



Consultation response

ICO draft guidance on consumer 'Internet of Things' products and services

About Parent Zone

Parent Zone is an organisation that sits at the heart of digital family life, providing advice, knowledge and support to shape the best possible future for children as they navigate a digitised world. Founded in 2005, we have collaborated with many organisations who share our vision, remaining responsive to the continually developing nature of digital technologies, and how they intersect with family life. We recognise enormous opportunities, whilst understanding the challenges that accompany them.

You can read the ICO's draft guidance on consumer 'Internet of Things' products and services, [here](#).

Our response

As ‘Internet of Things’ (IoT) products become more embedded in daily life – from smart thermostats to virtual assistants – we welcome new draft ICO guidance as timely. We are however concerned that there are significant gaps in the current guidance. Our view on the proposed regulatory approach is inevitably limited because of these gaps, and we set out a number of our concerns below.

In short, we question whether this regulatory approach is forward-facing enough to be effective when applied to a new era of digital technologies and IoT products. We note that the guidance covers a range of IoT products but equally recognise that certain categories of IoT devices – such as ‘always on’ wearables – appear to have been overlooked, or at the very least not given sufficient and explicit mention.

This is a significant blindspot considering the growing use of these products. In 2024, Meta reported selling over 1 million units of their Ray-Ban ‘smartglasses’¹ and we include further examples of wearables and their likely uptake in the following section.

The increasing accessibility of open source generative AI also means that the barriers to entry to this technology are far lower. As a result, we can expect a growing number of services to embed AI in their IoT products, including wearable devices but also a range of devices and toys that children use. We believe that these products will pose significant risks to users when it comes to their data and rights. There is an opportunity for the possible harms to be anticipated and minimised ahead of this tech reaching mass adoption. The current draft guidance and regulatory approach could be a missed opportunity to direct companies and establish guardrails, without further development.

In this response, we include a section on the likely uptake of these new technologies and then set out specific concerns relating to data, consent, and rights. A number of possible solutions and recommendations for the ICO are contained in our closing remarks.

¹ [Meta’s Ray-Bans smart glasses sold more than 1 million units last year | The Verge](#)

Emerging technologies

The uptake and use of tech like AI-assisted wearable devices and toys is set to increase – with factors like the improving capability of AI and decreasing monetary costs to users contributing to this. Mark Zuckerberg is on record as saying that those without AI smartglasses are "probably going to be at a pretty significant cognitive disadvantage"².

Wearable devices

Other case studies and developments also point to increased future uptake of these IoT products.

In 2025 Amazon acquired tech startup ‘Bee’, who produce AI wearables – Bee’s standalone bracelet device currently retails for less than \$50 and is designed to capture all of a user’s conversations in order to function as a virtual ‘assistant’. The Financial Times also reports that the popularity of Meta x Raybans AI glasses have led to ‘eyewear giants’ betting, perhaps optimistically, that smartglasses are set to eventually replace smartphones.³ Finally, and although specifics remain unclear, former senior vice president of industrial design and chief design officer at Apple, Jony Ive and OpenAI are in 2026 planning to begin shipping a ‘pocket-size, contextually aware, screen-free’ AI device.

The ICO’s draft guidance and regulatory approach offers multiple examples of IoT products but fails to specifically reference this category of wearable devices.

The absence of these products in the guidance is important: there is a clear distinction between a wearable wellbeing product like a fitness or heart rate tracker – which the guidance does reference – and an ‘always on’ AI wearable assistant. This difference in how these products function is crucial because the latter sort of wearable is deliberately designed to capture new categories of personal data (such as audio recordings of conversations) and to new extents (for example *all* of a user’s conversations, by default).

Because the capture and use of this data by these devices is novel, there are naturally new risks and harms around personal information, consent, and rights that need to be considered. For example, how can a third party’s – i.e. someone else involved in a

² [Meta Has Already Won the Smart Glasses Race | WIRED.](#)

³ [EssilorLuxottica bets on glasses replacing smartphones as value hits €100bn](#)

recorded conversation – personal data and their rights around access and erasure be protected? We explore this scenario in more detail below.

AI and children's toys

Whilst the ICO's regulatory approach does mention 'connected toys' the guidance fails to consider how a number of these products function currently, and how they will (or do) function when containing more sophisticated generative AI software.

For example, there is a distinction between a connected toy that can perform internet searches or play music based on a child user's prompts, and a connected toy that can mimic the behaviours and interactions of a genuine 'friend' or another human. This will pose specific challenges for the safety and rights of children.

The guidance does not currently appear to recognise the novel nature of these IoT products nor these additional categories of risk and harm. Failure to recognise these developments risks undermining the ICO draft guidance and regulatory approach.

Data

We are pleased to see the draft guidance recognise a broad range of data capture that can occur via IoT products. Reference to some of the complexities that can accompany data capturing – for example, the possibility of inherent bias within AI systems and how this might impact personal data processing – add important depth to the guidance and overall regulatory approach.

However we believe this approach is inadequately future-proofed and not anticipatory enough to recognise how data sharing and storing is likely to change, nor the impact this will have on some users of IoT products and relevant third parties.

Wearables and personal data

Some AI wearables are designed to function as 'always on'. Certain products – like Bee and Omi – record every conversation the user has whilst wearing the device, unless this feature is manually muted by the user. Though resulting in an 'effective' AI assistant – for example, creating to-do lists and event reminders based on information that may be forgotten or misheard – the level of data capture will likely be enormous and this will itself present risks and possible harms.

Third parties, for example, could easily and unknowingly provide personal information (contained in audio or video data) when having a conversation with an AI wearable user. 'Third parties' can refer to children, whose data requires special protections under UK

GDPR.⁴ A device may also capture personal data that a user themselves does not wish to have stored – for example when speaking to themselves, or when they have forgotten to turn off recording functions on their device. Given that these products are literally designed to be continuously worn, these scenarios are likely to occur frequently.

Oversharing or unintended sharing of data could also occur through children's use of AI-powered companion toys. Younger users of these products may not be able to differentiate between an IoT device and a toy which they have formed a personal bond with. If a child feels that a device is 'trustworthy' or does not understand what data collection can be used for by organisations, they may be less likely to exercise restraint when providing personal information about themselves or others.

As the ICO's guidance makes clear, without effective protections around data there can be no subsequent protection of consent or of rights.

Consent

The ICO sets out conditions where an individual's consent to store, process or share their data is valid. These conditions include consent being: 'freely given'; 'specific' (i.e. context-specific); and 'informed'.

We question whether obtaining this type of consent is likely or – in some cases even possible – when it comes to some use cases of IoT products like AI-powered wearables and children's toys.

Specific and informed consent

The ICO guidance states that in order to give specific and informed consent, people need to know:

- why an organisation wants their personal information
- what this organisation is going to do with their personal information
- who this information will be shared with (i.e. other companies)
- how they can withdraw their consent easily at any time

We agree that users of IoT products should have access to the above information when it comes to their personal data. However, there are situations where accessing personal information or withdrawing consent is more problematic where the information has been captured via always on data capture devices.

⁴ [Child online safety: Data protection and privacy - GOV.UK](https://www.gov.uk/child-online-safety/data-protection-and-privacy)

For example, a third party may consent to a brief in-person work meeting being recorded by another user's smartglasses or bracelet (this would be context-specific consent). However, if the conversation continues after the meeting 'ends', or if the nature of the conversation changes, then this consent no longer applies to a specific context. Further, in some use cases it is possible that third parties will be entirely unaware that their personal information is being captured, let alone what that information will be used for and by whom. If a third party is unaware that they are providing personal information they cannot plausibly be expected to have the ability to withdraw their consent "easily at any time".

The Age Appropriate Design Code states that the "passive collection of personal data" should be avoided by services and products.⁵ This in part helps ensure that children's data is not just collected by default and that consent, when given, applies to *specific* cases of data capture and processing. Whilst we support this guidance, we find it difficult to square with the nature of 'always on' devices. The ICO's regulatory approach needs to address this incompatibility to protect not just children, but individuals of all ages.

Freely given consent

Some IoT wearables may surface information and privacy agreements in ways that are disruptive and therefore dismissed without being properly understood. The ICO's regulatory approach stresses that services should not make use of 'confirmshaming' (i.e. nudging people towards making a decision about their privacy and data). However, obtaining informed consent from a user via (for example) their smartglasses as each conversation begins is, we would suggest, even more likely to nudge quick acceptance of conditions than a tick box on a social media platform. This will be particularly true for extended reality tech, where visual information surfaced is especially disruptive to the user experience.

We would also note that if a user does not know how – or if – they are providing personal information, nor what this will be used for, they cannot give consent freely. Our concerns around these IoT products and specific, informed consent therefore also apply to freely given consent.

Children's consent

UK GDPR and DPA 2018 specify that the consent of children under the age of 13 requires parental authorisation. We are pleased to see the ICO's approach reference this, as well as recognising that obtaining children's consent must be done in age-appropriate ways. Likewise, the Age Appropriate Design Code states that, for tech companies who process

⁵ [Age appropriate design: a code of practice for online services | ICO](#)

children's data, their use of this data must be explained in such a way that a child could reasonably understand and give permission (where appropriate).

We question how requests for parental authorisation will be surfaced as part of a child's interaction with wearable products and AI connected toys. We also question whether, if parents aren't fully aware of the personal and data-capturing nature of these products, their authorisation and consent (on their child's behalf) will itself be informed and valid. To support the ICO's approach, additional information and specific guidance for parents needs to be included in the guidance.

Similarly, some types of IoT products are designed to be companions rather than simply 'connected toys'. Research shows that both adults and children⁶ have a tendency to form 'relationships' with AI chatbots – viewing them as genuine friends or romantic partners with whom they have complex and emotional interactions. It is reasonable to expect similar outcomes in the context of children and young people when physical toys have similar functionalities. There are questions therefore around how freely a child or young person may provide consent. For example, when a child user views an IoT product as more than simply a device and instead as a conscious being (with its own thoughts and feelings) they may consent to agreements or provide permissions solely to avoid 'upsetting' their 'friend'. Alternatively, they may be worried that if they do not re-provide consent after an important update then the product will no longer like them or have the 'same relationship' with them. These scenarios would, we believe, result in a child or young person providing 'consent' but not doing so freely – owing to the nature of these IoT products and use of them.

The above concerns outline some of the difficulties in obtaining specific, informed and freely given consent for certain types of IoT products, alongside the need for further guidance.

⁶ [Coded Companions: Young People's Relationships With AI Chatbots | VoiceBox;](#)

[Me, Myself & AI: Chatbot research | Internet Matters](#)

Rights

We are pleased to see the ICO highlight users' rights and inform services on how they can help users realise these. We remain concerned however that the ICO's approach is not forward-facing enough for these rights to be preserved when it comes to the uptake and use of new technologies.

The 'right to erasure'

An individual can exercise their right to erasure only if they know that their personal data has been captured and which organisation has done so. Third parties who are unaware that data like their imagery or audio have been recorded by wearables cannot therefore exercise their right to erasure. It is possible for organisations producing wearables to introduce design features that inform third parties that a device is capturing data (for example, a red 'on' light appearing on a pair of smartglasses). Despite this, we remain sceptical that signs of being recorded would be recognised by all third parties – particularly in busy settings, settings where they may not expect to be recorded (such as a gym or outside a school), or where a third party is broadly unfamiliar with the nature of newer, novel devices.

In some cases users are required to submit a 'subject access request' in order to see what personal information has been stored by an organisation. Such a formal process may be at odds with use cases where children have developed a relationship with an AI-powered toy. These sorts of new interactions with novel technologies need to be considered by the ICO so that users can effectively understand and exercise their right to erasure.

The 'right to object'

A third party not knowing what data is being captured – or by whom – is also a barrier to their right to object to use or processing of their information.

Again, an individual can only object to storage or use of their data if they know that this data is being stored or used in the first instance. Individuals may also be unlikely to conceive that their data is being captured in very informal settings and interactions with others. For example, a wearable bracelet worn under a long-sleeve shirt during a 'private' conversation in someone's home or vehicle, could capture a wide range of personal information and data without a third party ever being remotely aware that this is taking place.

We should also expect that as these types of IoT products become more widespread it will become less clear which company has produced the device – particularly with

imitation devices appearing similar to more popular brands. This is a further obstacle to a third party understanding which organisation has captured their data, providing they are aware of this capture in the first instance. A lack of clarity around where an individual's data 'is' will be another obstacle to someone exercising their right to object.