Draft response - ICO consultation on the corporate strategy, summer 2026.

Executive Summary

We welcome the opportunity to comment on the ICO's new draft Corporate Strategy for 2026-2028.

Our response highlights the need for the ICO to maintain focus on its core functions which centre on upholding information rights and promoting data privacy for individuals. Throughout the strategy, these priorities should be reflected and not neglected in favour of actions targeted more strongly towards secondary growth and innovation objectives.

- We disagree with the proposed purpose stated in the draft strategy, 'to build trust in responsible UK data use and innovation', because it lacks reference to core ICO responsibilities of upholding and ensuring data rights.

- We support the intentions that are reflected in the four strategic outcomes but suggest these should be reframed for better clarity which would strengthen the strategy's messaging. As written, they lack focus on the impacts that can be directly achieved by the ICO's work on data and information protections.

- We support the areas selected as the four identified regulatory priorities but disagree with the framing of the priorities. We suggest the ICO should reframe these to align more closely with their remit and promote more appropriate, understandable goals.

- We are highly supportive of the included commitment to enforcement measures set out in the strategy and encourage the ICO to maintain and follow through on this intention to better ensure achievement of the strategy's potential impacts.

Our answers to the consultation questions relevant to Which? are provided below.

Q9: To what extent do you agree or disagree with our purpose 'to build trust in responsible UK data use and innovation'? Please comment on the reason for your answer.

Response: 'Disagree'.

We believe that the ICO's core functions are to uphold information rights, promote openness by public bodies and promote data privacy for individuals (as described on the gov.uk website)[1]. Building trust should not be the primary strategic purpose, but would rather be an outcome of improving and ensuring data protection.

---

[1] https://www.gov.uk/government/organisations/information-commissioner-s-office

A better framing of this purpose might be ‘ensuring responsible UK data use, which would build trust…’, bringing the focus back to concepts that are within the ICO’s remit. The current focus on building trust itself is too vague and broad; it takes on a responsibility that sits with all organisations that interact with data, not solely with the ICO.

We encourage the ICO not to neglect their core data protection aims and regulatory role in favour of priorities targeted more directly towards growth. The ICO’s purpose should focus on upholding individuals’ data privacy and other data rights, which in turn will support innovation and economic growth. For example, through their co-ordination, compliance and monitoring functions, regulators can drive the development and effective implementation of trust frameworks which are key to the effective operation of smart data and digital ID schemes[2].

Q10: To what extent do you agree or disagree with our strategic outcomes? Please comment on the reason for your answer.

- *People have increased trust, allowing them to engage confidently in the modern data economy, sharing their data with greater confidence and benefitting from its innovative use*
- *Organisations feel more confident using and sharing personal data safely, recognising that building public trust is a foundation for building their businesses and economic growth*
- *Public authorities are transparent, providing public information openly and on time, which helps foster trust in public services, especially as they undergo digital transformation*
- *Criminals and negligent or irresponsible organisations are appropriately held to account - protecting people, preserving fair and competitive markets, deterring poor practice and building trust in regulation.*

Response: ‘Neutral’.

The strategic outcomes are appropriate long-term targets as their achievement should be assessable and they generally align with the strategy’s stated regulatory priorities. In addition, the outcomes interlink in that the latter three should help to achieve the first (consumer trust). However, the outcomes are worded in a way that is too broad, lacks cohesion, and is confusing. To strengthen the ICO’s messaging, they should be reframed.

We are interested in the outcome regarding increased trust, as this can follow from ensuring strong protection and enforcement of individuals’ data rights, which is key in the modern data economy as data- and AI-driven services increase. On the other hand, trust can increase for reasons other than true boosts in protection - e.g. through consumer familiarity or false understanding of tools/contexts - and the strategic outcome should not accept an increase in trust which is not justified or in fact increases exposure to risk for consumers. The outcome of ‘increased trust’ should only be endorsed if it flows from real improvements to data protection levels and consumers’ feeling able to exercise their rights, for example through the development of Smart Data schemes. A better phrasing of a consumer-based outcome

[2] Which?, ‘Building consumer trust in Smart Data’, Dec 2024. [Link].

could reference people having an appropriate level of data privacy, which could drive increased trust.

The outcome relating to organisational confidence in safe data use is important. Our regular Consumer Insight Tracker survey results show that a majority of consumers are worried about both how organisations collect and use data about them (71%) and about the security of the data they share (72%)[3]. This is most commonly due to concerns about data breaches leading to scam/fraud targeting, and about the use of data when sold on, particularly for targeted advertising[4]. These are factors for which data-processing organisations are responsible. The survey results suggest that responsible data use by organisations, e.g. limited and transparent use of data which consumers feel they have validly consented to, would be one of the most impactful ways to improve consumer trust/confidence in data use. Better and clearer application of data rules by organisations, whether through improved understanding or simply greater respect for them, will help protect consumers and is a commendable outcome for the ICO to seek. However, it is essential that the ICO effectively enforces organisational adherence to data handling frameworks; current annual reports show that it is underperforming against targets for resolving data subjects' complaints[5]. This outcome requires strong underlying enforcement for it to be achieved.

We are highly supportive of the fourth outcome, particularly in relation to smart data risks and to online fraud from data misuse. The growth of smart data is a risk factor for increased poor data practice, due to the general increase in data flows and handling of personal data inherent to such schemes[6]. Online fraud remains the most common form of crime in the UK[7], and driving towards its reduction is important; the ICO should do what they can to achieve this from a data regulation point of view. By the regulator acting more strongly to enforce against those who misuse data, putting it at risk, security of data can be improved as the deterrent increases. However, the specification of 'criminals and negligent or irresponsible' actors as targets of this outcome unnecessarily narrows its scope. Cyber breaches can occur regardless of organisational intentions or attitudes, for example due to employee mistakes or circumstantial chains of events; it might not always be fair to label these negligent or irresponsible, but the ICO should still seek to address such events. We consider that a better objective would be for 'criminals and *all* organisations' to be appropriately held to account.

Beyond this, the mention of 'fair and competitive' markets in this outcome feels out of place as holding organisations to account for data protection breaches is unlikely to have competitive effects. If the ICO feels they can aid the competitiveness of digital (or other) markets and want to target this, this would be significant enough of an area to warrant its own strategic outcome.

Overall, all three of these outcomes place too much emphasis on markets, growth and increases in data sharing where they should focus more on increases in the strength of data

---

[3] Which? Consumer Insights tracker article, August 2026. [Link].
[4] Which? Consumer Insights tracker article, August 2026. [Link].
[5] Information Commissioner's annual report and financial statements 2025/2, page 42.
[6] Which?, 'Building consumer trust in Smart Data', Dec 2024. [Link].
[7] ONS Crime Survey for England and Wales, March 2026. [Link].

protection and compliance with data protection laws. These are the elements of markets that the ICO can have a direct impact on and therefore should look at in its outcomes.

Q11: To what extent do you agree or disagree with our regulatory priorities? Please comment on the reason for your answer.

- *Personal data use that helps, not harms, children*
- *Promoting trust and transparency in AI*
- *Public services that use people's data responsibly*
- *Building cyber resilience to keep people's data safe*

Response: 'Disagree'.

We support the intentions behind the *trust and transparency in AI*, and *building cyber resilience priorities*. However, we consider their framing to be misleading.

An initial note on the first priority ('data use that helps, not harms, children') is that we would encourage the ICO to widen this, for example by referencing 'vulnerable groups, including children'. This would better meet principles of equity and inclusion, and help to keep harms experienced by other vulnerable groups in society within public/regulatory consciousness.

Regarding AI, as its use increases across sectors it is essential that consumer protections increase alongside. There are clear data risks from AI - e.g. hyper-personalisation impacting consumer choice and pricing, exclusion of high-privacy consumers who opt out of data sharing, and loss of truly informed consent given the lack of transparency/understanding of how and when data may be used by AI. The capability and deployment of AI-based tools is also increasing quickly across various sectors. Our research shows that 69% of UK consumers are worried about how businesses are using AI in ways that affect them as a consumer[8]. Among the most common themes cited for this concern were data security issues (risk of scams) and a general lack of trust and control in AI as it evolves quickly and without specific regulation[9]. These are issues that improved levels and visibility of data protection could help to mitigate, as effective data regulation can tackle risks of scams and offset data-based AI risks by ensuring organisations follow processes that prioritise the security and safety of data they hold. Therefore, it is appropriate for the ICO to consider data in the context of AI to be a priority.

However, the ICO should be careful about aiming to promote trust in AI via robust and appropriate means, i.e. through better consumer protection, rather than in ways that encourage consumers to adopt AI whilst leaving them open to risk of harm. This priority would be better reframed to avoid language of 'promoting trust', which seems irresponsible - for example, 'promoting *trustworthy* and transparent AI' would be more reasonable.

Regarding cyber resilience, this is important to consumer safety in terms of online fraud, data breach and smart data risks, and we welcome the focus from the ICO on this. Data is key to the proliferation of more sophisticated frauds and is often a target of cybercrime.

[8] Which? Consumer Insights tracker article, August 2026. [Link].
[9] Which? Consumer Insights tracker article, August 2026. [Link].

Across the data- and AI-related questions asked in our consumer survey, fears about data breaches and consequent scams/fraud recurred as one of the top reasons given for worries across categories measured (data security, data use/collection, AI use); almost half of those who were worried about the security of the data they share linked this to fear of hacking and consequent scams, and this fear was frequently repeated when respondents were asked about their data use/collect and AI use concern along with comments questioning organisations' data security competence. This shows how front of mind data safety in terms of cyber-breaches is for consumers. However, given the breadth of the cyber resilience remit and the work of other bodies in this area, e.g. the NCA and NCSC, we encourage the ICO to make clear, once this strategy is in place, the practical approaches and actions it will take to support this priority. This priority risks implying taking responsibility for elements of cyber resilience that are not within its remit. It should be specific about what its role is in achieving progress in UK cyber resilience, which we expect would relate to guiding organisations to put robust data protection measures in place and enforcing compliance with required standards.

Q13: To what extent do you agree or disagree with the proposed measures? Please comment on the reason for your answer.

Response: 'Agree'.

We have considered the metrics that relate to assessment of impacts on consumers/ individuals. We support the range of metrics intended to measure the views of the public. However, some of these could be strengthened to deliver more meaningful feedback:

- Rather than (or in addition to) measuring the percentage who are 'aware of' data rights and 'confident' sharing their data, assessment should consider the percentage who *feel empowered to exercise* their data rights. Which? research has shown that people often feel powerless to engage with organisations that collect and use their data, which drives disengagement with the data economy[10].
- Asking about whether people feel confident that those who misuse data are 'held to account' feels vague. A more informative approach would be to ask whether they feel those actors *face consequences* and whether they feel *redress is available* in such situations.
- Questions could address not just data protection rights but also data portability rights, which could be key drivers of the ICO's interests in trust and innovation levels.

Q14: What impacts, positive or negative, do you expect the strategy to have?

If implemented with the backing of strong and committed enforcement by the ICO, the strategy could have positive impacts through its focus on four key areas. The high and steadily growing levels of data-related consumer concern in relation to data security and AI use shown by our consumer tracker[11] makes these areas good candidates for achieving improvements in consumer protection, confidence and engagement when it comes to data.

---

[10] Which? 'Control, Alt or Delete?' report, June 2018. [Link].
[11] Which? Consumer Insights tracker article, August 2026. [Link].

We note the strategy is intended to cover only a two-year period and this could limit its ability to be effective in fully achieving the strategic outcomes / long-term success. It will be important for progress and themes to be followed through in the following IC strategy.

Q18: Do you have any final comments you have not made elsewhere?

We would like to comment on the section 'Our Regulatory Approach'.

We agree with the commitment to enforcement of data protection rules by the ICO, as per the references to 'investigative interventions' and 'corrective measures' in the list of points from the new regulatory action framework (under the 'Our Regulatory Approach' heading at p11 of the draft strategy). Regulator-led enforcement against data protection breaches will be key to achievement of the strategic outcomes, given the low likelihood of regular enforcement by individuals and the ICO's ability to take an overview across cases to enable joined-up action and informed targeting of problem areas.

The ICO could go further by including an additional regulatory priority around Enforcement, or highlighting it within the Internal Transformation priority. In addition, the ICO should support Which's call to implement Article 80(2) UK GDPR right which would enable collective redress for consumers' data rights, removing a critical barrier faced by individuals in exercising their data subject rights[12], as an effective action in tackling all four of the stated regulatory priority areas.

---

[12] E.g. 'DSIT's call for evidence on Data Intermediaries - Which? Response', May 2025. [Link].