ICO Corporate strategy: Building trust in responsible UK data use and innovation

Context

In June 2025, the UK Data Use and Access Act 2025 confirmed the future transition of the ICO from a corporation sole governance model, with all powers and responsibilities vested in a single 'Information Commissioner', to a more typical Commission model with a non-Executive Chair and Board, and a separate CEO.

This represents a critical modernisation of the ICO, bringing greater resilience and diversity to our organisation’s strategy and direction.

At the time of writing, the date of transition to this new model is yet to be confirmed but is anticipated to be the autumn of this year. The new Information Commission, as required under the Data Use and Access Act, will then be in a position to prepare and publish its first strategy.

This strategy therefore sets clear priorities, provides direction and clarity to ICO stakeholders and staff during an important transition for our organisation.

Given the pace of change in many of the industries and sectors we regulate, and the need to align with our forthcoming transition to the Information Commission, the strategy covers a two-year period from 2026 to 2028.

Foreword from the CEO

Data is what data does. It might be the profile behind an algorithm deciding if we are creditworthy or invited for a job interview. It could be the trace left by a child scrolling through social media at midnight. It may be a life changing medical diagnosis made possible through advanced research. Or, more personally, it could be my assistive technology understanding and responding to my needs and preferences.

Our data is part of the fabric, some say the currency, of modern life - and the question of whether we benefit or are harmed from its use has never mattered more. The ICO exists because that question needs an answer people can trust.

But we are operating at a moment of genuine tension.

Data driven harms are real, and the impact when information rights are ignored can lead to life-changing harm and detriment. Avoidable data breaches continue to undermine trust in major institutions. The sheer complexity and apparent opacity of new technologies leave many people and businesses feeling confused and disempowered.

At the same time, the promise of data-driven innovation - better healthcare, more responsive public services, frictionless interactions with businesses big and small, and AI that genuinely improves lives – is equally real and urgent.

The UK cannot afford to squander that promise through regulatory uncertainty, irresponsible data use, the associated erosion of public trust and low adoption of beneficial new technology. We must also recognise that the task of complying with modern data laws and using data responsibly is not getting any easier.

Parliament has recently given the ICO a refreshed and modernised mandate that balances this inherent tension in our society and economy. This strategy describes how we will step up to that mandate and transition to our new governance model, not in the abstract, but by focusing on a clear purpose to build trust in responsible UK data use and innovation, and the regulatory outcomes most likely to help achieve it.

I do not accept that our remit means choosing between protecting people, enabling innovation and having regard for economic growth. If harnessed effectively, they should be inseparable. Organisations that invest in strong data protection build public trust which acts as the foundation for more successful innovation and sustainable growth.

Higher standards of data protection are also an important benefit of responsible innovation - as we see through the development of privacy enhancing technologies. Public services that are transparent deliver more trusted and effective outcomes. And children who feel safe online grow into adults who engage more confidently in the digital economy. When regulation is done well in partnership with all players in the system, protection and progress are mutually reinforcing and build public trust. From big tech to small businesses, government to civil society - a culture of trusted data use is a shared endeavour of consistent behaviour and clear expectations. Our relationships with our stakeholders will require partnership working, support and mutual accountability.

To Parliament: we take our accountability seriously. This strategy is built on our statutory duties, and we will report against them openly and with rigour. We welcome scrutiny - it is part of how public trust in regulators is itself maintained.

To businesses, large and small: I believe the vast majority of businesses are responsible, and we share the aim of reducing the cost/burden of regulatory compliance and enabling growth while maintaining high data protection standards. We expect you to focus on achieving legal compliance, demonstrating accountability and engaging with us openly when innovating. We commit to providing clarity, highlighting responsible practices and to taking proportionate, targeted action against those whose poor practice undermines the standards responsible organisations work hard to maintain.

To public services: the ambition to transform how government uses data to serve citizens is timely and necessary. But it can only succeed if the public believes their data is handled with care and they are benefiting from its innovative use. We stand ready to support that ambition - and to hold public bodies to account for maintaining appropriate standards of data protection using the full range of tools available to us.

To the public: you are why this strategy exists. The choices we make - about where to support and enable, where to investigate and sanction and how to allocate our resources - are all ultimately in service of your ability to trust the organisations and services that use your data. We will provide you with information and tools to protect yourselves where appropriate, and we will have your back in those areas where the risks are greatest.

To my ICO colleagues: this strategy is how we each show up to make a difference. It is the focus for our curiosity, the calibration for our collaboration, the target for our impact and the reason for our inclusive practices both within and outside the ICO. And it is the roadmap for how we must each continue to invest in our personal learning, development and growth.

The ICO is funded primarily through the payment of fees by those we regulate. With a remit spanning the whole economy we must deploy our resources, in line with clear priorities, and in ways which deliver best value for money. We also can't be everywhere at once. We have made deliberate choices about the issues we are prioritising in support of our strategic outcomes - children's data, AI, public sector data use, and cyber resilience. These are the areas where the risks are greatest, where public trust matters most, and where our intervention can make the strongest difference.

Our research and experience tell us that we do this most effectively when we are striking the right balance between acting proactively to prevent harm, enabling responsible innovation, and targeting our enforcement action on criminal, negligent and the most irresponsible practices. Under this strategy we will make sure this balance is struck openly and transparently. And we'll be open about our transformation from within too. A more agile, modern ICO is better placed to be a trusted partner, tracking and intervening where necessary in some of the most complex data use cases of our society and economy.

We will build on our transparency about how and what we regulate to encourage and enable our stakeholders to hold us to account for the outcomes we achieve. We will also engage directly, and with humility, in the important discussions our work rightly stimulates and when working in lockstep with our fellow regulators at home and overseas.

Trust is built slowly and lost quickly. The ICO team and I are committed to building it - consistently, transparently, in partnership with others and with a clear sense of purpose and outcomes.

I present this strategy by inviting all those with an interest in building trust in responsible UK data use and innovation to join with the ICO to achieve more together than we can accomplish alone.

Paul Arnold MBE
Chief Executive Officer

Our statutory duties

The UK Information Commissioner's Office, and the future Information Commission, is a statutory regulator. Our remit is defined by Parliament, and it is against these duties that Parliament ultimately holds us to account. Our work is centred on the governance of personal data and information rights under the:

- Data Use and Access Act 2025, the UK GDPR (as amended);
- Data Protection Act 2018;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004;
- Network and Information Systems Regulations 2018 (which is currently being updated and expanded in the Cyber Security and Resilience Bill); and
- other legislation entrusted to us.

Our core duties include:

- **Protecting personal data**: securing an appropriate level of protection for personal data, upholding people's rights and acting in the wider public interest.
- **Promoting public trust and confidence**: ensuring transparency, fairness and accountability in how organisations process personal data.
- **Regulating with innovation, competition and growth in mind**: acting proportionately while supporting innovation, competition and sustainable economic growth.
- **Safeguarding children**: children merit specific protection for their personal data, as they may be less aware of the risks, consequences, and their rights related to data processing.
- **Freedom of information and transparency**: overseeing and enforcing openness obligations on public authorities.
- **Cyber security**: improving UK cyber resilience.

In carrying out our core duties, we must also consider safeguarding public and national security and the importance of preventing, investigating, detecting and prosecuting criminal offences.

This breadth gives the ICO a distinctive role within the regulatory landscape because we are:

- one of the few regulators with a cross-economy remit, which gives us a system-wide view of how data is used across sectors, technologies and services;
- uniquely positioned to identify emerging risks, align expectations across different parts of the economy, and support consistent, trusted approaches to data use; and
- able to act as both a safeguard for people's information rights and an enabler of responsible innovation, so we can bridge the gap between protection, trust and economic growth.

This remit is the anchor for our purpose, the outcomes we intend to achieve, our regulatory approach and our priorities.

Our purpose

By setting our purpose to **build trust in responsible UK data use and innovation**, we want something simple yet meaningful:

For people to:

- know how their personal data is used;
- trust that it is appropriately protected; and
- believe they benefit from its innovative use.

These fundamental drivers of trust are the foundations of both data protection and sustainable growth for the UK data economy.

But people's trust in the way their personal data is used and protected has never been more under threat or at risk. Likewise, the potential opportunities available through innovative data use have rarely been more tantalising. The risk and opportunity landscape we must navigate as a regulator to achieve our purpose is therefore complex and carries a number of inherent tensions we must manage clearly.

This is why building trust is the thread running through everything we do.

What success looks like

Measuring a regulator's success is inherently complex. The outcomes we seek - such as increased trust in how personal data is used - are shaped by a wide range of factors beyond our direct control and are ultimately delivered by the organisations we regulate.

In addition to measuring perceptions of trust itself, we will therefore measure the specific changes in stakeholder behaviour which most directly maintain and build trust in responsible UK data use and innovation. We have captured these in the strategic outcomes we are prioritising.

Our strategic outcomes

Through our remit as a regulator, we will work to build trust in responsible UK data use and innovation so that:

- 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; and

- 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.

Working towards these strategic outcomes will see our work contribute to economic growth by:

- making sure organisations fully understand what the law enables, and the predictability of our response as a regulator, helping them to target investment and set their risk appetites with confidence rather than unnecessary caution;

- helping organisations minimise regulatory friction and the cost of compliance; and

- highlighting good data use and innovation practice and promoting the safe adoption of related tools and products.

Our approach is grounded in a simple theory of change. We can improve how personal data is used across the system by:

- setting clear expectations;
- enabling and highlighting responsible practice; and
- intervening proportionately where standards are not met.

This, in turn, builds public trust, enables organisations to innovate with confidence, and supports sustainable economic growth. These outcomes are mutually reinforcing, and our strategy is designed to deliver them together rather than in isolation.

Risks and priorities

Based on our ongoing scan of the environment we regulate, we are prioritising our actions under this strategy based on five systemic risks and opportunities. They represent the greatest barriers and opportunities to achieving our strategic outcomes.

Our risks and opportunities

A growing imbalance of power in data use reduces meaningful choice and control. In particular in digital services used and relied on by children and those at most risk of harm. This exposes those least able to protect themselves to disproportionate harm.

Rapid advances in AI and data-driven technologies outpace organisations' ability to deploy them safely. This creates risks of opaque and unaccountable decision-making that undermine confidence and innovation.

Escalating threats and weaknesses in organisational governance, especially cyber resilience and data stewardship, leave personal data exposed to loss, misuse and exploitation. This erodes trust in both individual organisations and the wider system.

The pace and scale of public sector transformation increases reliance on complex data sharing and digital systems without consistent accountability. This amplifies the potential for systemic failure across essential services and missed opportunities to innovate successfully and support economic growth.

Insufficient organisational culture, capacity and capability to keep pace with the scale and complexity of change in data use constrains our ability at the ICO to prioritise and deploy our resources flexibly and dynamically. This limits our effectiveness in responding to evolving demand.

We will keep these risks and opportunities under continuous review, and they will directly inform and drive how we allocate resources across our priorities and choices.

Our regulatory approach

Using our new regulatory action framework, we will continuously assess risk and determine the most effective mix of activity through:

- education, engagement and influence, to raise awareness, influence behaviour and resolve issues cooperatively through light-touch, high-reach interventions;
- support and guidance, enabling compliance by creating accessible, practical advice and tools tailored to organisational needs;
- regulatory cooperation, strengthening regulatory outcomes through collaboration with domestic and international partners;
- report handling to respond proportionately to self-reported breaches, complaints, and notifications, using them to inform broader regulatory action;
- authorisation and formal advisory mechanisms, to shape and approve data protection practices through the approval of corporate rules, codes of conduct and certification;
- investigative interventions, gathering evidence and assessing compliance through the use of notices, warrants and investigatory powers; and
- corrective measures, compelling compliance and deterring future breaches through corrective powers including warnings, reprimands, enforcement notices, penalties and prosecutions.

This new framework will guide how we balance our statutory duties. We will establish and deliver a balanced pipeline of regulatory interventions based on a clear assessment of risk and agreed outcomes.

Our evidence shows that prevention and early intervention deliver the greatest impact. We will therefore maximise opportunities to enable organisations to get it right first time by providing clarity on what the law requires and supports.

At the same time, we will take targeted and proportionate enforcement action where standards are not met, to deter poor practice and protect people.

Allocating our resources

The ICO is predominantly funded through fees paid by the organisations we regulate. Our annual operating budget is approximately £116m per annum. We must allocate this budget to achieve the best value for the 69.5 million people we are here to help protect and the approximately six million UK organisations we regulate.

This requires us to make difficult choices and important trade-offs between potential regulatory interventions, which by themselves are all valuable.

We must therefore allocate our resources in line with our regulatory approach, prioritising activities that deliver the greatest impact against our strategic outcomes. This means we will:

- focus our direct regulatory effort on areas of highest risk and systemic importance;
- invest proportionately less resource in routine or lower-risk work;
- maintain capacity and flexibility to respond to unexpected risks or issues of public interest; and
- focus on achieving the best value for money in all the work we do.

Where activity falls outside our priority areas, we will focus on agile approaches, identifying when we have achieved sufficient impact and redeploying our resources accordingly. Our leadership roles, responsibilities and operating model will reflect this approach.

Turning insight into action

Demand for our complaint and breach reporting services continues to grow. But we cannot afford to respond by increasing our investment in these services. We will therefore focus our detailed intervention on the cases that present the greatest harm or systemic risk.

We will use the wider body of complaints, reports and intelligence to identify trends and emerging issues across the economy. This insight will inform our priorities, shape our interventions and highlight poor practices that require attention.

Targeted engagement and supervision

Given the breadth of our remit, we will target our engagement and supervisory activity where it can have the greatest influence. We will:

- prioritise engagement with organisations and sectors with the greatest opportunity to inform and influence our outcomes;

- focus supervision on those entities and activities that align most closely to our four regulatory priorities; and
- work with organisations to understand their context and provide clear expectations for accountability.

Using technology to improve effectiveness

We will increase our use of AI and advanced data analytics to improve how we regulate. This will enable us to:

- automate processes and improve efficiency;
- enhance our ability to identify risks and emerging issues; and
- deliver more responsive and effective services to stakeholders.

As both a regulator and a user of these technologies, we will demonstrate what responsible adoption looks like in practice.

Leading and shaping the wider system

Our role extends beyond direct intervention. We have a responsibility to shape and influence the wider system in which data is used both domestically and internationally. We will exercise system leadership by:

- convening regulators, policymakers, industry and civil society to address shared challenges;
- aligning regulatory expectations to reduce duplication and inconsistency;
- working domestically and internationally to promote consistent standards and coherent approaches; and
- identifying and amplifying good practice across sectors.

International context

Personal data transfers underpin the global economy, innovation, security, and everyday services. But growing geopolitical complexity and changing national approaches are increasing compliance challenges for UK organisations and risks to public trust.

We at the ICO will respond through:

- focused, outward-looking international engagement;
- deepening bilateral and multilateral partnerships;
- practical guidance for UK organisations;
- shaping global standards;
- building new alliances where priorities align;
- rapidly applying international insight to support international data transfers; and

- enabling UK innovation and driving practical alignment across the global DPA community.

Our priorities

Our regulatory priorities

The most significant choice we are making is to focus as much effort as possible on four regulatory priorities. They reflect our assessment of the areas where we can, and need to, make the greatest difference to mitigate our most strategic regulatory risks and opportunities. We will review these priorities annually and report outcomes against each priority in our annual plans and reports.

1. Personal data use that helps, not harms, children

Children now grow up in an environment where personal data shapes much of their digital experience. **99% of children spend time online**, and nine in 10 own a mobile phone by age 11.[1] Their use of social media, gaming and rapidly expanding education technology services continues to increase.

Yet many children engage with services not designed for their age. The use of children's data in these services, places them at greater risk of profiling, targeted advertising, and exposure to harmful content. Parents also say they are worried about their children sharing personal information with people or services they do not trust.

So that children can engage more confidently online, we will work with partners in the UK and internationally to ensure providers in the digital and education technology sectors recognise:

- the specific risks their services represent for children; and
- embed a privacy by design approach.

By protecting children and providing greater clarity on how their data can be used responsibly, we will support the development of trusted digital services. This will help organisations to innovate with confidence and contribute to sustainable growth in the UK digital economy.

Together, we'll take action and build the trust of children and families to navigate the digital world safely and positively.

[1] Children's Media Literacy Report 2025

2. Promoting trust and transparency in AI

AI is reshaping how people live and how organisations deliver services. The OECD estimates AI could add £55–£140 billion to UK output each year by 2030, and investment is rising as organisations seek more personalised, automated and data-driven services. Public adoption is also growing rapidly: **the number of UK adults using AI doubled from 10 million in 2024 to 20 million in 2025**.

But trust lags behind. While the potential benefits of AI appear to be a regular topic of debate, only 33% of people trust companies using AI to protect their personal data, a figure that has declined each year since 2023.[2] While 63% of adults have heard of generative AI, only 33% are optimistic about its future impact.[3] People worry about safety, fairness, bias and transparency - concerns that must be addressed for the full economic and societal benefits of AI to be realised.

As personal data sits at the heart of AI development, we at the ICO have a critical role in:

- providing clarity and reinforcing responsible innovation. Building that trust is essential to unlocking the full economic potential of AI, enabling organisations to adopt and scale AI technologies with confidence and supporting productivity across the UK; and
- ensuring people can engage confidently in an AI-powered economy. By setting clear expectations for the responsible use of personal data in AI, we will reduce regulatory uncertainty and enable organisations to invest, develop and deploy AI technologies that are trusted and contribute to economic growth.

Together, we'll take action and build trust in safe and responsible AI innovation so its benefits can be realised confidently across the UK.

3. Public services that use people's data responsibly

Public services rely extensively on personal data - often the most sensitive data - to deliver essential services across areas such as health, policing, justice, welfare and local government. Although public bodies account for just 0.4% of data controllers, 29% process data for between 1,000 and 50,000 people, and 12% process data for more than 50,000.[4]

[2] Ipsos AI Monitor 2025
[3] ico-pair-2025-report.pdf
[4] Data Controller Study 2025 | ICO

Government digital transformation ambitions, including significant investment in AI, depend on strong public trust and clear accountability. Yet **fewer than half of the public trust government to keep their data safe**.[5] Without greater transparency and responsible data use, the benefits of innovation risk being overshadowed by mistrust.

Improving responsible data practices in the public sector will help people engage with public services with confidence.

By improving trust and transparency, we will:

- enable more effective digital transformation;
- support innovation in service delivery; and
- contribute to wider economic and societal benefits.

Together, we'll take action and build public trust in how their data is protected while improving essential services.

4. Building cyber resilience to keep people's data safe

Cyberattacks now represent one of the fastest-growing sources of harm to people and disruption to essential services. **The UK is the most targeted country in Europe**, with more than 600,000 organisations experiencing a breach last year and national economic losses exceeding £14.7 billion annually.[6] [7]

The effects on people are significant: 56% report being caught up in a data breach, and 71% of those say it had a direct impact - including loss of trust, stress and increased exposure to fraud.[8] Data shows that around 11% of fraud victims were targeted after their personal data was exposed in a breach.[9]

Cyber criminals are increasingly using AI to carry out attacks that are faster, more advanced and harder to detect. Complex digital supply chains create additional vulnerabilities, demonstrated by the CrowdStrike software incident which disrupted thousands of services and cost the UK economy between £1.7–£2.3 billion.

[5] Public attitudes to data and AI: Tracker survey (Wave 4) report - GOV.UK
[6] Cyber security breaches survey 2025 - GOV.UK
[7] Economic_modelling_of_sector_specific_costings_of_cyber_attacks.pdf
[8] ico-pair-2025-report.pdf
[9] Modelling_the_link_between_data_breaches_and_fraud.pdf

By strengthening cyber resilience and reducing the impact of data breaches, we will:

- protect people and help them feel more secure;
- help responsible organisations innovate confidently;
- hold negligent or irresponsible actors to account;
- help create a more secure and predictable operating environment for organisations; and
- support investment, innovation and growth across the UK economy.

Together, we'll take action and build a safer digital environment that protects people and strengthens the UK's economic and national resilience.

These four regulatory priorities provide the primary focus for our efforts and our stakeholders should expect to see a continuous focus on each.

Our work on these priorities will form part of a broader balanced programme of regulatory interventions.

Our transformation priorities

To execute this strategy effectively, we must build on our strengths. We must also continually review the culture, capacity and capabilities we need to respond to a dynamic, rapidly changing regulatory environment.

Routinely seeking to improve productivity and value for money from all our services and activities is therefore a core part of our work. The transformation programmes under this strategy focus on the areas where we need to make more fundamental changes to deliver on our purpose, our strategic outcomes and our priorities.

Streamlining customer services for people and businesses

Demand for our public services has risen sharply over the past two years, creating significant operational pressure across our customer service functions. Higher volumes, greater complexity, and more varied customer needs have affected our ability to respond as quickly and consistently as we would want, with impacts felt across the organisation.

We must transform our customer service operations to improve responsiveness, manage volumes, strengthen prioritisation, and create efficiencies that can be reinvested into our highest-impact regulatory priorities, while delivering better outcomes for the citizen.

We will ensure that our public-facing services operate within agreed service levels, and that we provide consolidated, digital-first and accessible services that are easier to navigate including more timely responses for customers.

We expect to see increased evidence of data protection complaints being resolved by the organisations who are complained about. This will increase our capacity to concentrate on the most significant harms. We will focus on the intelligence that individual customer experience gives us and intervene in broader issues with wider societal benefit. For the most systemic and highest-risk issues, we will use the full range of our regulatory tools in a consistent, risk-based manner, enabling more decisive use of enforcement where it delivers the greatest impact.

We will work to ensure significant cost reductions in public-facing services, enabling reinvestment in higher-risk regulatory priorities.

We will explore more flexible resource and complaint handling models, including those that may require legislative reform, and execute plans if they have the potential to lead to better outcomes for customers.

Becoming more data driven and digitally enabled

The use of data within our society and economy is now widespread and complex. The pace and breadth of change is increasing year on year. We must become a more agile, data-driven, technically capable regulator to keep up with this change, especially AI. This will enable us to demonstrate what responsible innovation with data and AI truly means in a modern organisation through our practical actions, not just our words.

We will significantly strengthen our use of data, technology and advanced analytics to support a more targeted, insight-led approach to regulation. This includes increasing our use of AI and automation to improve the speed, consistency and efficiency of our work, while enhancing our ability to identify emerging risks and act earlier. We will also develop better tools and services to help organisations understand and meet their obligations more easily.

At the same time, we will build the capability and infrastructure to respond effectively to increasingly complex and high-impact data use cases. As both a regulator and a user of these technologies, we will demonstrate what responsible innovation looks like in practice.

Strengthening our people capability and culture

Our new governance arrangements mean that the powers and duties currently held by a single 'Information Commissioner' will be held collectively by a new Information Commission board. Parliament has also updated the statutory duties which frame our remit as a regulator.

While these are technical changes, they call for a cultural shift in how we make our decisions and the way we regulate.

We will maximise the opportunity this governance transition creates to increase the diversity and resilience of our decision-making at the most senior level as well as to ensure we can delegate operational decision-making more easily. This will strengthen our agility, empowerment, and accountability at every level.

We will ensure a successful transition to the Information Commission with clarity of leadership roles and responsibilities aligned to this strategy. We expect to effectively absorb and respond to a more complex range of statutory duties. These duties require a more explicit awareness of factors such as innovation, competition and economic growth as part of our core regulatory remit.

We will evidence having sufficient capability and capacity to assess, and where necessary investigate, the most complex data use cases within our updated regulatory remit, and have flexible access to the talent and resources we need to deliver. This is enabled by the new ways of working our head office move will support.

Alongside this, we will build a culture that supports accountability, collaboration and continuous improvement in how we regulate and one that is demonstrated through the visible behaviours our colleagues at all levels display day-to-day.

Our progress

We will adopt a balanced approach to measuring success. This will combine system-level outcomes, including levels of public trust and confidence, with indicators that are more directly within our influence:

- the extent to which organisations are meeting their legal obligations;
- the observable improvement in data protection practices; and
- the reduction of risks and harms arising from the use of personal data.

Alongside this, we will assess our own effectiveness as a regulator, including:
- how clearly we set expectations;
- how proportionately we intervene; and
- how effectively we enable responsible innovation.

This assessment will be guided by our impact measurement frameworks.

By bringing these measures together, we will ensure we remain focused on delivering real-world impact across the system and maintaining clear accountability for the contribution we make to it.

We will track public perceptions and confidence through longitudinal research on public attitudes. We will use quantitative indicators to complement ethnographic case studies to provide deeper insight into how people experience and engage with the data economy in practice.

We will baseline and measure over time the percentage of the public who:

- are aware of data protection rights;
- trust organisations to use personal data responsibly;
- feel confident sharing personal data;
- have confidence in sharing personal data to access innovative services; and
- agree that they benefit from organisations using their personal data.

We will measure organisational confidence, capability and clarity through longitudinal surveys of organisations, alongside monitoring engagement with regulatory tools such as guidance, training and innovation services. We will support these indicators with case studies of responsible data-driven innovation.

We will baseline and measure over time the percentage of organisations that:

- feel confident using personal data (in a way that complies with data protection requirements);
- agree that data protection requirements enable them to use personal data to develop new or improved products and services;
- agree that building customer trust in how they use personal data is important for their organisation’s growth; and
- agree that their practices around responsible data use contributed to business outcomes, such as growth, customer engagement, or competitive advantage.

We will monitor transparency through trends in FOI compliance and complaints data, alongside engagement metrics for FOI guidance and practitioner resources. We will supplement these quantitative measures with feedback from FOI practitioners to assess capability, consistency and practical barriers to timely and open information provision.

We will baseline and measure over time:

- the number of authorities reporting transparency metrics;
- the percentage of agreement that public authorities are open and transparent about how they use information;
- the percentage of agreement that public authorities provide information in a timely manner;
- the percentage of public sector organisations agreeing their transparency helps build public trust; and
- the percentage of organisations that trust public services to use their organisation’s data responsibly when delivering services.

We will track the volume and type of enforcement interventions through internal monitoring. To assess deterrence and behavioural impact, this data will be complemented by qualitative case studies and in-depth research, helping to understand how enforcement activity protects people, supports fair and competitive markets, and drives improvements in organisational practice.

We will baseline and measure over time:

- the numbers and types of regulatory interventions (investigations, warnings, fines);
- the percentage of the public confident that organisations which misuse people's personal information are held to account by regulators;
- the percentage of the public who agree that the ICO's work helps protect them from harm and increases their trust in data protection regulation;
- the percentage of organisations which agree that the ICO's enforcement and guidance help protect their organisation from unfair competition and act as a deterrent for poor practice; and
- the percentage of organisations which agree that when organisations handle personal information badly, they are appropriately investigated and sanctioned.

Our performance reporting will provide transparent updates on progress against these indicators, alongside measures supporting our regulatory and transformation priorities. We will report annually on strategic outcomes, supported by quarterly updates on operational metrics and emerging trends. This will provide a clear and consistent view of how our regulatory activity is driving improvements for people, organisations and the wider economy.