public services

Deployed safely, AI human avatars can **enhance communication** by delivering clear, consistent and accessible information, and **strengthen engagement** by making interactions more relatable, emotionally compelling and impactful.

Organisations adopting AI avatars also report wider benefits, including the following:

- **Efficiency** and cost savings in producing high-quality content at scale, without the time and resource demands of traditional recording methods.
- **Consistency** in delivering technical or important information with accuracy and reliability.
- **Continuity** of communication and service when individuals are unavailable, or during major disruptions.
- **Accessibility and personalisation**, by providing content in multiple formats or languages to reach diverse audiences.

These advantages are demonstrated most clearly in two domains:

1. Creative and media industries, where avatars are used to extend performances into new contexts. For example, video games routinely integrate cloned likenesses of actors, and film and television productions use digital avatars for dubbing content across languages.

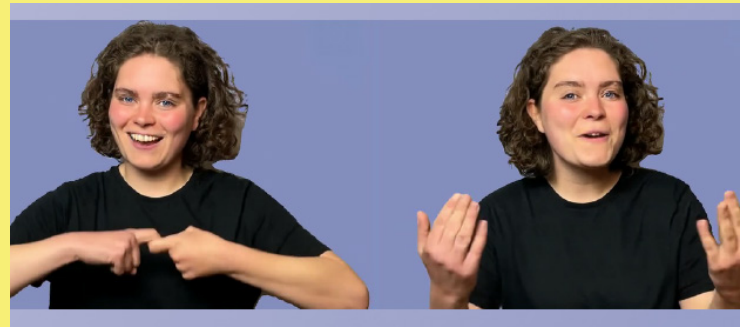
Examples

- UK production companies such as Musion and The Format Factory have used AI cloning to create life-size and video avatars of late public figures, including [Frank Sinatra](#) and [Gerry Anderson](#). DeepFusion Films created a [voice avatar of the late TV host Michael Parkinson](#) to conduct interviews with today's celebrities in the show *Virtually Parkinson*.
- The stage show *ABBA Voyage* toured the UK with full-body [holographic avatars](#) of the band, portraying the performers as they looked at the height of their career.
- Music artist Twigs collaborated with Cyberclone to create an [AI avatar](#) that appears in video promotion, demonstrating how the technology can help professionals refocus their time on core or higher-value work.
- H&M created [digital twins of 30 models](#) for use in their marketing campaigns, with models retaining ownership of their avatars.
- Food brand Lay's partnered with football player Lionel Messi to send personalised video messages featuring [his AI avatar](#).

2. Highly regulated service sectors, such as finance and transport, where accuracy and reliability are critical. Here, avatars can present complex information in video or voice formats, improving understanding for staff and customers alike.

Examples

- Transport for London is using a voice avatar for station announcements at Colindale during redevelopment works.
- Since 2023, London Waterloo have partnered with Signapse.ai to provide sign-language video avatars for timetable announcements. Transport for London is also piloting avatar signers in collaboration with Silence Speaks.
- UBS Bank uses realistic AI avatars of its analysts to deliver recorded client advice when the experts themselves are unavailable.
- Consumer finance company Klarna created a chatbot overlaid with its CEO's voice clone to respond directly to customer queries.



Video avatar of BSL translator © Signapse

Tangible benefits for UK businesses and organisations

Large and small UK organisations using video avatar technology developed by the company Synthesia report tangible benefits in cost reductions, time saving and increased audience engagement with their communications. For example:

- Bolton College, a further education institution based in Manchester, adopted AI avatars to create learning videos for their students. Teachers reduced time spent recording videos by 80% (from 3 days to 30 minutes) and added 400+ videos to the College's training library in one year.
- HR tech company Screenloop, leveraged AI avatars to produce high-quality training videos in 5 days from script to delivery. They report 500 % savings on video budget, cutting the cost per video by approximately £1,700 versus production methods previously used.
- International SOS, a global health and security service provider, used AI avatars to produce multilingual staff training and compliance videos at scale. This raised compliance training completion rates by 12% to 97% within two months.
- Teleperformance, a global customer experience management company based in London, integrated AI avatars to streamline e-learning video production. The approach cut 5 days off production per video, delivered cost savings of up to £3,700, enabled consistent, standardised training across 170+ countries.
- Medistrava, a healthcare communications agency, used AI avatars to create explainer videos of technical products for healthcare professionals in different languages. The agency reports an 80% faster workflow and improved audience participation at large conference events.

Risks and challenges of AI human avatars

While AI human avatars have the potential to deliver significant benefits, these gains are accompanied by risks and challenges, which need to be managed with appropriate planning and resources.

At present, UK organisations have limited access to tailored tools or practical strategies to support the safe use of AI human avatars in their operations.

Targeted government intervention is needed to address this gap and enable the responsible and effective use of AI human avatars across sectors.

Case study: ScotRail and the voice of Gayanne Potter

In early 2025, ScotRail introduced an AI voice system developed by ReadSpeaker to modernise its train announcements. The Scottish-accented voice was later revealed to be a digital clone of actor Gayanne Potter, used without her knowledge or consent. ScotRail now faces potential litigation and reputational damage, undermining the efficiency and cost-saving benefits that the technology had promised. This case highlights how weak procurement standards and inadequate protections can erode public trust, incur costs and set back innovation.



Scottish voice over actress Gayanne Potter © BBC

We highlight the following risks and challenges in AI human avatar use by UK businesses and services:

Misinformation

Realistic avatars can mislead audiences, especially when deployed with persuasive language and false content. Avatars can increase risks of fraudulent impersonation, misattribution, and disruptions to democratic processes like elections.

Bias, discrimination and cultural homogenisation

AI avatars can produce inaccurate or biased results, like misrepresenting accents or appearances, because cloning tools tend to be trained on dominant markets and cultures. This can cause discrimination, undermine diversity and erode public trust in communications.

Cybersecurity vulnerabilities

Avatars rely on sensitive personal data that, if misused, can expose individuals and organisations to fraud or identity theft. Weak security around storing and sharing assets heightens these risks.

Environmental impact

Advanced Generative AI systems, cloning tools and real-time avatars are energy-intensive, yet their true footprint is under-reported, leaving users unable to measure and offset the environmental impact of their own use. Without sustainable practices, widespread adoption will contribute to environmental harms.

Labour replacement and displacement

Avatars can increase efficiency but risk displacing creative and technical roles, especially for professionals such as actors, translators, or customer support staff whose work may be replaced in part or in full. The impact of avatars on the workforce, as with other AI technologies, is yet to be comprehensively documented.

Over-reliance and emotional dependence

Avatars used in sensitive contexts like education, healthcare or memorialisation risk creating emotional dependency and reduced human interaction amongst users. These risks intensify when avatars are deployed in addictive settings such as gaming or pornography.

Data, privacy and IP infringement

Avatars created without appropriate permissions and informed consent may infringe data protection regulations and intellectual property rights like copyright. Current UK law does not adequately protect against unauthorised digital likeness use.

Loss of control and unfair contracts

Avatars can amplify inequalities for vulnerable workers who may be pressured to sign away rights to their likeness, intellectual property or data. These contracts strip individuals of consent, control and fair remuneration, as well as personal and creative agency.



Focus on: Rights, ownership and control of AI human avatars

Ownership of AI human avatars is not straightforward. Their creation is a multi-stage process that both reuses existing materials and generates new assets including biometric templates, fine-tuned models and outputs.

Consequently, the law treats the avatar not as a single, unified object, but as a bundle of assets, each governed by different rights like intellectual property and personal data protection.

What appears to be a seamless digital double is, in legal terms, a patchwork of fragmented rights across multiple stakeholders.

Overview of the digital cloning process

Most avatars are created in four key stages:



1. Tool selection

Organisations choose between off-the-shelf cloning tools or bespoke systems created by a third-party provider or in-house. The provider's terms of service often determine who controls data, models and outputs throughout the process.



2. Likeness data collection

Raw datasets recording the likeness of a specific individual must be gathered, typically photos, video, audio or motion-capture scans. These materials often need reformatting to be compatible with the chosen tool, which may generate further digital artefacts such as biometric templates. This step is focused on capturing and structuring the individual's likeness before fine-tuning.



3. Fine-tuning

At this stage, the AI system is calibrated with the prepared datasets and artefacts so it can accurately reproduce the person's features, expressions or voice. This process is known as "fine-tuning". The result is a persistent fine-tuned model: a reusable digital asset capable of generating convincing digital imitations of the individual at scale.



4. Output generation

The fine-tuned model is prompted to produce videos or voice recordings that can be integrated into new media or services such as films, training content, customer information, chatbots or interactive products.

Rights attaching to each asset

- **Underlying likeness** – The face, voice, or gestures of an individual are not protected by UK-wide likeness rights. Instead, protection is piecemeal, via personal data protection rights (e.g. UK GDPR), trademark or passing off in very limited cases. Other jurisdictions, such as Guernsey, California, or France, offer more robust personality rights.
- **Performances** – Embodied actions like speech or movement are protected when recorded under the Copyright, Designs and Patents Act 1988 (CDPA). But UK performers' rights do not cover digital imitations, leaving a regulatory gap directly exploited by cloning technologies.
- **Likeness datasets** – Audio, video, or 3D scans may be protected by copyright, performers' rights or personal data regulations. Where they arise, those rights often vest in, or are transferred to, the user of the digital cloning tool, who rarely is the person in the recordings.
- **Biometric artefacts** – Biometric templates often fall under personal data protection regulations and may be covered by copyright arising in the hands of the person who produced them, often the technology provider or its user.
- **Fine-tuned models** – Applicable rights and ownership of fine-tuned models are unclear. Providers frequently assert copyright, contract or trade secret protection over those models, yet they embed sensitive biometric data that engages the personal data rights of the individual being cloned, which should provide privacy safeguards as a result. There is legal uncertainty in how to lawfully and effectively balance the commercial rights of technology providers and users on the one hand, and the privacy of the cloned individual on the other, when the latter is not in control of the avatar.
- **Outputs** – AI-generated content may attract copyright, depending on its originality and the creative process. Authorship and ownership of AI-generated outputs remain uncertain and the subject of ongoing litigation and government consultation.
- **Prompts** – Prompts may contain creative content attracting copyright, performers' rights or personal data engaging GDPR. Ownership usually belongs to the person supplying the prompt.



Contractual control and inequity

Because statutory rights are fragmented, in practice technology providers and users rely on contracts to determine who controls avatars. This contract-based approach can exacerbate power asymmetries. Common patterns include:

- Perpetual “buy-out” contracts requiring workers to assign likeness data and rights indefinitely, often as a condition of employment or freelance engagement.
- Non-negotiable contracts granting technology users wide rights over the avatar, with limited scope for withdrawal or renegotiation by the person represented in the avatar.
- Avatars created for vulnerable groups (such as children, patients or consumers) without clear mechanisms for informed consent or later revocation.

UK workers' representative organisations like [Trades Union Congress \(TUC\)](#), [University and College Union \(UCU\)](#) and [Equity](#) advocate for stronger statutory and contractual protection of workers represented in avatars. Countries like Denmark are [actively reforming their national law](#) to bridge the gaps in protection described above.

Policy implications

- Ownership of AI avatars is fragmented under UK law, leaving individuals exposed to losing control over their digital likeness and organisations unclear about compliance. The UK's current framework is therefore unfit for purpose and will leave UK businesses and services unable to access the growth opportunities of the technology without policy intervention.
- Clearer statutory protections are urgently needed to balance innovation with accountability: safeguarding individuals from exploitation while enabling businesses to invest with confidence.



Recommendations

1. New Likeness Protection Rights

- The government should introduce UK-wide statutory likeness protection to safeguard individuals against unauthorised use of their image, voice or name in avatars and AI-generated content.
- These rights must provide both personal and proprietary statutory rights, with effective remedies. The UK government should ensure likeness rightsholders have easy access to enforcement forums, for example through the Intellectual Property Enterprise Court's Small Claims Track.
- The Department for Science, Innovation and Technology (DSIT), working with the Intellectual Property Office (IPO) and Information Commissioner's Office (ICO), should lead this reform. It should draw on the IPO's consultation on digital replicas and ICO's forthcoming programme of work on AI and biometric data.
- Comparative approaches, such as Guernsey's regime, protections in India, the US states of California and New York, or Denmark, as well as more recent proposals linking likeness rights with contractual protections, should inform the reform.
- Any new likeness rights must be carefully designed to prevent full or perpetual transfers away from the identity-holder, ensuring individuals retain long-term control and agency over their digital selves.



© Parliament.TV

2. Fair Contracts

Statutory protection against unfair terms

- The government should introduce statutory protections to limit exploitative contractual clauses requiring individuals to transfer likeness, intellectual property or personal data rights in full or indefinitely for digital cloning purposes. Such terms should only be enforceable where consent is demonstrably free and informed, and where fair remuneration is provided.
- The UK government should issue a notice, akin to the "copyright notices" issued by the IPO, to limit the interpretation of historical contracts as permitting the creation of AI human avatars, when no clear, informed consent to this effect has been obtained.

Guidance and contract templates

- DSIT, in collaboration with the Department for Business and Trade (DBT) and the IPO, should publish voluntary best practice principles and contract templates to guide ethical contracting around AI avatars. These resources should include plain-language clauses, model consent provisions and separate terms for likeness, training data and re-use of generated content.
- Existing tools, such as [Equity's AI toolkit](#), and the [European Union of the Deaf's contract template and framework](#), provide useful reference points.

Collective agreements

- Government should actively support collective bargaining and sectoral agreements that address the deployment of AI avatars in the workplace. This includes convening roundtables with unions, employers and technology providers to develop fair terms across industries. While performers' unions have initiated negotiations in the screen sector, other areas such as education, customer services and public administration require similar frameworks.

3. Guidance on the safe use of AI human avatars

Procurement guidance

- DSIT or DBT should establish procurement standards for organisations considering AI avatar tools. These standards must include due diligence checks on cybersecurity compliance, data provenance and licensing, ownership of fine-tuned models, and ethical deployment practices.

Rights and risk management, including cybersecurity

- DSIT, with the IPO and ICO should issue joint guidance for businesses and public services explaining how intellectual property and data protection law apply to the creation and use of AI avatars, supported by statutory interpretation notices and best practice resources.
- DSIT and DBT should issue sector-specific risk management resources to help organisations address vulnerabilities linked to AI avatars. Guidance should cover cybersecurity safeguards against data theft and leaks, as well as strategies to manage reputational, legal and ethical risks.

Awareness campaign and glossary

- DSIT, supported by the IPO and ICO, should lead a public awareness campaign explaining how digital cloning technologies operate, highlighting opportunities and risks, and promoting responsible adoption. This campaign should include a standardised glossary of terms to ensure consistency in training, regulation and cross-sector communication.

4. Information on the environmental impact of AI human avatars and sustainability standards

- DSIT or DBT should commission research to measure the environmental impact of AI human avatars in pre-recorded and live interactions. This information should inform guidance on sustainable practices and practical standards to help businesses and services account for their environmental impact with accuracy.

Glossary

AI avatar, human avatar or avatar, the digital recreation of a person's likeness using AI technologies.

AI model, algorithms trained to complete complex tasks.

AI system, an advanced computer program capable of performing tasks associated with human intelligence like analysing information or translating text.

AI tool, synonym for AI model or AI system.

AI training, the initial development phase of an AI model encoding knowledge and instructions into its algorithms to perform a task consistently.

Algorithm, a mathematical formula instructing a computer to perform a specific task.

Bias, the tendency of AI systems to generate prejudiced errors.

Biometric template, a persistent digital asset capturing identifiable features of a person, extracted by technology and used as a reference for their likeness.

Chatbot, a computer program that simulates conversations with human users.

Dataset, a body of information which can be used and processed by a computer.

Deepfakes, the digital imitation of a person, is synonymous to AI human avatar. The term 'deepfake' is predominantly associated with online image-based abuse.

Digital cloning or cloning, the process of digitally recreating a person's likeness.

Driving performance, a performance delivered by a third party to animate or 'drive' new movement or speech in the likeness of another. Driving performances are used to animate AI human avatars.

Fine-tuned model, the version of the AI system calibrated to reproduce a specific individual.

Fine-tuning, calibrating an existing AI system or AI model to the specific likeness of an individual. This process is distinct from AI training.

GDPR, General Data Protection Regulations.

Generative AI, AI systems capable of generating content like text, image, sound or film.

Hallucinations, errors generated by an AI system which can sometimes look plausible.

Likeness, the features of a person, such as their face, voice or gestures.

Machine-readable, information formatted to be understood by a computer programme like digitised images, text and sound, or values in a spreadsheet.

Output or AI-generated output, text, sound, image or video content produced using AI systems.

Performance, a person's embodied actions like speech or movement.

Prompt, an instruction directing an AI system to generate content. Instructions can be given in text, image, audio or video format.

Synthetic, AI-generated or machine-generated content.

Training dataset, the content that AI systems learn from in order to perform specific tasks.

Voice clone, the digital imitation of a person's voice, typically created with AI. It can also refer to an AI model fine-tuned to the vocal likeness of a person.

Voice print, an AI model fine-tuned to the vocal likeness of a specific individual.

Credits & acknowledgements

With thanks to research participants and contributors.

- This research finalised in September 2025, and made possible by the University of Reading's Policy Fund and Replique.
- Please cite this resource as: Mathilde Pavis and Dominic Lees, *AI human avatars: opportunities and risks for UK businesses and services* (2025, [SMRN](#) & [Replique](#)).
- For queries or further research, you can contact the authors at:



Dr Mathilde Pavis

✉ mathilde@workwithreplique.com



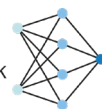
Dominic Lees

✉ d.lees@reading.ac.uk

- Graphic design by: Milos Stojanovic. Rights reserved. Rights to images and illustrations may be reserved by their owners.
- **Replique** advises creative agencies, media executives and organisations to help understand, manage and lead on AI and digital avatar technologies. Founded by legal and policy expert Dr Mathilde Pavis, Replique equips professionals with the knowledge, tools and strategies to navigate digital cloning with clarity and confidence. To find out more, visit www.workwithreplique.com
- **The Synthetic Media Research Network (SMRN)** brings together researchers, businesses, and stakeholders to promote ethical innovation in AI-generated media. We address the social, legal, and political challenges of Generative AI while exploring creative applications in the creative industries and other sectors. As an independent hub for thought leadership, SMRN fosters dialogue on ethical, business, and regulatory issues, working to build shared values and public trust in this transformative technology. To find out more, visit <https://research.reading.ac.uk/synthetic-media-research-network>



Synthetic Media
Research Network



repliQue

