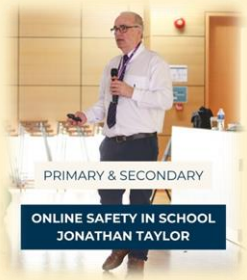
Online Safety for Schools



AI Smart Glasses: Benefits, Risks & Legal Considerations

1. Introduction

AI-enhanced smart glasses — wearable devices with cameras, microphones, AI assistants and real-time visual/voice processing — are emerging rapidly. They promise new ways to interact with digital information and the physical world. However, they raise unique **safeguarding, privacy, data protection, and legal challenges**.

This briefing summarises key benefits, potential dangers, and current legal frameworks that apply in the UK, EU and more broadly.

2. Key Benefits of AI Smart Glasses

Accessibility & Assistive Use

- Can support individuals with **visual impairments** or language needs by:
  - Real-time translation of text and speech
  - Object recognition
  - Navigation assistance
- These features can improve independence and inclusion.

Hands-Free Information Access

- Wearers can receive contextual information while on the move — for example:
  - Directions
  - Translated signs
  - Immediate answers to voice queries
- Useful in professional settings such as manufacturing, fieldwork, and healthcare.

Potential Educational Support

- Could support learners with additional needs by providing:
  - Prompting or coaching via AI
  - Immediate translation (for EAL learners)
  - Visual/reading assistance in real time

3. Major Risks & Pitfalls

A. Privacy & Unconsented Surveillance

AI glasses often include **discreet cameras and microphones**. This raises serious privacy concerns because:

- Wearers may record or capture bystanders **without their awareness or consent**.
- Miniaturised designs can make people unaware they are being filmed or analysed.

Risk Example: Demonstrations show facial recognition and doxing tools can combine live video from these glasses with public data to identify individuals in real time, leading to privacy breaches and misuse.

Implication: Unconsented data capture may violate personal rights and data protection laws.

B. Data Protection & Cybersecurity

AI glasses often collect, process, and transmit sensitive data (visual, audio, contextual), sometimes continuously:

- Data sent to cloud servers may be vulnerable to breaches or misuse.
- Third party AI systems processing this data may lack transparent controls over retention and secondary use.

This creates compliance risks under data protection regimes and workplace privacy laws, including:

- **GDPR / UK Data Protection Act 2018**: Any identifiable information processed triggers legal obligations.
- **Breach notification and security requirements** apply if sensitive data is exposed.

C. Ethical & Societal Concerns

AI smart glasses could:

- Enable pervasive surveillance, even in public spaces, chilling personal behaviour and freedom.
- Potentially erode anonymity, leading to issues of consent, profiling, and social discomfort.
- Compound biases in AI recognition systems, with disproportionate impact on marginalised groups.

This highlights concerns about **how society expects privacy in physical spaces**.

D. Safety, Distraction & Misuse

- Heads-up displays or notifications could cause *reduced situational awareness* and distraction, similar to phones or GPS.
- Misuse in sensitive areas (classrooms, workplaces, medical settings) can disrupt trust and operations.
- Some workplaces are already banning these devices due to legal or security concerns.

4. Legal & Regulatory Frameworks

A. UK & Data Protection

In the UK, the **Data Protection Act 2018** (implementing GDPR principles) applies to all processing of personal data — including recording images or audio via smart glasses.
The Information Commissioner's Office (ICO) has indicated that **wearable camera use may constitute personal data processing**, triggering obligations such as:

- Lawful basis for processing
- Transparency and consent
- Potential **Data Protection Impact Assessments (DPIAs)** for systematic high-risk recording
- Informing people before recording begins, where practical

Recording or processing identifiable images of others without legal basis may breach these rules.

B. EU AI Act

Under the **EU AI Act (2025)**, AI systems that collect or interpret biometric, facial, or voice data are often classified as **high-risk**, requiring:

- Additional documentation and compliance steps from manufacturers
- Transparency and safety declarations
- Clear data governance frameworks for AI behaviour

This impacts the sale and use of smart glasses in the EU, and sets a regulatory direction that may influence UK or global standards.

C. Other Applicable Law

- In some countries and jurisdictions (e.g., certain U.S. states), audio recording without consent is illegal.
- Location-specific privacy or photography laws (e.g., Japan) prohibit recording in public without permission.
- Intellectual property and venue terms can restrict recording in concerts or live performances.

5. Policy Implications & Practical Considerations

For organisations (schools, workplaces, public venues):

Policy Development

- Establish clear rules for when and where AI smart glasses are permitted.
- Ensure compliance with **privacy and data protection laws**.
- Require visible indicators or signage where recording may occur.
- Set out consent and data handling protocols.

Safeguarding

- In schools or public organisations, consider the risks to bystanders, pupils, staff and vulnerable groups.
- Avoid covert recording situations and emphasise informed consent.

Security & Risk Management

- Limit use in sensitive areas
- Ensure secure network connections and data encryption
- Educate users on responsible use

6. Summary

AI smart glasses have exciting potential — particularly for accessibility, information access, and real-time assistance. However, without robust safeguards and compliance with current legal frameworks such as **UK GDPR / Data Protection Act** and the **EU AI Act**, their use raises **significant privacy, ethical, safety, and legal risks**.

Balancing innovation with rights protection and transparency is critical as these technologies mature and become more commonplace.

QR CODE FOR DETAILS CURRENT ONLINE SAFETY WORKSHOPS

Presented by: Jonathan Taylor MSc
www.onlinesafety4schools.co.uk
onlinesafety4schools@ymail.com

Online Safety 4 Schools

Online Safety 4 Schools