



DATA SHARING DURING CORONAVIRUS

The Clinically Extremely Vulnerable People Service

Summary of a private roundtable

Gavin Freeguard and Paul Shepley

Introduction

This short paper summarises a roundtable discussion held in summer 2022 about the Clinically Extremely Vulnerable People Service (CEVPS). This was a new public service that the UK government launched at the beginning of the pandemic in March 2020 to identify, notify and support vulnerable individuals who had to 'shield' to protect themselves. It brought together public servants from several government departments and others involved in the service, including the Information Commissioner's Office (ICO), local government and supermarket chains. The roundtable was held under the Chatham House Rule – nothing anyone said is attributed to them or their organisation, unless they have asked for it to be. The discussion does not represent the views of the Institute for Government.

The roundtable forms part of a wider piece of Institute for Government research looking at government data sharing during the pandemic. The project takes six case studies and uses a roundtable on each to explore what worked well, what could have worked better and what lessons government should learn for future data sharing. Reports on each of the roundtables will follow through winter 2022-23 and we will publish a short report drawing together key themes and recommendations in February 2023.

Overview of the CEVPS

The government started developing the new public service to protect clinically vulnerable people on 9 March 2020, due to concerns about how the pandemic would affect them and the likely need for shielding. By 20 March, NHS Digital had produced the first iteration of a list of clinically extremely vulnerable people (the initial Shielded Patient List) from NHS data. On 23 March, as the UK went into a national lockdown, a full public-facing service for clinically extremely vulnerable people went live, including a website, a telephone helpline service and the infrastructure to collect, store and share data about who shielding individuals were and how they might be supported.

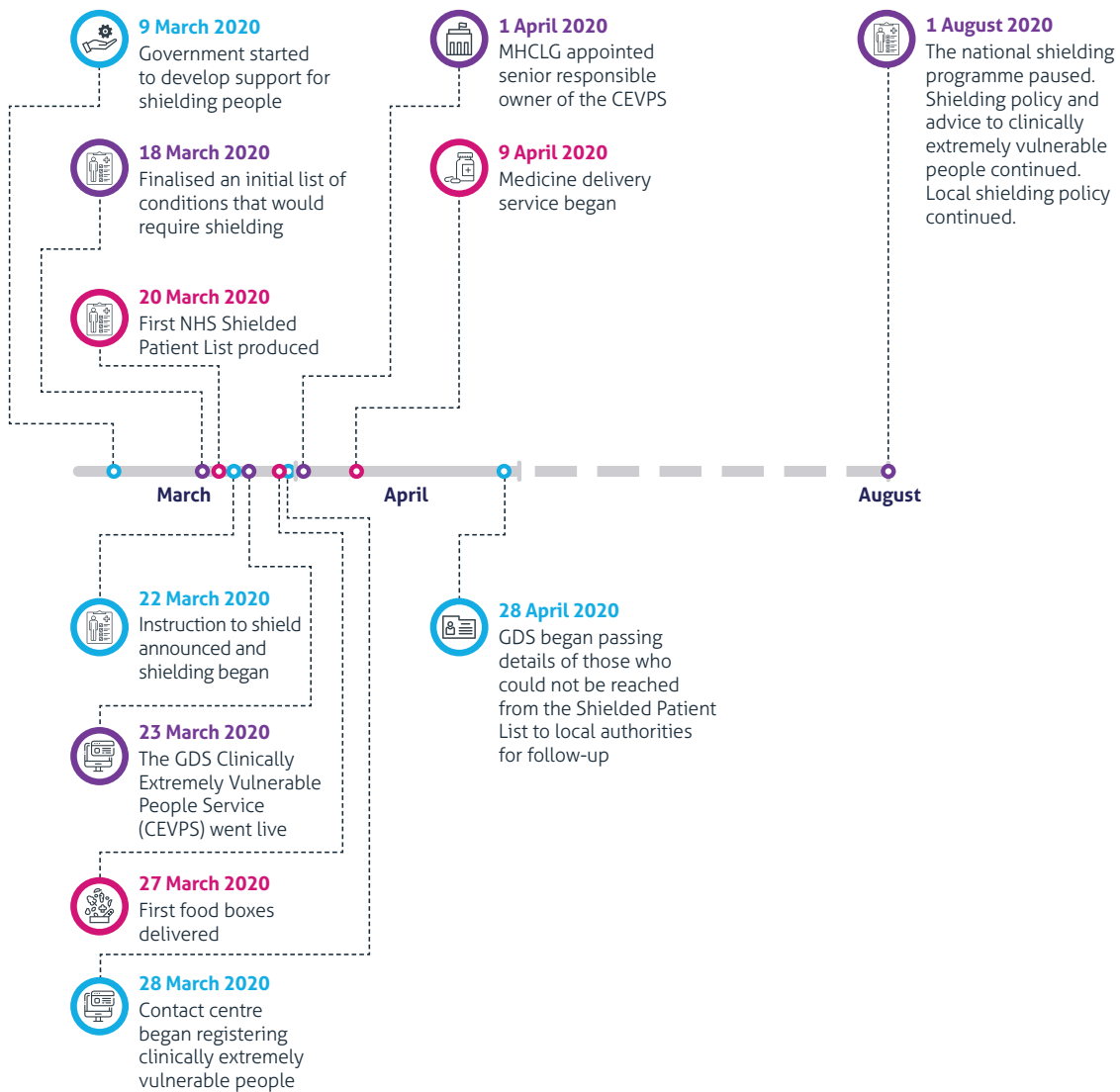
The NHS advised those instructed to shield to stay at home until further notice to minimise their chance of catching Covid, and they would therefore need support to get food, medicines and care. The CEVPS was designed to provide support to the shielding population through the provision of food parcels, preferential access to supermarket home delivery slots, medicines and medicine deliveries, and access to care. The service required a collaboration between NHS Digital, which created the initial Shielded Patient List, the Department for Environment, Food and Rural Affairs (Defra), which was initially tasked to lead the service due to its existing links with food companies, the Government Digital Service (GDS), the Ministry of Housing, Communities and Local Government (MHCLG, now the Department for Levelling Up, Housing and Communities), the Department of Health and Social Care, NHS England and NHS Improvement, GP surgeries, local government, wholesale food suppliers, supermarkets, and medicine and care providers.

The Shielded Patient List was created from national data that NHS Digital collected from across the NHS, taking data from Hospital Episode Statistics, general practice patient data, the Maternity Services Data Set and data on medicines prescribed in primary care. It was then adapted and maintained with further additions and removals using manually input clinical judgments from NHS trusts, foundation trusts and general practitioners (GPs).¹ NHS Digital managed and produced the Shielded Patient List as the data controller. The list was a live list that was updated as the clinically extremely vulnerable criteria were updated, which enabled GPs and NHS trusts to add patients they considered to be clinically extremely vulnerable or remove them from the list as appropriate. The NHS used the list to contact patients to provide advice and guidance on shielding policy. The list was regularly shared with GDS, as the data controller for a separate CEVPS List.

The CEVPS List was a list of people who contacted the CEVPS for support. GDS developed a registration service and matching capability to identify individuals who wanted help, working with MHCLG to provide local authorities with relevant information about individuals who wanted support in their areas. As well as local authorities, relevant data from the CEVPS List was also provided to supermarkets and food, medicine and care providers so that support could be provided in various forms to people who registered with the service. The Department for Work and Pensions also set up an additional call centre including to phone people and check on their wellbeing.

Ultimately, vulnerable individuals were able to request support from the CEVPS either through the GOV.UK website or the call centre, which required regular updates to the CEVPS List and Shielded Patient List and informing all involved in providing support. All participating organisations were regularly provided with updates to both lists via feedback loops that GDS and NHS Digital had developed, which updated the lists as the clinically extremely vulnerable definition or the support for or requests by vulnerable individuals changed.

Timeline Key dates during the creation of the CEVPS



Source: Adapted from *Protecting and supporting the clinically extremely vulnerable during lockdown*, National Audit Office, 2021.

Key themes from the discussion

The clear, urgent need for a support service was motivating and provided project clarity. The strong sense of social purpose created goodwill between people, departments and organisations to find solutions to problems, making sure data could be shared as needed.

Having a multidisciplinary team drawn from a range of departments and public bodies from the beginning was integral to producing a functional service rapidly. The CEVPS project team had leadership from different areas, depending on the task. GDS, on behalf of the Cabinet Office, was at the centre of the CEVPS development, working closely with NHS Digital, while MHCLG was involved in linking up local authorities and Defra with food suppliers. In addition to these split responsibilities, the personnel involved represented a combination of policy, legal, security, technical and data sharing expertise. The team then designed the service with data security and information governance baked into the technical solution, implementing a privacy-by-design approach along with timely involvement of data protection and privacy expertise. This allowed GDS's early engagement with the ICO about what legal provisions could be used to support the data sharing needed to support the CEVPS and how accountable data controllership^{*,2} within the CEVPS would be achieved.

UK law is permissive, but data sharing should be scrutinised. The CEVPS represented exceptional sharing of health data with local government at pace, but not all data sharing should be this fast. Rather, a clear and considered justification for sharing data, which should be scrutinised over an appropriate period of time, is essential for good management and public trust. Participants were clear that the UK General Data Protection Regulation (GDPR) provided a useful basis to guide the creation of a gateway for legal and necessary data sharing. In the CEVPS case, the flexibility of the UK GDPR enabled rapid data sharing in the public sector, given the justifiable public health reasons. The team gave suitable importance to the accountability principle, in terms of incorporating appropriate data protection measures and being able to show compliance with the UK GDPR,³ by recording the requirements and justifications for decisions made for the CEVPS via regular updates to a central record log.

Public engagement and transparency prevented any perceived contentious issues stopping the project. The project team were aware of the potential for concerns about sharing information from within the health care system with other government organisations and the private sector, and prepared accordingly by engaging with the regulators, internal special interest groups (the NHS's Independent Group Advising on the Release of Data, for example) and the media and via communications channels. By offering internal and external transparency about what, how and why data was being shared, and only sharing the minimal data required, the team avoided a negative public response.

* Accountable data controllers are responsible for guaranteeing that data processing complies with the UK GDPR.

Areas covered during the discussion

Project clarity and purpose

A recurring theme at the roundtable was that success was predicated on **the serious need for and the specific purpose of** the CEVPS. The team responsible had a clear mission with support from senior decision makers and ministers to deliver a service that would save lives. This kind of senior support removed barriers between organisations and gave the team space to build the service, while daily meetings with the GDS markdown team to report progress kept the team motivated and accountable.

Clarity motivated the team and the purpose of the service enabled collaboration across organisational boundaries. For example, due to the need to give preferential access to supermarket home delivery slots, government shared a list of those who had registered for support with shielding (the CEVPS List) with supermarkets for matching with their own customer databases. The data was provided with a clearly defined purpose for supermarkets' processing and limitations over how supermarkets could use the data; they were required to never use the data for anything other than supporting the service and had to delete the data once the shielding service ended. This was outlined from the start in the relevant data sharing agreement.

The narrow focus of the project also helped leaders make decisions about additional requests for access to the CEVPS List. At one point, an external organisation asked the project leaders for access to the whole CEVPS List for purposes unrelated to supporting vulnerable people and beyond the anticipated use of the data. This request was refused because it was out of scope of the data sharing agreement, highlighting the benefits of having clear and specific project and data sharing agreements and Data Protection Impact Assessments (DPIAs) in place for simplifying decision making.

Adaptable solutions

While the overarching project purpose was clear, the CEVPS went through multiple iterations in line with policy decisions and clarifications. These varied, from deciding how to build the initial Shielding Patient List* and whether to allow self-referral additions to the list, to how to check whether everyone on the list was receiving support. All of these points had to be clarified between the project team and policy makers as situations arose, in part due to the necessary speed of service implementation, and the outcomes that needed to be incorporated into the technical design and data sharing agreements as they went along.

The original technical solution for the CEVPS assumed the CEVPS List to be a fixed one and shared information with local authorities and supermarkets accordingly. But as the service operated, feedback loops were built in to allow individuals to opt out of support, through contacting the service's bespoke call centre, via their local authority or in some cases writing to their MP. The roundtable participants described the situation, once MPs started receiving letters, where a new information flow into the service had to be established, added into the DPIA and incorporated into the service. One participant

* No single information source was available to identify all who needed to shield and instead NHS Digital built this up over time.

said that they had ended up developing a “customer management system” and had they known that was the final output, the original build would have been different, with various information feedback loops incorporated into the service from the start.

Team capability

All participants were clear that the service succeeded due to having a **multidisciplinary team from the start**. The team consisted of data protection officers and people with security, legal, technical and policy expertise from the participating departments. Such a mixture of expertise made it quicker to understand different motivations and the decisions that had to be made. Technical experts gained a clear understanding of the emerging policy they needed to build towards, and senior decision makers had direct access to legal and security expertise, allowing them to identify obstacles and know what was and was not possible. Jessica McEvoy, then a deputy director at GDS and now principal consultant at software consultancy Scott Logic, helped to bridge this policy and technical world on the CEVPS project. She expressed that: “Getting all the right people in the ‘room’ from the start was key to the success of the initiative.”

The CEVPS, given the sensitivity of handling personally identifiable data, required a DPIA, which was started on day one of the project. A DPIA is a process that identifies the data protection risks and helps data controllers minimise those risks.⁴ Writing the DPIA involved understanding what functions the service had to administer, what data was necessary to support this, and where and how the data would be collected and stored, requiring the full range of skills from the team to ensure all aspects were fully considered. The DPIA was iterated as policy decisions were made and new information was brought into the project, but having an early draft helped the team identify risks and put solutions in place without slowing progress on the technical build. The DPIA also helped define requirements for the systems, prioritise decisions and identify capabilities to best support the project.

The roundtable participants all agreed that having early input from information governance and legal perspectives was essential to the success of the CEVPS. One participant explained that too many projects are designed and built without considering the legal aspects of sharing and holding data, which often require redesigning the technical solution to ensure data is properly protected. Any prolonged discussion about data security for the CEVPS would have delayed support to the shielding population. Having a multidisciplinary team in place from the start meant many of these possible delays were avoided.

Having information governance and legal perspectives also encouraged the team to build in privacy-by-design and data minimisation* best practices. This was especially important when sharing information with the private sector and other organisations, which needed to know if someone was shielding but did not need to know the medical condition that was leading them to shield, for example. Part of this came from having a clear list of who needed access to what data, with a clear separation of business reporting and management information from personal data processing.

* Data minimisation involves only taking in or passing on necessary information. For example, the service did not need to know the medical conditions requiring individuals to shield, only that they should shield. As a result, it never held individuals’ medical information.

Participants all agreed that the mixture of capabilities in the team prevented incorrect solutions being progressed during the build, with one noting that they had never “had so much liaison [between] the policy, data protection officer, legal and technical people” on a single project, and that this was an innovation to repeat in the future.

Data sharing agreements

The CEVPS required the sharing of personal information (that is, names, addresses and the fact that people were clinically extremely vulnerable) from the health system with other government departments and local authorities to set the service up. Personal data obtained from the health care system is covered by a common law duty of confidentiality,⁵ which has a more onerous set of data sharing requirements than the UK GDPR.

As the CEVPS was designed, the project team iterated their justification for sharing confidential personal information. ‘Public interest’ under the common law duty of confidence was first explored. The reasons for sharing were then examined in March 2020 with the National Data Guardian and the ICO to help the project team assess risks and consider what was required from a transparency and process perspective. Participants at the roundtable praised this “risk stratification group”, given the urgency and novelty of the data sharing, especially for obtaining input from the regulator – the ICO – to inform the service. Being able to quickly identify a clear legal route for such an unprecedented sharing of personal health information showed the flexibility and permissibility within the UK GDPR.

For clarity over how data was shared, a tiered approach was developed that streamlined the selection of the legal basis used for different bits of data sharing (that is, public task in the first instance and if not, then legitimate interest). The tiered approach also encouraged the collation of a decision log for which legal basis was used in different parts of the service, which was especially important when multiple legal bases might be relevant for the different data shares. This highlights how much data sharing is possible within existing legislation given a genuine purpose and support from participating organisations.

The initial data sharing route for local authorities specifically was later superseded by the release of the Control of Patient Information (COPI) notice in March 2020 by the secretary of state for health and social care.⁶ The COPI notice created a ‘Covid-19 purpose’ for the sharing of confidential medical information across organisations in the health service and beyond for activities to protect public health, provide health care services and monitor and manage the outbreak. COPI was quickly integrated into the DPIA as the final legal route, given the specific reassurances around the sharing of health data for the pandemic response.

By using the temporary COPI notice as the legal justification for sharing and collecting data, the list of clinically extremely vulnerable people and associated services using this data had a built-in end date. This provided reassurance to those involved with the service that the rapid sharing of personal data would only be possible because of

and during the health emergency. But this kind of data sharing would be difficult to immediately stand up or replicate during a future emergency without more thought about how to share the data or re-issuing new, similar COPI notices.

Role of local authorities

Local authorities were responsible for handling the data listing the clinically extremely vulnerable people in their area and providing support beyond the early centralised home delivery food parcel scheme. This included care and medicine provision and, later in the pandemic, food provision* and checking on support being provided, which then had to be reported back to central government. This presented a challenging data task that local authorities were not always prepared for. But they ultimately managed to support a successful service.

As the Shielded Patient List was updated continually, the full list data was provided to local authorities daily, which would then need to be matched with previous lists (to detect any changes in the people being supported) and matched with existing local authority datasets (to see what overlapping support or information was available). As the service matured, the format of the data being provided to local authorities evolved, which required local authorities to change their data management practices. This was difficult for less technically able local authorities, which had to join five different data feeds to inform decisions about aspects of service provision.

Partly in acknowledgement of the need for technical support, MHCLG organised teach-in sessions, which technical specialists supported. This helped local authorities use the data as effectively as possible and it helped identify any issues with the data that the service might not be able to resolve (for example, not being able to distinguish between people with the same name in the same postcode). Feedback through the teach-in sessions and other routes eventually led to the service incorporating unique property reference numbers (UPRNs) to individual entries so that support could be better targeted (especially when multiple shielding people lived at one address). Multiple participants expressed a regret that a local authority voice was not present in the multidisciplinary team during the initial decision making and design process. It was thought that having MHCLG present in those discussions would be enough, but on reflection, participants agreed it would have been even better to include a selection of those who were ultimately responsible for service delivery to input their needs into the service design.

Beyond internally handling the data, local authorities had questions about what else they could do with the CEVPS data. To help, MHCLG produced various guidance notes, which included a list of what could or could not be done under the data sharing agreement in place. This was later changed to detailing key points relevant to local authorities, including answers to questions that local authorities were asking, such as how data could be shared with others such as care homes.

* A standard food box was arranged by government to be delivered by the wholesale food suppliers. Local authorities provided further support to meet religious, dietary or cultural requirements that were not met by the standard box.

Providing general advice and guidance to local authorities (for example, it was better to give guidance such as “data can be shared to support care provision” rather than “data can be shared with sub-contracted care providers”) was useful as it provided some leeway depending on their circumstances, while providing confidence that they were compliant with data protection requirements.

Public engagement

Participants thought that government risked a negative public response in sharing personal information – particularly with supermarkets. When the service was first announced, challenging headlines were published about how health data might be shared with supermarkets without individuals’ consent.⁷ Government quickly clarified the plans to explain that a minimal amount of data was being passed to the supermarkets, which in some cases could be matched with their existing customer databases, so that the shielding population could have preferential access to home delivery slots.

The rapid and confident response was possible due to the time the team spent working with supermarkets on the data sharing arrangements, given the risks and perceived risks to public trust of sharing personal information with the private sector. Data protection officers from the supermarkets worked with the ICO to determine their own legal position for holding data from the CEVPS and had to show how this data would be deleted as requested at the end of the service. Central government could have helped link up supermarket data protection officers so they could better collaborate with the ICO, but otherwise this was successful in creating a publicly defensible position for the data sharing.

Success in reassuring the public relied on a number of factors. The demonstrable need for a service that could support the vulnerable shielding population in the face of a national emergency gave a very clear justification for quickly taking action, which was supported by well-planned data security that was incorporated from the beginning of the project. Early engagement with the ICO ensured there was a legal justification for the data sharing and the service had in place a communications team that was fast to respond to difficult media headlines. One participant expressed that “knowing the data was going into a secure service was useful from an assurance perspective”, while practising data minimisation and setting time limits for all organisations for holding the data were other methods used to instil public confidence.

The roundtable participants were very positive about their public engagement and awareness activities, albeit that the speed required to start the service limited these activities. Proof of the success of public engagement was the lack of evidence to suggest that the public made many complaints about the service.

Key lessons and recommendations from participants

Participants drew out several key lessons and recommendations for government, based on their experience of creating and running the CEVPS. These included:

- Bringing in information governance and legal expertise at the beginning of a project should enable greater and more accountable data sharing to happen.
- Government should engage with the public in an open and transparent way at all stages of setting up new data sharing projects, so that the public are aware of what data is being shared, why it is being shared, the benefits of data sharing and what the data sharing will enable. This engagement will require transparency about the risk of data sharing and potentially involve publishing the DPIA.
- DPIAs should move from being internal, compliance driven documents to public-facing and accessible documents. Increased “working in the open” on data sharing initiatives and agreements will increase public confidence and trust.
- When establishing new and novel data sharing agreements, risk stratification groups of “critical friends” should help to work through the risks of data sharing as viewed from different perspectives and the logic of and need for sharing the data. Critically, these should involve the regulator (that is, the ICO) to help them understand the project requirements and collectively identify the process points that must be worked through to open a legal sharing route.
- The education of senior decision makers and ministers on data sharing and how to build successful data sharing agreements must continue. The pandemic shows what can be achieved at speed, but this will not be true for all cases. Data sharing takes a range of expertise, a common sense of purpose and priority and an ongoing focus. This must all be reflected in the education provided to senior decision makers, given how many aspects must come together to deliver a successful data sharing agreement.
- A balance should be struck between centralisation and localisation. It should be possible to avoid duplication of effort – whereby local authorities conduct the same type of analysis as each other – and instead do more central processing of information.
- Government should be better prepared for data sharing during future emergencies. This could be through a new objective in the Digital Economy Act 2017 to enable data sharing in accordance with emergency preparedness.

Gavin Freeguard is a freelance consultant and associate of the Institute for Government
Paul Shepley is a data scientist at the Institute for Government

References

- 1 Comptroller and Auditor General, *Protecting and supporting the clinically extremely vulnerable*, Session 2019-2021, HC 1131, National Audit Office, 2021
- 2 Information Commissioner's Office, 'What does it mean if you are a controller?', ICO, retrieved 11 December 2022, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-a-controller/>
- 3 Information Commissioner's Office, 'Accountability principle', ICO, retrieved 11 December 2022, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accountability-principle/>
- 4 Information Commissioner's Office, 'Data protection impact assessments', ICO, retrieved 11 December 2022, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>
- 5 Bhatia N, 'The Common Law Duty of Confidentiality (CLOc) a brief factsheet', NHS, retrieved 11 December 2022, www.nhsdatasharing.info/CLoC%20Factsheet%20NB.pdf
- 6 NHS Digital, 'Control of patient information (COPI) notice' NHS Digital, retrieved 11 December 2022, <https://digital.nhs.uk/coronavirus/coronavirus-covid-19-response-information-governance-hub/control-of-patient-information-copi-notice>
- 7 Hern A, 'UK supermarkets contacting vulnerable patients 'must delete data when crisis abates'', *The Guardian*, 7 April 2020, retrieved 11 December 2022, www.theguardian.com/business/2020/apr/07/uk-supermarkets-contacting-vulnerable-patients-must-delete-data-when-crisis-abates

The Institute for Government is the leading think tank working to make government more effective.


We provide rigorous research and analysis, topical commentary and public events to explore the key challenges facing government.

We offer a space for discussion and fresh thinking, to help senior politicians and civil servants think differently and bring about change.

Copies of this IfG Insight are available alongside our other research work at:

 instituteforgovernment.org.uk

 enquiries@instituteforgovernment.org.uk

 +44 (0) 20 7747 0400  +44 (0) 20 7766 0700

 [@instituteforgov](https://twitter.com/instituteforgov)

**Institute for Government, 2 Carlton Gardens
London SW1Y 5AA, United Kingdom**

December 2022

© Institute for Government 2022

The Institute for Government is a registered charity in England and Wales (No.1123926) with cross-party governance. Our main funder is the Gatsby Charitable Foundation, one of the Sainsbury Family Charitable Trusts.