ROYAL STATISTICAL SOCIETY

DATA | EVIDENCE | DECISIONS

RSS RESPONSE TO CABINET OFFICE CONSULTATION ON MAKING PUBLIC SERVICES WORK FOR YOU WITH YOUR DIGITAL IDENTITY

5 May 2026

1 Introduction

1.1.1 The Royal Statistical Society (RSS) is a membership organisation and charity that advocates for the importance of statistics and data in society. We are a learned society and professional body for statisticians and data professionals in the UK and internationally, with over 11,000 members across the UK and worldwide. We work to ensure that policy formulation and decision-making are informed by robust evidence and are undertaken in the public interest.

1.1.2 We have a long-standing interest in how government collects, links and uses data. We have consistently highlighted that limitations in data sharing and record linkage make it harder to make effective use of administrative data for analysis, evaluation and official statistics. In this context, the Society has previously encouraged government to explore wider and more consistent use of personal identification numbers across services, as a means of improving data quality, reducing duplication and enabling privacy-preserving linkage.

1.1.3 Experience during the Covid-19 pandemic reinforced the importance of data linkage. The pandemic demonstrated both the value of effective record linkage for surveillance of the spread of the virus, analysis and timely decision-making. It also highlighted the practical difficulties that arise when identifiers, permissions and governance arrangements are fragmented – making it harder to bring together data from multiple sources at pace, slowing scientists' ability to understand transmission, evaluate interventions and inform public debate. The RSS therefore views the development of a national digital ID system as directly relevant as a way to address long-standing challenges with data linkage.

1.1.4 Digital ID has the potential to affect the wider data landscape in the UK, including the effective use of wider administrative data, surveys and official statistics. Public trust, data linkage and the quality of statistics are interdependent: loss of trust risks wider harm to data provision and representativeness. Design choices made now will therefore have downstream statistical consequences that persist well beyond initial implementation. We need to ensure that we can demonstrate that improvements in data linkage and governance can generate public benefits –

both in terms of improved public understanding and in terms of better evidence-based – decision-making and hence can increase public confidence.

1.1.5 This response focuses on these cross-cutting considerations. While recognising the potential benefits of a well-designed digital ID system, we emphasise that those benefits are conditional on strong governance, transparency, clear separation between operational and statistical uses of data, and safeguards to protect trust and statistical integrity. Our aim is to support the development of a system that improves public services and public understanding while strengthening, rather than undermining, the evidence base on which public decisions depend.

1.1.6 Beyond technical design, the RSS also notes that public trust in digital identity will be influenced by how it is communicated, including the policy contexts in which it is introduced. Communication that emphasises broad public benefit, clear safeguards and voluntariness is likely to support confidence more effectively than framing that links digital identity primarily to enforcement or compliance objectives.

2 Q1.0.1 What do you think the main benefits will be, if any, for the government's new national digital ID system?

2.1.1 If implemented carefully, a national digital ID system – and the new universal unique identifier that the consultation says the government is considering – has the potential to simplify identity verification for individuals, reduce administrative burden across public services, and improve the consistency and quality of administrative data. We are particularly interested in the potential to address long-standing challenges around data linkage. More consistent use of trusted identifiers could support effective record-linkage across datasets, helping to reduce duplication, identify under-reporting and improve the quality of evidence available for operational, analytical and statistical purposes, including official statistics. Achieving this is dependent on maintaining clear distinctions between identity assurance for service delivery and the use of data for statistical analysis.

3 Q1.0.2 What do you think the main drawbacks will be, if any, for the government's new national digital ID system

3.1.1 From our perspective, the main drawback of a national digital ID and universal unique identifier system would arise if they were introduced or communicated in a way that undermines public

trust in government use of personal data. The RSS has consistently highlighted the value of data sharing and record linkage for improving evidence and public decision-making, but such benefits are contingent on public confidence. If the digital ID programme is perceived as insufficiently transparent, poorly governed, or associated with purposes that generate public concern, this could harden scepticism about data use more broadly and make it harder to make the positive case for responsible, privacy-preserving data linkage.

3.1.2 This risk is particularly important because trust is not evenly distributed across society. Any erosion of confidence is likely to be felt most strongly among groups that are already less engaged with public services or less willing to share data, with potential consequences for data quality, representativeness and the production of official statistics. Careful design, governance and communication are therefore essential to ensure that the programme strengthens, rather than weakens, the foundations for effective data use across government. This consultation is a welcome first step towards minimising this risk – but it is important that government should remain cognisant of it.

4 Q1.0. 4 The government proposes to use the digital ID system to enable more modern, efficient and personalised public services. Which public services would you want the government to prioritise making faster or more efficient using the system?

4.1.1 Priority should be given to services where identity verification currently creates delays or barriers, such as health services, social security, local authority services and education-related services. In determining priorities, government should recognise that early adopters of digital ID are likely to be demographically skewed. Care will therefore be needed in interpreting early performance improvements so that apparent gains are not driven by selection effects rather than genuine service transformation, particularly where performance data are subsequently used for statistical reporting or public accountability.

5 **Q3.2.4. For those who opt for a digital ID, government would develop a method to securely identify and match people across different public services to simplify everyday interactions between individuals and the state. For instance, such an approach could help ensure changes in an individual's information are easily and quickly reflected across services, like a name change. This would reduce the need for people to update their information separately for each service. It could also let government move away from old-fashioned and bureaucratic processes, towards proactive, hassle-free services that are available at the point of need. To what extent do you agree or disagree with the adoption of such an approach to public sector transformation?**

5.1.1 Secure identification and matching across public services could materially improve user experience and public sector effectiveness by reducing repetition and ensuring information is updated consistently. The Covid-19 pandemic demonstrated the importance of effective record-linkage for surveillance, analysis and timely decision-making, as well as the costs when permissions, identifiers or data flows are fragmented. A well-governed digital ID system could help address some of these structural limitations, supporting privacy-preserving linkage where analysis is carried out within appropriate frameworks such as accredited Trusted Research Environments, and provided public confidence is maintained.

6 **Q3.2.5. What ethical issues, if any, can you think of when designing a way to identify and match people across services?**

6.1.1 Key ethical issues include proportionality, function creep (where systems initially justified for one purpose start being used for other purposes), and ensuring that linkage does not extend beyond well-defined and justified purposes. There are also distributive considerations: groups with lower trust in government or lower digital access may experience greater perceived risk. To build trust, it is important that the government demonstrates trustworthiness – and transparency around how data is processed and who it is shared with is an important way to do this. It is welcome that the consultation document commits to this.

6.1.2 At the same time, experience during the pandemic illustrated that insufficient linkage can itself have ethical consequences, limiting the effectiveness of surveillance and delaying evidence-based responses. Ethical design should therefore consider both risks of over-reach and risks arising from fragmented or poor-quality data that weaken public decision-making.

7 Q3.2.6. What technical issues do we need to think about when designing a way to correctly identify and match people across public services?

7.1.1 Technical design considerations include accuracy of matching, management of uncertainty, prevention of duplication, and interoperability between systems. The pandemic highlighted the value of well-designed personal identifiers in reducing data entry errors and improving coverage. Equally important is clear architectural separation between identity systems used for service delivery (and specifically to inform decisions with impacts for individuals) and analytical systems that maintain and utilise statistical datasets derived through secure linkage. In both instances there will be a need for robust auditability and governance to maintain data quality and trust.

8 Q5.1.2. Principles of data minimisation and empowering users to ensure they have greater control over how much data they share when using their national digital ID at point of use will be central to the design and implementation of the digital ID system. How should the government ensure transparency around how national digital ID data is used?

8.1.1 Transparency should encompass not only what data is shared at the point of use, but how digital ID data may be used across government, the safeguards that apply to different uses, and the public value those uses support. The pandemic demonstrated that public support for data linkage was strengthened where there had been prior consultation, clear communication and use of trusted research environments. It is important that transparency clearly distinguishes between operational uses of identity and statistical or research uses of data, which are governed by different principles and protections under the Code of Practice for Statistics.

8.1.2 That foundational transparency does need to be linked to the opportunities for user control. Wider commercial examples of private data management include the opportunity for users to be selective about which permissions they grant and to change their minds and to withdraw permissions. Consideration should be given to the different ways in which such user control might be implemented.

9 Q5.4.1. What additional oversight mechanisms, if any, should be put in place for the national digital ID system?

9.1.1 Obviously, government needs to monitor the uptake and the use of Digital ID (and the demographical differences in these metrics). Critically there should also be regular, independent monitoring of levels of public trust – in the quality and representativeness of government data and in the appropriateness of government use of data -. Given the importance of these issues to public understanding and accountability, relevant outputs should be published as official statistics, in line with the Code of Practice. Such oversight can also help safeguard statistical independence by ensuring that data derived from the digital ID system are not misused or selectively interpreted to justify operational or policy decisions.

10 Q6.1.5 Do you believe there are any other wider impacts from introducing the national digital ID system that have not been considered in this consultation?

10.1.1 One wider impact not fully explored is the likely demand to compare service performance between digital ID users and non-users, particularly during early, voluntary adoption. Given that uptake is unlikely to be uniform, such comparisons risk being misleading without careful statistical treatment. This has implications for producers of Official Statistics, who may face pressure to produce analyses that are not methodologically sound or are used beyond their appropriate statistical purpose, and suggests a need for cross-government consideration of how performance data are interpreted and communicated.

10.1.2 In addition to system design, the way in which the national digital ID is communicated publicly will be important for building and maintaining trust. Public perceptions of digital identity are shaped not only by technical safeguards but by the broader narrative used to explain who the system is for and how it will be used. Experience suggests that where digital ID is primarily associated with enforcement or compliance-focused policy areas, public confidence may be harder to establish, particularly among groups that already have lower levels of trust in government data use. Clear, consistent and inclusive communication (emphasising safeguards, voluntariness, and public benefit) should therefore be treated as a core component of the system's governance, rather than as a secondary consideration.