Making public services work for you with your digital identity

Citizens Advice
consultation response

citizens advice

May 2026

Introduction

Citizens Advice provides free, confidential and independent advice to help people overcome their problems. We have a network of over 200 independent local Citizens Advice charities across England and Wales, who provide independent advice across a whole range of areas, from benefits to housing, and immigration and debt.

This document summarises our responses to the government's consultation on Digital ID : Making public services work for you with your digital identity.

We regularly help people where they are engaging with public services or trying to access support they are entitled to, and as a result have a unique insight into the challenges that people face when interacting with public services. We also provide vital support to people facing digital exclusion, including helping people to access public services as well as other essential services. We have drawn on these insights when producing our response.

Below we have summarised our overall perspectives. Read on for our full consultation response.

Overall perspectives:

- There are some people who come to us for help who may benefit from Digital ID where they do not have access to traditional forms of ID (like passports). However, we do not believe that Digital ID will meet the needs of all groups who currently struggle to prove their identity, including digitally excluded people without access to smartphones, limited internet access or low digital confidence. It will therefore be essential to retain strong non-digital options for people to prove their identity and access public services.
- We support the ambition around moving towards more hassle-free government services and can see use cases where data matching could help to smooth people's interactions with public services, reduce the need for lengthy paperwork and help people to claim support they're eligible for. But whilst there are benefits to be gained from such an approach, there are also risks. We urge the government to take a cautious approach to data matching that takes account of public attitudes.
- Digital ID should not be required for people to access services and benefits, and we worry that the transition towards Digital ID could result in the erosion of other non-digital channels. The government must take steps to preserve

alternative channels, including setting out clear expectations for third party organisations around accepting multiple forms of ID.

- Roll out and implementation must be based on trust and engagement, with an ongoing focus on public engagement particularly when considering where data matching is used to ensure that the programme has public support.
- If the government implements Digital ID, this must be supported by:
    - Emergency support to help people if they get locked out of the system, or face problems due to errors with their data.
    - Mechanisms to ensure that people can get corrections and urgent support where their data is incorrect, or where incomplete data has resulted in problems.
    - Protection of non-digital channels to ensure that people who cannot or do not want to use the Digital ID can still access key services.
    - Good systems to support proxy support, recognising that some individuals may rely on friends, family or other trusted people to access the system.
    - Strong cybersecurity systems and robust data governance processes.

Contents

Introduction 1

Contents 3

Questions on Part 1: Our Ambition 5

What do you think the main benefits will be, if any, for the government's new national digital ID system? 5

What do you think the main drawbacks will be, if any, for the government's new national digital ID system? 5

One of the government's aims for the new national digital ID system is to make it easier for people to prove who they are. To what extent do you agree or disagree that the proposed system could help achieve this aim, and why? 6

Questions about Chapter 3.2: Transforming public services 8

Are there examples of any barriers or inefficiencies that prevent you (or people you support) from interacting with public services that you think the digital ID system could help with? 8

Have you ever faced issues with knowing which public services are available to you based on your circumstances or, if you support other people, have you faced similar issues when supporting them? 9

Have you ever been unable to or had difficulty accessing a public service because you were unable to prove your identity or, if you support other people, have you faced similar issues when supporting them? 10

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? 11

What ethical issues, if any, can you think of when designing a way to identify and match people across services? 12

Questions on Part 4: Inclusive 14

Questions about Chapter 4.2: Unlocking access across society 14

We are committing to an inclusion programme to ensure everyone eligible in the UK can access the digital ID. Some people may face barriers to creating or using the national digital ID. This may be due to difficulty accessing traditional proofs of identity (like passports) or due to a lack of digital access, skills or confidence. Are you aware of any other barriers not captured in the consultation? 14

Which other barriers are you aware of and why? 14

The government is committed to making sure the national digital ID system stays true to the approach outlined in the Digital Inclusion Action Plan. This includes providing local level support, increasing access to the internet and helping people develop digital skills. Is there any particular support not captured in the consultation or the Digital Inclusion Action Plan that would help you or other people to use the national digital ID? 15

Which other forms of support would be helpful and why? 15

Chapter 4.2 of the consultation includes a non-exhaustive list of those people who may benefit the most from additional support measures to ensure they are able to access the national digital ID. Are there any groups not included in the list that you believe could also be at risk of ID or digital exclusion? 16

Questions about Chapter 4.3: Commitment to supporting inclusion 18

We are considering dedicated accessible support for those who are digitally excluded, delivered locally, in-person and by trusted organisations. Are there any other ways you think the government should consider supporting those who are digitally excluded? 18

Please explain what you support measures should be considered. 18

Questions about Chapter 4.4: Accessibility 20

The government intends to engage with a range of people and organisations outside of government to help ensure the design and delivery of the national digital ID system is accessible. Can you suggest any specific organisations or types of organisations which the government should engage with? 20

Questions about Chapter 4.5: Alternative access routes 21

We are exploring alternative ways to access the national digital ID for those who cannot use a device. What do you think are the most important barriers for government to address when designing alternative access routes for the national digital ID? 21

Questions on Part 5: Trusted 24

Questions about Chapter 5.4: Ensuring strong oversight and governance 24

What measures can you suggest, if any, that could be put in place to make sure people can resolve issues with their national digital ID? 24

Questions on Part 1: Our Ambition

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

At Citizens Advice, we agree that Digital ID could help the government to deliver improved modern public services and reduce unnecessary data security risks, by reducing the amount of personal data people have to hand over to organisations.

We also expect there will be a cohort of people who don't have access to other forms of ID (like a passport, or driver's license) but who do have access to a smartphone who may benefit from being able to access an alternative form of ID.

However, we do not believe that Digital ID will meet the needs of all groups who currently struggle to prove their identity, including digitally excluded people without access to smartphones, limited internet access or low digital confidence. It will therefore be essential to retain strong non-digital options for people to prove their identity and access public services.

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

- **Risk of exclusion from new Right to Work Checks:** Removing the option to use paper forms of ID for Right to Work checks carries a significant risk of excluding people from the labour market who may struggle to access Digital ID. While the government intends this approach to reduce illegal working, it's important to consider the risk of people with the right to work in the UK, but without access to Digital ID, or a biometric passport or eVisa, being unfairly excluded from accessing a job. It is also likely that unscrupulous employers or criminals will continue to bypass a new Right to Work scheme, if it is not accompanied by more proactive labour market enforcement to provide an effective deterrent to breaking the rules.
- **Risk of lock outs or loss of access unless support is in place:** People could lose access to their Digital ID if their phone is lost, damaged or stolen, or due to possible outages with the underlying services. It's important there is support in place to help people access services promptly if this happens, including retaining alternative access points for public services.

- **Device costs:** Whilst the government intends that the ID will not have up-front charges, device costs could be a substantial barrier to access. The Digital ID will likely require a secure operating system to be in place, which means only newer phones will support it. This will likely require people to regularly update their device to retain access, which creates an affordability barrier. At Citizens Advice, we regularly see people who are unable to access government Apps because they are using old devices.
- **Risk of fraud or unauthorised access:** Fraud challenges are growing more complex with AI technology such as deepfakes and voice cloning growing more realistic. There will need to be robust processes in place to authenticate users, including where people are seeking access after getting locked out of the system (e.g. after changing device), and these may need to be in-person.
- **Risk of data errors or incorrect matching:** The government has set out that it plans to put an approach in place to match and identify people across government services. Whilst this could provide benefits, it also brings risks where incorrect or incomplete data is included in matching. As a result there will need to be support in place to ensure people can correct their data or appeal decisions that they think have been based on incorrect or incomplete information. We also encourage the government to consider the role of trust and data sovereignty in any data sharing practices. Trust is of paramount importance to encourage adoption.

One of the government's aims for the new national digital ID system is to make it easier for people to prove who they are. To what extent do you agree or disagree that the proposed system could help achieve this aim, and why?

Neither agree nor disagree.

At Citizens Advice, we see there are some circumstances where the Digital ID may make it easier for people to prove who they are. For example where someone does not have a traditional photo ID, like a passport or drivers license, but does own a smartphone.

However, while some of the people we help who don't have traditional forms of ID do possess a smartphone, many of them do not. Where cost is a prohibitive factor that has prevented someone from obtaining a traditional photo ID (like a passport) this is unlikely to be mitigated by Digital ID, as smart phones can be expensive and may need to be regularly replaced to meet the operating and security standards required of a Digital ID.

Many of the people we help who face issues proving who they are also face other barriers that are unlikely to be addressed by Digital ID. For example, many of the people we help face digital exclusion, including issues accessing the internet, or low digital confidence. As a result these groups may be unlikely to interact with Digital ID.

Questions about Chapter 3.2: Transforming public services

Are there examples of any barriers or inefficiencies that prevent you (or people you support) from interacting with public services that you think the digital ID system could help with?

Yes.

At Citizens Advice, we see a range of barriers that can make it difficult for people to access public services or support. We surveyed 175 Citizens Advice advisers to find out what the main barriers are for the people who come to Citizens Advice for help when it comes to accessing public services. The most common barriers identified were:

- People do not know what public services or support is available to them or whether they are eligible (reported by 87% of advisers)
- The application form requirements are confusing or hard to understand (82%)
- People don't have access to reliable internet or struggle with online application processes (82%)
- People find it difficult to access help to complete their application (e.g. long phone waits or lack of face-to-face support) (75%)
- People find it difficult to get the right evidence (e.g. medical evidence) (55%)
- People need translation support (41%)
- People find it difficult to prove their identity (e.g. they don't have a passport or drivers license (40%)
- People find it difficult to prove they are eligible (e.g. don't have access to letters or documents to prove they are eligible) (31%)
- People feel uncomfortable claiming support (26%)
- People are concerned about privacy, or who their information may be shared with (14%).

As evidenced by the above, ID access is one of the common barriers that can make it difficult for people to access public services, but this barrier is much less common than other issues like application forms requirements that are confusing or hard to understand, and lack of reliable internet access.

Some of these barriers may be reduced through the Digital ID rollout where it includes data matching. For example this could reduce the need for lengthy applications where

information is already held by the government. But Digital ID will not be able to address some of the other barriers - or may exacerbate them - for example where people don't have access to the internet or struggle with online processes.

On identification, 28% of advisers said that clients "often" or "very often" face issues applying for services or support due to issues proving who they are (e.g. they do not have a passport or drivers license).

But perspectives were split on the extent to which they felt Digital ID would make it easier for clients to prove their identity when accessing public services and support. Whilst 34% of advisers thought Digital ID would make it easier for people to prove their identity, 21% felt it would make no difference, 24% felt it would make it harder and 21% said they were not sure.

Some advisers reported that many of their clients had access to a smartphone, so they felt the Digital ID could provide a useful alternative to them where cost (or other barriers) have prevented them from accessing other forms of photo ID. They felt Digital ID could be useful in these cases, where it may help people to access banking or public services where they currently struggle to prove their ID due to a lack of photo identification.

But more frequently advisers raised concerns about how Digital ID would work for other groups of people who are highly represented among the people we help at Citizens Advice. This includes:

- People who don't have access to smart phones or who don't have access to the internet, including where this is due to cost barriers.
- People with low digital confidence, with some advisers reporting that many of the people they support struggle already with accessing services like email or using apps, and as a result have high reliance on advisers supporting them to complete applications.
- People with limited internet access or in areas with poor phone connectivity who may struggle to access verification codes.

Have you ever faced issues with knowing which public services are available to you based on your circumstances or, if you support other people, have you faced similar issues when supporting them?

Yes.

As a frontline organisation, Citizens Advice regularly sees examples of situations where people struggle to identify what public services are available to them. In a survey of Citizens Advice advisers, 87% of advisers said that not knowing what support is available

to them or whether they are eligible is a main barrier clients face when it comes to accessing public services and support. This was the most commonly reported barrier to accessing public services, closely followed by application form requirements being confusing or hard to understand, and not having access to the internet or struggling with online application processes.

Many of the people we advise need help navigating welfare support - this both includes understanding what support they may be eligible for, as well as how to access this support. In some cases people are not aware of the support that is available, but we also help people who know about support but where there are misunderstandings around whether support is automatically put in place or whether it requires a separate application.

For example, as identified in our response to the Ministry of Housing, Communities and Local Government's consultation on council tax, we regularly see examples where people in receipt of Universal Credit mistakenly believe that they do not need to apply for council tax support as they assume it will be automatically attached to their Universal Credit claim.

Have you ever been unable to or had difficulty accessing a public service because you were unable to prove your identity or, if you support other people, have you faced similar issues when supporting them?

Yes.

Citizens Advice has experience supporting people who have faced difficulty accessing welfare support and banking services because of difficulties proving their identity. Most commonly this is where people do not have access to traditional photo ID, like a passport or drivers license.

As set out in our previous response, 28% of advisers said that clients "often" or "very often" face issues applying for services or support due to issues proving who they are. But perspectives were split on the extent to which advisers felt that Digital ID would make it easier for clients to prove their identity when accessing public services and support. Just 34% of advisers said Digital ID would make it easier for people to prove their identity, whilst 21% felt it would make no difference, 24% felt it would make it harder and 21% said they were not sure.

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?

Somewhat agree.

We support the principle of moving towards more proactive and hassle-free services.

Data matching could help to target support more effectively to individuals, reducing the level of support going unclaimed. This could help to maximise people's incomes and enable them to better weather cost of living pressures. For example, Turn2Us estimate that £9.6 billion goes unclaimed in Universal Credit, whilst 185,000 unpaid carers could be missing out on Carer's Allowance. Appropriate use of data matching could also reduce bureaucracy and simplify application processes by reducing the level of information people are expected to share to prove their eligibility for services, where this information is already held by the government.

Where appropriate data matching could also help to ensure that people who are eligible for passported benefits get access to these. For example we regularly see issues where people who are eligible for Council Tax Support are not receiving this - either because they are not aware of the support or because they do not know that they need to apply separately. Data matching could potentially help to automate this support.

However, approaches to data matching need to be treated with caution and sensitivity. This should take account of public attitudes, as whilst there are some areas where people are likely to support the use of data matching, there will be others where there is very low public support.

We anticipate that people are more likely to support data matching where it is used to make it easier for people to access support, or smooths burdensome administrative processes (e.g. updating services after a name change). However people are likely to be less supportive of data matching where they fear it is or may be used to monitor or surveil them, or where it could result in support being withdrawn. Recent high profile cases where incomplete data matching has resulted in support being wrongly withdrawn - such as Child Benefit payments being stopped due to incomplete travel

data included in HMRC analysis - are likely to make people particularly nervous around where data matching could impact their entitlements or lead to them being wrongly accused of fraud.

There is also a risk that data matching errors could result in people receiving more support than they're entitled to, or to which they are not entitled at all. People should not have to repay overpayments caused by data matching errors. We already see issues around this in relation to Universal Credit payments, where people can face serious hardship when asked to repay overpayments that have resulted from government errors.

High profile examples like those related to Child Benefit payments, or overpayments of Carers Allowance, where data matching has resulted in poor outcomes for people, are likely to undermine trust in data matching, and could consequently result in people choosing not to engage with Digital ID.

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

At Citizens Advice, we see a number of ethical issues that government will need to consider when considering use of data matching across services:

- **Public attitudes and consent** - as set out in our previous answer, there will be areas where people are supportive of the use of data matching - for example where it makes it easier to access support. But there will also be areas where people do not support data matching, or have concerns about data being used for surveillance. When devising its approach to data matching we urge the government to take account of public attitudes, and not to implement use cases that would be unsupported by the public. This is also important to the success of the programme, as a lack of public trust will undermine adoption of Digital ID.
- **Sensitive data** - there are some categories of data where people are likely to be particularly concerned about data sharing, and where disclosure should only take place under a consent process and only for limited purposes. This includes special category data like health information.
- **Third party data sharing** - Data matching should not include matching people to third party services. Where information needs to be shared for a legitimate purpose (e.g. a childcare provider needing to check someone's eligibility), this should be done in ways that minimises any data sharing with third party

organisations (for example using a system to provide confirmation of eligibility, rather than sharing data).

- **Error risk** - this could include where individuals are incorrectly matched to data that belongs to someone else, or where incomplete or incorrect data results in errors. For example in the recent case where HMRC data was matched with international travel data to identify people who were claiming child benefit whilst living overseas, HMRC incorrectly identified some individuals as living overseas due to gaps in international data and poor assumptions built into the model. Errors could have substantial impacts on individuals. At the sharp end this could result in support being withdrawn/denied, individuals wrongly being marked as deceased, individuals being asked to repay overpaid support, or individuals wrongly being flagged as committing fraud. The designed approach must have robust processes in place to prevent these kinds of issues. It is also vital that there are mechanisms in place to enable people to inform the government of errors, request corrections to their data and appeal decisions.

Questions on Part 4: Inclusive

Questions about Chapter 4.2: Unlocking access across society

We are committing to an inclusion programme to ensure everyone eligible in the UK can access the digital ID. Some people may face barriers to creating or using the national digital ID. This may be due to difficulty accessing traditional proofs of identity (like passports) or due to a lack of digital access, skills or confidence. Are you aware of any other barriers not captured in the consultation?

Yes.

Which other barriers are you aware of and why?

At Citizens Advice, we agree with barriers set out above. Another key barrier to adoption will be trust. People lose trust in digital products and the organisations rolling them out for multiple reasons:

- **Being forced to adopt a digital service reduces trust:** Many digitally excluded people feel angry at being forced to adopt a digital service. They want to walk into their local bank branch, or job centre, or council building as they have done their whole lives. Having these options removed, especially when they may be excluded for affordability or confidence reasons, can damage relationships with services. We recommend a long tail of support for non-digital channels, so that policies can be adopted slowly through behaviour change and motivated by convenience and benefits, not loss of support.
- **Experiences of fraud reduce trust with the digital world:** Many people will have experienced fraud, identity theft or data breaches, which may have come with substantial financial or emotional impacts. After experiencing such events people may be more nervous about interacting with digital interactions - this is something we see when supporting some clients. The success of this scheme needs to understand that trust is built slowly and lost quickly, and that many people are coming from a baseline of low trust with the digital world. Ongoing community support will be vital to support adoption.
- **Poor practice in data sharing reduces trust:** From the public debate around Digital ID it is clear that some individuals are concerned about how their data will

be shared and which organisations will have access to it. It will therefore be important that the programme puts in place strong and transparent governance approaches to ensure people can feel confident about how their data will be used. This also extends to partner organisations - they must have impeccable reputations around data governance to maintain public trust.

- **Negative past experiences with digitised public services reduces trust**: Although policymakers may perceive a strong difference between a digital service run by HMRC and one run by the local police (being drastically different organisations), members of the public may not perceive this difference in the same way. Where an authority pushes them to use a digital service, and they have a negative experience, their overall trust can be eroded with digital public services as a whole. This is why the success of GDS, GDS local, Customer First and other digital initiatives are all tied to the successful adoption of Digital ID.

To address these barriers, we recommend:

- Ongoing protection of non-digital channels
- Ongoing community support to support adoption.
- Partnerships with organisations with an impeccable reputation around data governance to maintain trust with the public.
- Transparent, easy to understand data and governance frameworks.
- An understanding that the success of GDS and digitalised public services as a whole will impact the success of this work.

The government is committed to making sure the national digital ID system stays true to the approach outlined in the Digital Inclusion Action Plan. This includes providing local level support, increasing access to the internet and helping people develop digital skills. Is there any particular support not captured in the consultation or the Digital Inclusion Action Plan that would help you or other people to use the national digital ID?

Yes.

Which other forms of support would be helpful and why?

At Citizens Advice, we believe the following will be vital to ensure the success of the Digital ID scheme:

1. **Swift recovery support.** When phones get stolen or system errors happen, people get locked out of essential services. At Citizens Advice, we see the

detriment to people's lives when being locked out of a digital service means they can't access their visa status, funds or housing. Swift recovery support will be an essential part of service design to maintain trust and adoption.

2. **Ongoing human, in-person support.** Due to the sophistication of deepfakes and voice cloning, we question how easy it will be to support issues remotely. We urge the design team to explore how people will prove who they are when a data matching issue or system error occurs. It may be that human, in-person support is the only viable option.
3. **Proxy support within design.** The Digital ID scheme will need to enable proxy support from family, friends and carers. Currently safety protocols rarely allow for this, but at Citizens Advice we see daily the number of people who must share passwords or sensitive information with friends, family and support workers to access basic support. Some people, even with digital training, will never be able to access digital services, for example in cases of advanced dementia, some schizophrenia or learning disabilities.
4. **A clear communications plan which offers tangible benefits to users.** This should steer clear of sensitive, politicised topics and focus on actual pain points for users. Adopters need a reason to make this change.
5. **Transparent, easy to understand data and governance frameworks.** There must be clarity on data sharing, data sovereignty and governance. The public needs to understand where their data is going to be able to trust the scheme.
6. **Strong cybersecurity.** Data breaches may weaken the trust that the public have in the scheme. It is therefore important that there are strong cybersecurity processes in place to reduce the risk of data breaches and unauthorised access.

Chapter 4.2 of the consultation includes a non-exhaustive list of those people who may benefit the most from additional support measures to ensure they are able to access the national digital ID. Are there any groups not included in the list that you believe could also be at risk of ID or digital exclusion?

Please specify which other groups may be excluded and describe how they might be impacted. Please do this for each group you identify.

At Citizens Advice, we consider the list of excluded groups in the consultation to be fairly comprehensive. This list also helps to define who will benefit from targeted support. We would add some key points to this:

1) **Digital inclusion is not a fixed state.** Anyone in the UK can become suddenly digitally excluded: their phone is stolen; they lose their income; technology takes a leap forward, and so on. Any digital ID scheme needs to build routes to support and recovery of ID information/access into the foundation of its design. People will suddenly and unexpectedly lose access to their digital ID; this is inescapable. Therefore this scheme must build in provisions for this expected outcome.
2) **The people listed in the excluded groups of this consultation may be more likely to move between inclusion and exclusion.** For example, when someone on high income has their phone stolen, they can quickly buy a new one. For someone facing poverty, they may not be able to afford to replace the device, and will be locked out of ID and potentially essential services for longer. Therefore, provision to support urgent recovery of ID information/access must be tailored towards these groups.
3) **Non-digital recovery support must be swift.** If digital ID becomes a foundational access point to essential services, it is high risk to lose access. Lack of access, even for a short time, could lock people out of urgent access to essential services. We see this already in banking and eVisas; people come to Citizens Advice in great distress because they are locked out of an account, can't get hold of customer support and can't access funds or prove their visa status. They are often issued deadlines by other services (eg. proving visa status for employment or benefits) which they then can't meet, with knock on detrimental impacts. Therefore, the digital ID scheme design must offer swift non-digital recovery support**.** It must also make provisions for instances of prolonged temporary exclusion, such as when a phone is confiscated by the police.
4) **One phone does not necessarily equal one person.** Amongst low income groups, device sharing is common due to affordability challenges. The design of this scheme must recognise that 2 or more people may want to prove their ID from the same device.
5) **Identification control can be a form of abuse.** Combining the method of communication (a phone) with a method of identification (Digital ID) could increase risks to people in exploitative situations, such as modern day slavery or domestic abuse. The scheme design must consider that some people may have a second, hidden phone, and if an abuser can somehow discover this fact from the Digital ID app itself, this could increase risk to individuals in exploitative situations.

In summary, we recommend the Digital ID scheme design:

- must offer swift non-digital recovery support.
- make provisions for instances of prolonged temporary exclusion, such as when a phone is confiscated by the police (this can last months).

Questions about Chapter 4.3: Commitment to supporting inclusion

We are considering dedicated accessible support for those who are digitally excluded, delivered locally, in-person and by trusted organisations. Are there any other ways you think the government should consider supporting those who are digitally excluded?

Yes.

Please explain what you support measures should be considered.

At Citizens Advice, we have identified the following key points to think about inclusion:

1) **Digital inclusion is not a fixed state;** people will inevitably lose access to their Digital ID, through a lost phone or technological error. Because ID can become a gateway to essential services, swift recovery support will be vital to support people's urgent access to services.
2) **Proving who you are may need to be done by a human, in person.** Deepfakes and voice cloning have reached levels of sophistication which means resolving queries digitally will be limited.
3) **People in distress need human support**. When being locked out of a digital channel means you cannot access funds, secure a place in nursery or prove your identity to the police, the stakes are high. In these moments, many people do not want to speak to a chatbot or automated call response - they desperately need to talk to a person who can understand their need and help them resolve it. At Citizens Advice, we see the distress of being locked out of digital services every day.

4) **People with certain health conditions and disabilities may always need human support**. For some, digital support is simply not an available channel, given the limits of current technology. We regularly see people in Citizens Advice services who are registered blind and unable to complete multi-factor authentication methods or people with health conditions like advanced dementia, who are unable to use digital interfaces.
5) **Proxy support will need to be built into scheme design.** Human and/or in-person support may be the best way to overcome the challenges of proxy support.
6) **Support must be long term, not just transitionary.** There is no golden age where the whole UK population will be digitally included: people will move in and out of inclusion as devices break; technology will continue to advance; financial situations change; mental health needs change. There will always be a need for recovery support when a phone is lost or technical support is needed.

Due to the sophistication of deepfakes and voice cloning, we question how easy it will be to support issues remotely. We urge the design team to explore how people will prove who they are when a data matching issue or system error occurs. It may be that human, in-person support is the only viable option.

UK Government must protect non-digital routes to identification. In existing public services, we see a slow erosion of non-digital channels. As services have become digitalised, the non-digital channels either disappear or become so high friction, it is almost impossible to use them. At Citizens Advice we see people every day locked out of digital services.

Our latest research on digital inclusion (publication forthcoming) shows that essential services (such as Universal Credit, housing, council tax, banking, telecoms) sometimes offer non-digital routes which are almost impossible to use.

Organisations show a phone number as an alternate route to digital support, but people often report excessively long wait times. When they do speak to a person, they are sometimes told erroneously that the only way to make an application or access information is online. Sometimes they meet an automated voice response that they cannot get to understand them, or are signposted to another website or phone number. In one case of applying for a replacement birth certificate, a citizen was told there was no way to do this non-digitally.

People get stuck in loops over and over and find themselves unable to talk to a human or get the information they need. If this happens in the Digital ID scheme, friction will be

high and trust will be eroded. Nordic ID schemes have demonstrated that community engagement is highly important to successful adoption.[1]

For the Digital ID scheme to be successful, protections must be put in place to protect non-digital routes. Successful technological transitions include a mix of policy and behavioural decisions which help support and incentivise changes, often with a long tail of support for the original method. TFL stopped accepting cash payments in 2014 on London buses, but Oyster cards were introduced in 2003, using incentives and a long tail of behaviour change so that citizens did not feel forced. Similarly, the adoption of Chip and Pin payments in the early 2000s had a long tail where signatures were still accepted.[2]

We recommend the Digital ID scheme has a similar long tail of support for non-digital ID. We recommend exploring guidance, regulation or statutory responsibility for non digital IDs to remain accepted. Many people will be unable to reap the benefits of Digital ID, and once it is adopted, it is likely we will see a quiet erosion of paper ID acceptance. Government has an obligation to those who cannot access Digital ID to ensure they are not locked out of essential services. Encouragement alone will not achieve this.

To protect trust with the public, the government must offer transparent governance frameworks. Alongside clear communications supporting motivation and behaviour change, there must be clear, simple communication on what is happening to the public's data, who owns it and who it is shared with.

Questions about Chapter 4.4: Accessibility

The government intends to engage with a range of people and organisations outside of government to help ensure the design and delivery of the national digital ID system is accessible. Can you suggest any specific organisations or types of organisations which the government should engage with?

We recommend working with community-based organisations focused on digital inclusion, such as ourselves (Citizens Advice), Age UK, and Good Things Foundation. We think it's paramount for the design team to work to high accessibility standards, not just

[1] Digital identity for all?, Nordregio, June 2025
[2] Examples from The Connection Project Report 'Misconnected: How the UK can choose a better digital future', March 2026.

in terms of the user interface, but the situations people find themselves in, such as lacking confidence, fearing scams or sharing devices due to affordability issues.

Questions about Chapter 4.5: Alternative access routes

We are exploring alternative ways to access the national digital ID for those who cannot use a device. What do you think are the most important barriers for government to address when designing alternative access routes for the national digital ID?

At Citizens Advice, we urge the design team to consider:
1) the urgency of need for alternative access routes
2) the role of proxy support in alternative channels
3) government must protect non-digital channels for ID, alongside alternative channels.

1) The design of alternative routes must focus on the urgency of support when things go wrong. When people are locked out of essential services, they can find themselves unable to access funds or essential services. Therefore, being locked out can result in high detriment. We see this regularly with eVisas, benefits and housing; people locked out through poor non-digital channels and unable to resolve their query, with a ticking clock of a deadline they must meet. Therefore, one of the key elements of non-digital routes is that citizens must be able to access them swiftly.

We're also aware that in some countries that have already adopted Digital ID, a lack of emergency support has been a key challenge with people's experiences of the service. For example, in one country citizens complain that their Digital ID platform does not have good emergency support in place, with access points that are faulty or hard to use, and long waiting lists to access support. This can leave people cut off from services whilst they seek resolution.

Any alternative channel must therefore be swift to resolve, and must have emergency recovery support built in. Due to the sophistication of deepfakes and voice cloning, we question how easy it will be to support issues remotely. In considering alternative channels, we urge the design team to explore how people will prove who they are when a data matching issue or system error occurs. It may be that human, in-person support is the only viable option.

2) Proxy support must be built into alternative channel design. Many people facing digital exclusion rely on proxy support from family, friends and carers. Currently, safety protocols rarely allow for this, but at Citizens Advice we see daily the number of people who must share passwords or sensitive information with friends, family and support workers to access basic support. Some people, even with digital training, will never be able to access digital services, for example in cases of advanced dementia, some schizophrenia or learning disabilities.

3) The UK Government must protect non-digital routes to identification. In existing public services, we see a slow erosion of non-digital channels. As services have become digitalised, the non-digital channels either disappear or become so high friction, it is almost impossible to use them. Although alternative channels are important, we maintain that non-digital channels must be protected.

Our latest research on digital inclusion (publication forthcoming) shows that essential services (such as Universal Credit, housing, council tax, banking, telecoms) sometimes offer non-digital routes which are almost impossible to use.

Organisations show a phone number as an alternate route to digital support, but citizens often report excessively long wait times. When they do speak to a human, they are sometimes told erroneously that the only way to make an application or access information is online. Sometimes they meet an automated voice response that they cannot get to understand them, or are signposted to another website or phone number. In one case of applying for a replacement birth certificate, a citizen was told there was no way to do this non-digitally.

People get stuck in loops over and over and find themselves unable to talk to a human or get the information they need. If this happens in the Digital ID scheme, friction will be high, trust will be eroded, and the scheme will fail. Nordic ID schemes have demonstrated that community engagement is highly important to successful adoption.[3]

For the Digital ID scheme to be successful, protections must be in put in place to protect non-digital routes. Successful technological transitions include a mix of policy and behavioural decisions which help support and incentivise changes, often with a long tail of support for the original method. TFL stopped accepting cash payments in 2014 on London buses, but Oyster cards were introduced in 2003, using incentives and a long tail of behaviour change so that citizens did not feel forced. Similarly, the adoption of Chip and Pin payments in the early 2000s had a long tail where signatures were still accepted.[4]

---

[3] Digital identity for all?, Nordregio, June 2025

[4]Examples from The Connection Project Report 'Misconnected: How the UK can choose a better digital future', March 2026.

We recommend the Digital ID scheme has a similar long tail of support for non-digital ID. We recommend exploring guidance, regulation or statutory responsibility for non digital IDs to remain accepted. Many people will be unable to reap the benefits of Digital ID, and once it is adopted, it is likely we will see a quiet erosion of paper ID acceptance. Government has an obligation to those who cannot access Digital ID to ensure they are not locked out of essential services. Encouragement alone will not achieve this.

Questions on Part 5: Trusted

Questions about Chapter 5.4: Ensuring strong oversight and governance

What measures can you suggest, if any, that could be put in place to make sure people can resolve issues with their national digital ID?

At Citizens Advice, we suggest the following measures to ensure people can resolve issues with their Digital ID:

Swift access to emergency recovery support when people cannot access their digital ID. Phones break, financial circumstances change, errors happen; people will need swift support when things go wrong.

We see the impact of being locked out of public services regularly, people locked out of digital systems for eVisas, benefits and housing and unable to resolve their query, with a ticking clock of a deadline they must meet. The detriment of being locked out could have a strong negative impact on people's lives; we see people unable to access funds, secure jobs or get their child into nursery, purely because they are locked out of digital systems and unable to resolve a query. The UK Government should also learn from some of the challenges seen with existing Digital ID systems where there is limited emergency support, for example in some countries users of Digital ID systems complain that a lack of emergency contingency means they are "cut off" from services whilst they wait for support.

Therefore, emergency recovery support must be swift, effective and designed around digitally excluded people. This must be built in from day 1; if resistant adopters hear friends and family are locked out, their trust and interest in adopting will decline.

Support to recover identification must be designed around increasingly sophisticated fraudulent systems. Deepfakes and voice cloning are rapidly evolving; we suggest in person support will be necessary around the county to help verify identities.

We recommend introducing a process for complaints and support with a 4 week resolution window. Although elements of concern could be covered by the ICO, under current redress pathways, it won't always be clear which route citizens should take. To build and maintain trust, citizens will need a clear route to complaints and redress with a swift resolution.

We also recommend exploring regulatory and legislative ways to protect people's rights to use non-digital ID. In other public services, we have seen a quiet erosion of non-digital channels, whereby the friction is so high they become almost impossible to use. This includes long waits on the phone followed by a support team who signpost citizens to complete the task online. We are concerned that Digital ID will follow this precedent; and that third parties will stop accepting non-digital ID. We recommend finding ways to protect citizens' right to use non-digital ID, so that people who cannot use it are not excluded from participation in society.

Citizens Advice helps people find a way forward.

We provide free, confidential and independent advice to help people overcome their problems. We are a voice for our clients and consumers on the issues that matter to them.

We value diversity, champion equality, and challenge discrimination and harassment.

We're here for everyone.

citizensadvice.org.uk

Published [insert month and year].

Citizens Advice is an operating name of The National Association of Citizens Advice Bureaux.

Registered charity number 279057.