



**South African – European Union Dialogue Facility**  
**International Dialogue on**  
**Strengthening Open Digital Governance in South Africa**

***Report on the South African Experience***  
***in Open Digital Governance***

**Luci Abrahams and Mark Burke**

**LINK Centre, University of the Witwatersrand**



**Prepared for the SA–EU Strategic Partnership Dialogue Facility**

**April 2022**

## Table of Contents

<b>1. Introduction: Perspective on Open Digital Governance Foundations in South Africa</b> .....	1
<b>2. Evolution of Digital Governance in South Africa</b> .....	2
<b>3. Digital Leadership through Policy, Strategy, Regulation and Institutional Arrangements</b> ...	5
<b>3.1. Policy and Strategy</b> .....	5
<b>3.2. Regulation and Enforcement</b> .....	7
<b>3.3. Institutional Arrangements</b> .....	9
<b>3.4. Public Sector Digital Capabilities</b> .....	10
<b>3.5. Standards and Interoperability</b> .....	11
<b>4. Case Studies</b> .....	11
<b>5. Case 1: Digitalisation in Public Health Services – Accelerating Public Health</b> .....	12
<b>5.1. Strategic Leadership</b> .....	13
<b>5.2. Policy and Regulatory Environment</b> .....	13
<b>5.3. Standards and Interoperability</b> .....	14
<b>5.4. Systems and Applications in Health Service Digitalisation</b> .....	14
<b>5.5. Data Sharing, Privacy and Cybersecurity</b> .....	15
<b>6. Case 2: Digital Transformation in Basic Education – Collaborative Engagement of Role Players</b> .....	15
<b>6.1. Systems Applications in Education: Making the Case for Communities of Knowledge and Practice (CoKPS)</b> .....	16
<b>6.2. Digital Leadership for Open Digital Governance in Basic Education</b> .....	19
<b>6.3. Policy and Regulatory Environment for Schools: New Operating Guidelines, Data Sharing and Cybersecurity</b> .....	20
<b>7. Key Challenges</b> .....	21
<b>8. Priorities to Unlock and Accelerate Open Digital Government</b> .....	22
<b>References</b> .....	24

## Abbreviations

4IR PMO	-	4IR Project Management Office
ABIS	-	Automated Biometric Identification System
AFIS	-	Automated Fingerprint Identification System
BAS	-	Basic Accounting System
BI	-	Business Intelligence
CCMDD	-	Centralised Chronic Medicine Dispensing and Distribution
CHPC	-	Centre for High Performance Computing
CIO	-	Chief Information Officers
CPA	-	Consumer Protection Act
DPSA	-	Department of Public Service and Administration
CPSI	-	Centre for Public Service Innovation
CRT	-	Cybersecurity Hub Security Incident Response Team
DHIS	-	District Health Information System
DIRISA	-	Data-intensive Research Initiative of South Africa
ECTA	-	Electronic Communications and Transactions Act
eNATIS	-	Electronic National Transport Information System
EVDS	-	Electronic Vaccination Data System
FIC	-	Financial Intelligence Centre
FICA	-	Financial Intelligence Centre Act
FM	-	Financial Management
FMS	-	Financial Management System
FOSS	-	Fee and Open Source Software
GCIO	-	Government Chief Information Officer
GITOC	-	Government Information Technology Officers Council
GIS	-	Geographic Information Systems
GPCE	-	Government Private Cloud Ecosystem
GDPR	-	General Data Protection Regulation
HANIS	-	Home Affairs Identification System
HIS	-	Health Information System
HNSF	-	Health Normative Standard Framework
HPRS	-	Health Patient Registration System
HRM	-	Human Resource Management
HSRC	-	Human Sciences Research Council
ICSDM	-	Integrated Case Document Management System
IFMS	-	Integrated Financial Management System
IIMS	-	Integrated Inmate Management System

IJS	-	Integrated Justice System
IM	-	Information Management
LOGIS	-	Logistical Information System
NATIS	-	National Transport Information System
NDP	-	National Development Plan
NEIMS	-	National Education Infrastructure Management System
NHI	-	National Health Insurance
NHIRD	-	National Health Information Repository and Data-warehouse
NPR	-	National Population Register
NPRS	-	National Patient Registration System
NT	-	National Treasury
PAIA	-	Promotion of Access to Information Act
PERSAL	-	Personnel and Administration System
PHC	-	Primary Healthcare
PIVA	-	Person Identification and Verification Application
POPIA	-	Protection of Personal Information Act
RICA	-	Regulation of Interception of Communications and Provision of Communication-related Information
SACN	-	South African Cities Network
SAHRC	-	South African Human Rights Commission
SAPS	-	South African Police Services
SARS	-	South African Revenue Service
SCM	-	Supply Chain Management
SITA	-	State Information Technology Agency
SVS	-	Stock Visibility System

## **1. Introduction: Perspective on Open Digital Governance Foundations in South Africa**

This introduction comments on the South African experience in relation to the five overarching insights presented in the paper on international experience. The commentary is based on the brief discussion of the evolution of digital government in South Africa, the brief overview of South Africa's digital leadership experiences, and two case studies, namely digitalisation of public health services and early digital transformation in basic education. The paper is a foundation for dialogue, noting that ongoing research is required to inform practice.

### **Overarching Insight 1: A 21st century public service for 21st century citizens: Mission, leadership, and positioning of institutions responsible for public service innovation for open digital governance**

The South African public service has thus far not exhibited a sufficiently strong mission of transitioning to digital government or building the foundations of digital governance. South Africa needs to be much more strongly mission-driven at those critical points at which citizens depend on government for quality of life and for their future livelihoods, and where digital enablement would make a difference. Public health digitalisation efforts have mushroomed, yet there is much to do to invest in the many parts of the public health service and the many types of health services delivery that could benefit from digitalisation, particularly at the primary healthcare level where quality of life is affected. Slow progress in building digitally-enabled basic education and blended learning has limited the opportunities for improving the quality of the learning experience, essential to building future livelihoods. Looking to the future, strengthening collaborative engagement, with citizens as key role players in governance, is necessary to anchoring a mission orientation.

### **Overarching Insight 2: Shifting to “digital-first”: Digital applications and data-driven public services for open digital governance**

The opportunities to introduce and exercise a “digital-first” approach to building open digital governance in South Africa should be carefully explored. Adopting a digital-first approach means exploring digital enablement first as a solution to the challenges of accountable, open and transparent government; it does not mean adopting digital enablement under all circumstances, just for the sake of going digital. Where the benefits of such digital enablement outweigh the associated risks, a digital-first approach would be warranted.

### **Overarching Insight 3: A 21st century public servant for a 21st century public service: Human capability for open digital governance**

The South African public service is in a process of major, long-term transition, where the focus has been on improving the capacity of the state to deliver, in terms of policy and in terms of service to citizens, in order to ensure equity and quality in service delivery, within the paradigm of a developmental state. Human capability for open digital governance is but

one aspect of this bigger picture of continually building the capacity of the state. Nevertheless, it is an important foundation for the 2020s.

#### **Overarching Insight 4: Making open governance possible: Legislation, regulatory frameworks, and standards for open digital governance**

South Africa has established a few of the legislative foundations needed for open digital governance, notably personal data protection under the Protection of Personal Information Act, No. 4 of 2013 (POPIA), noting the commencement date of initial sections on 11 April 2014, and the commencement date of the other sections on 1 July 2020, with the exception of two sections. South Africa has also introduced cybercrimes legislation, namely the Cybercrimes Act, No. 19 of 2020. Other legislation that will be required to create a suitable legislative framework includes cybersecurity legislation and regulations to promote open data initiatives for the re-use of public sector information.

#### **Overarching Insight 5: Public service innovation: Continually building a future orientation for open digital governance**

Various initiatives in open digital governance are evolving in South Africa, across the spheres of government, as discussed in the next section. Furthermore, in the period since the formation of the Centre for Public Service Innovation (CPSI) in 2001, it has encouraged initiatives in open innovation for the public service (see [www.cpsi.co.za/open-innovation/](http://www.cpsi.co.za/open-innovation/)), and the Department of Public Service and Administration (DPSA) has stewarded an open data initiative (DPSA, no date). These initiatives need to be more strongly foregrounded as part of mainstreaming open innovation and open digital governance, facilitated by the DPSA.

In this paper on the South African experience relevant to open digital governance, the education and public health case studies relate to and offer insights into each of the five overarching insights.

## **2. Evolution of Digital Governance in South Africa**

The emergence of digital governance has been an ongoing evolutionary process in the South African public sector for 70 years, following a similar path to public administrations in developed countries. The process triggers *significant changes in the properties of the institutions of governance* through a combination of information, computing, communication and connectivity technologies over this period, including the new structures, cultures, roles and skills requirements (Vial, 2019). This evolutionary process has been spearheaded by the introduction and rollout of digital management support systems that comprise transaction processing systems, management information systems, executive information systems, decision-support systems, enterprise resource planning systems and supply-chain management systems, among others (Cloete, 2003).

These technologies automate the back-office administration and management and the front-office service delivery environments. This multifaceted phenomenon involving various services and technologies changes the nature and place of citizen–government relations, and changes the casting and roles of the actors involved (Lindgren & Jansson, 2013). It

facilitates the automatic exchange of information and delivery of transactions between citizens and government, enables additional communication channels, and enables 24/7 access to government services (Lindgren et al., 2019). *Automation* enables *datafication*, the process by which data is collected, stored, shared and analysed digitally (Amoore & Piotukh, 2016; Lips et al., 2009). The adoption of these technologies also means that the interaction between citizens and government is increasingly *mediated digitally* (Berry, 2014; Cohen, 2015).

The Division of Economics was one of the first public entities to implement an electronic tabulator in 1952 (NARMIC, 1984). The introduction of computers in the public sector must be understood in the context of the growing diffusion of technology at the time, with the computer industry growing by 30% annually in the 1960s (Leonard, 1978). The Bewysburo started converting paper-based records related to tax particulars and the Population Register for Bantu to computer-readable magnetic tape in 1996 (Edwards & Hecht, 2010). The Department of State Expenditure introduced the cash-based accounting and batching system, the Financial Management System (FMS), in 1973, which would be used for another two decades before being replaced (DPSA, 2003).

The 1990s witnessed the introduction of several large-scale, *system-wide transversal management support systems* in the South African public service (DPSA, 2003). The Personnel and Administration System (PERSAL) has been in operation since 1990 as an integrated human resource, personnel and salary system that interfaces with other systems from financial, educational, insurance institutions and medical aid and pension funds. The Basic Accounting System (BAS), which was developed in 1993 and came into operation in 1995 to replace the FMS, is a basic accounting system introduced to cater for government's accounting needs. Vulindlela, a data warehouse providing human resources, financial and logistical reports by extracting data from internal and external operational data systems, was launched in 1997 (Paterson et al., 2015). The Logistical Information System (LOGIS) has been operational since 1998 and provides management information to control and regulate stock levels and movable assets (DPSA, 2003).

In the early 2000s, several large-scale digital systems to support the delivery of services were introduced in specific sectors and domains, as illustrated by the following examples. In the health sector, the District Health Information System (DHIS) was introduced in 1996 and extended to the entire country by 2001, with the aim of collecting aggregated routine data from public health facilities in the country (Garrib et al., 2008) and constitutes an integral part of the emerging Health Information System (HIS). The South African Police Services (SAPS) purchased the Automated Fingerprint Identification System in 2002 (Breckenridge, 2005), to replace the manual system introduced in 1925 (SAPS, 2003). The Department of Transport oversaw the development of the Electronic National Transport Information System (eNATIS) over the period 2002 to 2007, when it replaced the National Transport Information System (NATIS), with effect from April that year (Auditor-General South Africa, 2008). In 2007, the South African Revenue Service (SARS) introduced its eFiling platform under its modernisation programme to enable automated tax returns (Carreira & Mtshali, 2019).

Government also recognised the need to re-invest in updating its transversal systems and to upgrade or introduce new digital platforms that could take advantage of affordances provided by newer technologies, though often hampered by delays in the implementation of these initiatives. In 2005, Cabinet approved the implementation of the Integrated Financial Management System (IFMS) as a joint initiative between National Treasury (NT), the DPSA and the State Information Technology Agency (SITA) to modernise the management of back-office processes in the public service in the domains of Financial Management (FM), Human Resource Management (HRM), Supply Chain Management (SCM) and Business Intelligence (BI) (DPSA, 2018a).

Several sector-specific digital platforms, management systems and databases were introduced in the second decade of the 21st century. Examples of these include the introduction of the National Health Information Repository and Data-warehouse (NHIRD) and the National Patient Registration System (NPRS) to support digitally-enabled health services, and the Integrated Case Document Management System (ICSDM), the Person Identification and Verification Application (PIVA), and the Integrated Inmate Management System (IIMS) for digitally-enabled service provision in the integrated justice system (IJS).

Local governments in South Africa have also increasingly adopted digital technologies to support service delivery and promote participation by citizens in planning and decision-making processes. Metropolitan municipalities with their larger tax base in urban areas have spearheaded digital governance initiatives by digitalising services such as invoicing and billing of rates and taxes, reporting of service interruptions, making available spatial data information using geographic information systems (GIS), and supporting property valuation services, among others. Increasingly, municipalities are using e-participation platforms that support engagement with citizens using SMS, websites, Facebook, Twitter and YouTube channels (Okeke-Uzodike & Dlamini, 2019).

Promoting active citizenry to strengthen development, democracy and accountability is one of six interlinked priorities for South Africa, according to the National Development Plan (NDP) (NPC, 2012). The NDP views a robust democracy as an essential prerequisite for the kind of developmental state needed to tackle poverty and inequality. One of the ways in which an active citizenship can be enabled, according to the *National e-Government Strategy and Roadmap* (DTPS, 2017), is to expand the technological capabilities of citizens and businesses for participation in the government decision-making process. Digital technologies are increasingly viewed as a means to enhance the quality of democracy through their role in the increased speed and scale of information provision and informing citizens; developing new ways of political and citizen participation; creating new ways of organising; and facilitating the establishment of new political actors and communities (Lindner & Aichholzer, 2020).

Digital technologies, thus, have the potential to transform the way in which citizens are informed by and interact with government, and to influence decision-making through platforms that enable monitoring public services and actions, consultation, deliberation, and co-production and co-creation. Supporting these activities requires a mix of transparency, accountability, trust and legitimacy. For example, a number of measures have been adopted



by the Parliament of the Republic of South Africa to inform and invite citizen participation in the legislative process, including a presence on platforms such as Facebook, Twitter, YouTube and Instagram (Odeyemi & Abioro, 2019). South Africa is also a member of the Open Government Partnership (OGP) and has committed to upholding the principles of open and transparent government. The DPSA has played an active role in the consultation process to define South Africa's priorities in this regard. The country launched an initiative called Open Data South Africa (<https://opendataza.gitbook.io/toolkit/>) aimed at encouraging the use of government data for social impact under the stewardship of the DPSA, and working with OpenUp, the CPSI, The Innovation Hub, Geekculcha, Open Cities Lab and the Human Sciences Research Council (HSRC). Initiatives such as Municipal Money (<https://municipalmoney.gov.za/>), a web portal making available extensive municipal financial information in an easily accessible format, is aimed at promoting transparency as part of the NT's budget participation reform process, in addition to the existing Online Budget Data Portal called Vulekamali (<https://vulekamali.gov.za/>). The City of Cape Town (<https://odp.capetown.gov.za/>) and the eThekweni Municipality (<https://edge.durban/>) have both launched open data initiatives to foster transparency through the sharing of information. The South African Cities Network (SACN) has launched the South African Cities Data Almanac, a city-centric data portal providing evidence, analysis and insight ([www.scoda.co.za](http://www.scoda.co.za)).

As outlined above, the evolution of digital government can be periodised into four main periods. Prior to the 1990s, it was enabled by the introduction of mainframe computers with complex interfaces and centralised administrative systems that systematised and initiated the automation of operational support functions such as financial management. This was followed by system-wide transversal management support systems during the 1990s. From the 2000s, the rollout of large-scale systems to support service delivery in sectoral domains can be observed. Since the second decade of the 21st century, increasingly sophisticated and connected databases and management systems were introduced that started interfacing across transversal and service domains. The implementation of digital management support systems that enable public service digitalisation has not been without challenge. The implementation of large-scale systems has been plagued by cost overruns and delays. Several factors have contributed to this situation, including business cases that motivate the approval of public funding but often understate and underestimate the costs and complexity of projects, poor procurement practices and corruption, and limited implementation capacity (DHA, 2021; Ensor, 2021).

### **3. Digital Leadership through Policy, Strategy, Regulation and Institutional Arrangements**

This section reviews how digital leadership is expressed across the policy, strategy and regulatory domains for open digital governance.

#### **3.1. Policy and Strategy**

The development of digital government must be understood in the context of public service transformation as well as policy guidance focusing explicitly on digitalisation.

The challenge confronting the post-apartheid government was transforming the public service into a democratic structure and improving the public service's capacity to play a developmental and transformative role. In the year preceding the democratic elections, approximately 1,187,600 public servants were employed in the public service of South Africa and the ten Bantustans. A critical task awaiting the new government was the amalgamation of these separate "states" into one nation, as well as the rationalisation of these disparate public administrations into one national public service. The *White Paper on the Transformation of the Public Service* (RSA, 1995) envisioned a public service that would improve the lives of the people of South Africa. The policy made an explicit link between achieving national objectives and doing so through the expansion and improvement of public services. The *White Paper on Transforming Public Service Delivery (Batho Pele)* (DPSA, 1997, p. 11) sought to provide a practical implementation strategy for the transformation of public services and, in particular, aimed to bring about a shift away from "inward-looking, bureaucratic systems, processes and attitudes, and a search for new ways of working which put the needs of the public first, is better, faster and more responsive to the citizens' needs."

The first policy on digital government, issued in 2001 and entitled *Electronic Government: The Digital Future*, emphasised the role of technology in moving away from the bureaucratic organisation around agencies operating like "stove pipes", and streamlining their functions according to the needs of the citizens through their internal efficiency and effectiveness, as well as the costs and quality of governance (DPSA, 2001). The *National Integrated ICT Policy White Paper* (DTPS, 2016) incorporated the digital transformation of the public service as a core pillar and called for the development of a detailed, integrated national digital government strategy and roadmap. This policy prioritised the development of a single access point for all digital government services, providing affordable access, protecting privacy and security, and establishing a system to assure digital identity for citizens when transacting with government. The envisioned strategy and roadmap were published the following year (DTPS, 2017), prioritising the development of a national digital government portal for the delivery of e-services, back-end integration to achieve a single view of the citizen, the establishment of a data warehouse to host citizen information, implementing a common cloud architecture, and the use of e-ID technology for authenticating and securing the identities of parties to an e-transaction. Three important policy developments focused on cybersecurity, digital identity and data further elaborate some of the priorities identified in the digital government policy.

Government adopted a *Policy on Free and Open Source Software Use for South African Government* (DPSA, 2006) with the objective of directing public sector organisations to adopt free and open source software (FOSS) and to migrate current proprietary software to FOSS. The State Security Agency (SSA) published a *National Cybersecurity Policy Framework for South Africa* in 2012 (SSA, 2012) to provide for measures for cyberspace security, combatting cyber warfare and crime, and the establishment of a Cybersecurity Hub Security Incident Response Team (CRT). The Department of Home Affairs issued a draft *Official Identity Management Policy* in December 2020 for public consultation setting out the options and approaches that government is considering to manage, among others, digital identity (DHA, 2020b). The policy discussion document identifies a single digital population

register that is biometric-based and that can provide a single view of a person as a key element of digital identity management. It further recognises that legislation will be necessary to establish clear rules to govern accessing and processing the population register records. The Department of Communications and Digital Transformation (DCDT) published the *Draft National Policy on Data and Cloud* (DCDT, 2021b) with the objectives of unlocking the value of data, enhancing data analytics capabilities, and promoting responsible decision-making for growth and well-being. The draft policy document proposes that all public data must be captured in digital format by default and that a copy of data generated in South Africa should be stored in the country and co-owned by government.

Digital government policy sits at the intersection of policies aimed at service delivery transformation, on the one hand, and the use of technologies to enable the internal transformation of government administration, on the other hand. These policies have been elaborated over time, with those adopted in the early years having a technology bias. This was followed by policies with a stronger service transformation bias, and, more recently, by policies with a risk mitigation bias insofar as cybersecurity, digital identity and data ownership are concerned.

### **3.2. Regulation and Enforcement**

The key legislative and regulatory measures relevant to open digital governance relate to privacy, data protection, e-commerce and cybersecurity.

The coming into force of the *Protection of Personal Information Act* (POPIA) of 2013 in July 2020 marked a significant milestone in the establishment of the regime to protect personal information in South Africa. POPIA is designed to give effect to the constitutional right to privacy and seeks to regulate how personal information may be processed, by providing persons with the rights and remedies to protect their personal information while establishing measures to ensure respect for and to promote, enforce and fulfil the rights protected. A principle-based approach underpins the legislation, like the approach adopted in the General Data Protection Regulation (GDPR) of the European Union. The principles relate to notice and consent; correction, destruction and deletion of personal decision-making; data minimisation; data storage limitation; purpose limitation; quality of data; and access by the data subject, among others. Importantly, POPIA limits the use of automated decision-making in that the data subject may not be subject to a decision which results in legal consequences based solely on the basis of the automated processing of personal information intended to provide a profile of such a person (section 71). Exclusions from the scope of POPIA include de-identified information, the processing of information that involves national security, defence or public safety, or that which is processed for the purpose of the prevention and detection of criminal activities, among others. POPIA makes provision for the establishment of the Information Regulator, which is responsible for education and awareness, monitoring, and enforcing compliance. Sanctions under the Act include a fine or imprisonment for a period not exceeding ten years, or both.

Several other pieces of legislation regulate access to and the sharing of data. The *Promotion of Access to Information Act* (PAIA) of 2000 regulates access to information in both the

public sector and the private sector, giving effect to the constitutional right of access to information held by the state or any other person required for the exercise of protection of rights. Responsibility for regulating initially vested for nearly two decades with the South African Human Rights Commission (SAHRC), but has now been shifted to the Information Regulator. The *Financial Intelligence Centre Act* (FICA) of 2001 establishes the Financial Intelligence Centre (FIC) to combat money laundering by empowering the regulator to store records for five years about financial transactions between banking institutions and their clients, and to gather and make available information to investigating authorities. The *Electronic Communications and Transactions Act* (ECTA) of 2002 supports digital government by providing for the filing, creating or retaining of documents in the form of data messages by public bodies. ECTA addresses the intentional and unauthorised access or interception of data, interference with data, and the unlawful production, sale, distribution or use of a device designed to overcome security measures for the protection of data. Chapter VIII of ECTA also deals with the protection of personal information, based on similar principles as outlined in POPIA. The *Regulation of Interception of Communications and Provision of Communication-related Information Act* (RICA) of 2002 provides for the regulation of the interception of certain communications, the monitoring of certain signals and radio frequency spectrums, and the provision of certain communication-related information.

The *Consumer Protection Act* (CPA) of 2009 regulates the consumer's right to privacy related to direct marketing, in which case the consumer has the right to refuse to accept, to require another person to discontinue, or to pre-emptively block communication. The CPA further makes provision for the establishment of the National Consumer Commission, which is responsible for resolving disputes between consumers and suppliers and enforcing compliance. The Competition Commission recognises that consumer protection law is key to addressing potential big data harm to privacy, but signals that it is an issue that extends beyond consumer protection laws (CCSA, 2020). The *Cybercrimes Act* of 2020 came into force in December 2021 and codifies and imposes penalties for the commission of cybercrimes, including the illegal interception of data and the abuse, misuse and possession of personal information where there is a reasonable suspicion that it is used in the commission of a crime. The Act further makes provision for the institutional framework to address cybersecurity, including a cyber response committee, a cybersecurity centre and a national cybercrime centre.

With many different pieces of legislation bearing on privacy, data protection and cybersecurity, conflicting outcomes may emerge that are contrary to the intentions of the legislature. For instance, the Cybercrimes Act imposes obligations on institutions to report cybercrimes, but they may not have the incentive to do so if they did not put in place the necessary precautions, since this may expose them to sanction under POPIA, which requires organisations to protect personal data.

### 3.3. Institutional Arrangements

The mandates and responsibility for open digital governance are vested in three leading ministries, while each individual ministry and related agencies in the public service leads digital transformation efforts within their respective transversal and sectoral domains.

The DPSA is responsible for establishing norms and standards relating to functioning, organisational structures, conditions of service, labour relations, information management and digital government, and transformation and innovation to improve effectiveness and efficiency in the delivery of services (DPSA, 2021). A core programme of the DPSA is that of the Government Chief Information Officer (GCIO) focusing on digital technology enablement, stakeholder, risk and service management. This function is responsible for creating an environment for the deployment of digital technology as a strategic tool of public administration. The GCIO also serves as the chairperson of the Government Information Technology Officers Council (GITOC) established in 2002. The GITOC comprises Chief Information Officers (CIOs) from national government departments and provincial government IT Officers. This is an inter-departmental forum expected to support and guide government IT and Information Management (IM) policies for operationalisation. The medium-term strategic priorities of the GITOC are spectrum, internet connectivity, reconfiguration of government departments, and progressing the implementation of the e-government strategy and roadmap (Tredger, 2021). The DPSA is in the process of operationalising the Office of Standards and Compliance to promote and monitor compliance with minimum norms and standards (DPSA, 2021). This capability can be deployed to ensure that government departments and entities adhere to digital standards related to interoperability and cybersecurity, for example.

The DCDT is mandated to lead the country's transition to the digital economy. The DCDT plays a leading role in several policy domains, including the *National Integrated ICT Policy*, the draft *Data and Cloud Policy*, and the draft *Policy Direction on 5G Spectrum*. It provides leadership in respect of the *National e-Government Strategy and Roadmap*, the *National e-Strategy*, and the *Digital and Future Skills Strategy* (and Implementation Programme). The DCDT has established various mechanisms to drive its mandate. It is currently in the process of establishing the State Digital Infrastructure Company to consolidate the state technology infrastructure, has embarked on the reconfiguration of the State Information Technology Agency (SITA) into the State Digital Services Company, established a 4IR Project Management Office (4IR PMO) to coordinate related projects nationally, and operationalised the e-Services Portal in collaboration with SITA (DCDT, 2021a). At a programmatic level, the DCDT is driving the Broadcasting Digital Migration Programme, the SA Connect Broadband Rollout, and the development and implementation of the Digital Economy Master Plan, among others.

The Department of Science and Innovation (DSI) is playing an increasingly important role in digital government, especially in respect of Big Data. The mission of the DSI is to provide leadership, an enabling environment, and resources for science, technology and innovation in support of South Africa's development. The department is currently in the process of finalising the National Big Data Strategy for Research and Development to maximise the

return on investment in research and big data (DSI, 2021). The DSI oversees key institutions that serve as nodes in the data and innovation landscape, such as the Centre for High Performance Computing (CHPC) and the Data-intensive Research Initiative of South Africa (DIRISA).

As an agency of government, SITA plays a crucial role in digital government development, with its mandate to improve service delivery to the public through the provision of information technology, information systems and related services in a maintained information systems security environment. The agency is responsible for the technical aspects of digital government enablement, including network provision, transversal data processing, interoperability and security, and procurement (SITA, 2021). SITA hosts most of the government's critical databases, such as the Department of Home Affairs' Population Register, and the financial, logistics and employee databases. SITA is in the process of rolling out the Government Private Cloud Ecosystem (GPCE) as a fundamental building block in the quest for digitalising government.

Each department assumes responsibility for the digitalisation of its services. There are several ongoing large-scale interventions in support of open digital governance by individual departments and clusters of departments. For instance, the digitalisation of civic registration services by the Department of Home Affairs is underpinned by the rollout of key digital systems as building blocks, including the National Population Register (NPR), the Home Affairs Identification System (HANIS), the Automated Fingerprint Identification System (AFIS), and the Automated Biometric Identification System (ABIS), together with the Live Capture System that supports the digitalisation of the service at the front-office (DHA, 2020a). The Integrated Justice System (IJS) comprises a cluster of departments and entities involved in the end-to-end criminal justice business processes, from the reporting of a crime to the release of a convicted person. Person and case integration, together with the establishment of a single transversal database, forms the key pillars to bring about the end-to-end digitalisation of the IJS (DoJ&CD, 2017). Eight departments and entities are connected to the IJS Transversal Hub and can exchange information in real time between the systems. This is a central messaging platform that allows each connected government department or entity to exchange information with the others.

With overlapping mandates and the level of digital government maturity varying by department, the DPSA considers the existing governance arrangements to enable digital government as "outdated owing to digital transformation and other trends" (DPSA, 2020b, p. 14). A complex digital ecosystem has evolved with an institutional landscape characterised by overlapping mandates and institutional fragmentation that has given rise to serious coordination challenges.

### **3.4. Public Sector Digital Capabilities**

In view of the critical role of the government in catalysing and implementing changes to support digital transformation, the Diagnostic Report of the Presidential Commission on the Fourth Industrial Revolution (RSA, 2020, p. 284) recognises that "human capacity development of public sector employees becomes a necessary priority focus". The report

proposes the development of stackable competencies that are micro-credentialed and enable people to enter and exit the education and training system at multiple points as part of a lifelong learning process, introducing relevant technology and devices, and digital and future skills.

The National Digital and Future Skills Strategy (RSA, 2020) recognises that digital skills development is required for civil servants, including the need for incorporating digital competencies in job descriptions and the need for continuous online learning. The Implementation Programme for the National Digital and Future Skills Strategy of South Africa, 2021–2025 (DCDT, 2021c) proposes the implementation of a combination of initiatives, including (i) the development of the technical skills required to operate, manage and sustain the digitally mediated processes of government and the underlying technological systems and databases; (ii) the growth in digital literacy with a particular focus on data management and analytics for frontline service staff; and (iii) the advancement of digital leadership skills among public service leaders and managers. The DCDT has established a Digital Skills Forum to lead, oversee and coordinate the implementation of the national digital skills programme (DCDT, no date).

### **3.5. Standards and Interoperability**

The DPSA has introduced several standards, guidelines and toolkits to promote, among other things, interoperability across the digital system of governance. This includes planning guidelines for IT (DPSA, 2002); minimum information security standards (DPSA, 2007); minimum interoperability standards (DPSA, 2017); ICT security incident management guidelines (DPSA, 2018b); ICT service continuity management guidelines (DPSA, 2018c); electronic signature guidelines (DPSA, 2019a); ICT security guidelines (DPSA, 2019b); and a directive on the usage of cloud computing services (DPSA, 2022). The DPSA plans to issue a set of public service data standards (DPSA, 2020b). The extent to which these standards and guidelines are adopted in practice and how they influence interoperability across the public service is unclear.

## **4. Case Studies**

The factors driving open digital governance are explored through the lens of two case studies, in public health and in basic education. The table below highlights some of the key issues observed in the case studies described in the next sections.

**Table 4.1: Synopsis of public health and basic education case studies**

	<b>Public Health</b>	<b>Basic Education</b>
<b>Digital Leadership</b>	<ul style="list-style-type: none"> <li>• Strong leadership by the NDoH</li> <li>• Clear strategic frameworks and successive digital health strategies providing continuity</li> </ul>	<ul style="list-style-type: none"> <li>• Characterised by multiple layers (national–provincial–district–school–parents–communities) at which leadership is required, with a significant role for Communities of Knowledge and Practice (CoKP)</li> </ul>
<b>Policy and Regulation</b>	<ul style="list-style-type: none"> <li>• Policy priorities embedded in successive frameworks, strategies and compacts</li> <li>• Implementation of National Health Insurance provides an anchor and is a key driver</li> </ul>	<ul style="list-style-type: none"> <li>• e-Education White Paper sets out strategic priorities but has not been updated</li> <li>• The Professional Development Framework for Digital Learning is an important guide and support mechanism</li> </ul>
<b>Digital Innovation</b>	<ul style="list-style-type: none"> <li>• Service digitalisation is enabled through a range of databases, systems and applications, including the Health Patient Registration System (link to HANIS), the District Health Information System (DHIS), the National Health Information Repository and Data-warehouse (NHIRD), the Centralised Chronic Medicine Dispensing and Distribution (CCMDD) system, the Stock Visibility System (SVS), MomConnect, and the Electronic Vaccination Data System (EVDS)</li> </ul>	<ul style="list-style-type: none"> <li>• Internet connectivity is available at schools, but insufficient broadband</li> <li>• Media centres and dedicated CAD classrooms, with few smart classrooms</li> <li>• 111 recommended digital learning apps on the DBE website</li> <li>• Awareness level maturity</li> </ul>
<b>Data Sharing, Privacy and Cybersecurity</b>	<ul style="list-style-type: none"> <li>• Health information is sensitive information</li> <li>• Tracing Database (Covid-19) provided serious challenges to privacy</li> <li>• Challenges in the health system remain due to, among others, network, power and system failure, and obsolete computers and operating systems</li> </ul>	<ul style="list-style-type: none"> <li>• Clear guidelines on personal data protection for learners will need to be designed</li> </ul>

## **5. Case 1: Digitalisation in Public Health Services – Accelerating Public Health**

Open digital governance is of significant importance to public health as it provides the opportunity for citizens and residents of South Africa to co-manage their own health. Co-management means that citizens and residents of the future must become able to manage their health (and their children’s health) from childhood to end of life. This will require a shift from a command-and-control public health system to a co-managed public health system, particularly at the primary healthcare level, where citizens and residents have extensive access to knowledge about health matters. In other words, public health services are not only about governmental services, but also about family health and community health management from the bottom up. This raises some levels of risk, including tech development risks, general cybersecurity risks, and specific risks for personal data protection.

South Africa faces a quadruple burden of disease consisting of HIV/AIDS and related diseases; maternal and child morbidity; lifestyle-related non-communicable diseases; and



violence, injuries and trauma (NPC, 2012). These largely contribute to the ten leading causes of death in the country (Smith & Nicol, 2020). Furthermore, the country has a two-tier health system, characterised by the high cost of care in the private sector, which caters for only 16% of the population with medical aid, and a public sector that provides healthcare to the remaining 84% of the population. One of the central tasks of successive post-apartheid governments has been to transform a dysfunctional public health system which perpetuated discrimination based on race and inequality into a more comprehensive and integrated one that provides access to care for the poorest and most marginalised (Pillay & Motsoaledi, 2018).

The potential for sharing patient information in digital form across organisational and other boundaries in ways that shift information and knowledge about care beyond single encounters between patients and the health system to a longitudinal record of care is one of the most significant drivers of the digitalisation of health services (McLoughlin, Garrety & Wilson, 2017). Patient information in digital form renders health information visible, mobile, easy to access and exchange, and able to move with the person as he or she moves around the health system. Therefore, the digitalisation of health services through the implementation of digital health information systems is regarded as one of the critical means by which to achieve integration and transformation towards a primary care-based health system, in the context of health services that were institutionally fragmented at the end of the apartheid across 14 separate health departments that prioritised the hospital sector rather than provision at the primary level (Coovadia et al., 2009).

## **5.1. Strategic Leadership**

The National Health Act, No. 61 of 2003 enjoined the national department to facilitate and coordinate the implementation and maintenance of health information systems across all levels to create a comprehensive national health information system. The ministry has been actively mobilising stakeholders through various platforms and forums. The e-Health Strategy South Africa (NDoH, 2012) provided a strategic framework to guide priorities and investment in the digitalisation of health services. The adoption of a second-generation strategy, the National Digital Health Strategy for South Africa, 2019–2024 (NDoH, 2019), reinforced the priorities set out in the first strategy. Incremental investment in digital infrastructure and systems over the past two decades, led by the NDoH, has put in place the key building blocks for the emergence of a national Health Information System (HIS).

## **5.2. Policy and Regulatory Environment**

Section 27 of the Constitution of the Republic of South Africa guarantees everyone the right to access healthcare and places obligations on the state to progressively realise affordable and quality healthcare (NDoH, 2020). The *White Paper for the Transformation of the Health System in South Africa* (NDoH, 1997) translated these obligations into a set of policy priorities. These included the restructuring of the health sector to unify the fragmented health services and reduce disparities and inequities in health service delivery, and to increase access to improved and integrated services based on primary healthcare (PHC) principles. The National Health Act provided the legal and regulatory framework for the implementation

of the identified policy priorities. These policy priorities have been embodied in the *Health Sector Strategic Framework 1999–2004*; the *Strategic Priorities for the National Health System 2004–2009*; the *10 Point Plan for 2009–2014*; and the *Presidential Health Compact* finalised in 2019.

South Africa is committed to moving the country towards the goal of Universal Health Coverage (UHC) through the implementation of National Health Insurance (NHI) to ensure citizens have access to quality healthcare services that are delivered equitably, affordably, efficiently, effectively and appropriately, based on social solidarity, progressive universalism, equity and health as a public good and a social investment (NDoH, 2017). The envisaged National Health Insurance (NHI) has made the implementation of a standardised patient-information system more urgent, given the requirement for a patient-level data platform that can support reimbursement and resource management (Nicol et al., 2021). The NHI information system will be necessary to monitor the extension of coverage in all population sectors; to track the health status of the population and production of disease profile data for use in computing capitation allocations; to support all financial and management functions; to enable planning and decision-making around contracting, purchasing and communication strategies; and to produce reports for health facilities and health system management (NDoH, 2017).

### **5.3. Standards and Interoperability**

The gazetting of the National Health Normative Standard Framework for Interoperability in e-Health (NDoH & CSIR, 2014) in April 2014 has been instrumental in articulating an interoperability framework along the journey of developing a comprehensive health enterprise architecture specification for the country (Katuu, 2016). The Health Normative Standard Framework (HNSF) facilitates interoperability between different digital health systems based on complying with standards; ensures the maintenance of digital shared registers and repositories; makes provision for appropriate security and auditing services for data integrity and security; and enables analysis for planning purposes (Health Systems Trust, 2014).

### **5.4. Systems and Applications in Health Service Digitalisation**

The NDoH approached the Council for Scientific and Industrial Research (CSIR) to develop the digital Health Patient Registration System (HPRS). The HPRS architecture consists of multi-tiered client-server architecture, incorporating (i) a client tier; (ii) a presentation tier; (iii) a business tier; and (iv) a data tier (Myllyoja et al., 2016). It serves as an online registry of all patients using healthcare services in the country, which can be accessed at any facility to provide health workers with patients' demographic information and their most up-to-date health records. It provides a Patient Registry and Master Patient Index using the South African Identity Number or other legal person identification systems to verify patient identity through an interface with the Department of Home Affairs' National Identification System (HANIS). As of March 2021, 59 million individuals were registered on the HPRS, with 3,220 PHC facilities and 52 hospitals implementing the system (NDoH, 2021). Additional systems supporting the digitalisation of health services in the public sector include the District Health

Information System (DHIS), the National Health Information Repository and Data-warehouse (NHIRD), the Centralised Chronic Medicine Dispensing and Distribution (CCMDD) system, the Stock Visibility System (SVS), and MomConnect.

The Electronic Vaccination Data System (EVDS) was launched by the NDoH in April 2021 to manage multiple aspects of the national vaccination rollout by keeping track of the vaccination process, including vaccine stocks, adverse events reported, and the tracking of whether vaccines are paid for by the state or private medical aids (Ownings, 2021). The main interface of the system is a public-facing registration portal and communication is conducted through SMS. Updates to the system are undertaken by a private company that is a subsidiary to one of the largest telecommunications providers in the country. The work of the service provider is supported by the CSIR, which is responsible for the management of system data using the NHI data centre at its location. The rollout of the EDVS was enabled by the digital backbone of the NHI developed over the past several years and has expanded the capabilities of the HPRS platform. The NDoH is the owner of the data and is responsible for the data protection and governance policies in line with the relevant legislative requirements (SAMRC, 2021).

## **5.5. Data Sharing, Privacy and Cybersecurity**

Health data is regarded as “sensitive” personal data, given the nature and influence of such data on the lives of people and on fundamental rights such as privacy (Townsend, 2022). South Africa launched a COVID-19 Tracing Database in April 2020 to enable the tracing of people who had come into contact with a person with COVID-19. The tracing was undertaken through the collection of mobile phone data to identify and locate individuals, and posed a serious risk to the constitutional right to privacy. One of the features of the Tracing Database was the establishment of a COVID-19 Judge who received weekly reports from mobile phone operators with authorisation to give directions on further steps to be taken to protect the right to privacy of those persons whose data had been collected (Klaaren et al., 2020). This occurred in addition to the requirements that the data could only be used for the purposes for which it was collected and could not be retained beyond a period of six weeks, after which it had to be de-identified. Nevertheless, ethical concerns arose about the balancing of privacy protection against the need to fight a public health crisis. Moreover, the Tracing Database gave rise to concerns about the production of a real-time government surveillance database (Klaaren et al., 2020). Research also suggests that privacy and data security in public hospitals remain a concern. Public hospitals continue to face significant cybersecurity threats arising from technological vulnerabilities such as poor networks, power and system failure, obsolete computers and operating systems, and outdated hospital systems, despite having in place policy and regulatory frameworks and security measures that include encryption and firewalls (Chuma & Ngoepe, 2021).

## **6. Case 2: Digital Transformation in Basic Education – Collaborative Engagement of Role Players**

The rationale for the focus on digitalisation in basic education is that this is the space where the open digital governance of the future will be built, or not be built. This case study reviews

key events in the transition to digitally-enabled education in public ordinary schools in South Africa and considers the gaps in current e-education practice from the perspective of open digital governance.

There are many challenges to getting the system of digital enablement working for schools. Challenges include the limited quality of infrastructure access, limited access to and knowledge of educational applications, limited access to and knowledge of information about digital pedagogy, and limited opportunities to learn and experience the use of digital technologies in schools. Hence, this is an important frontier of public service digitalisation, because it is the only space in which future generations of young South Africans can become digitally literate, in all subjects, in preparation for post-school education, the world of work and civic engagement. Civic engagement includes voting, engagement with local, provincial and national governments and their entities, and engagement in the communities within which South Africans reside. While middle- and high-income households may have the levels of disposable income that can enable them to acquire the digital skills and capacities needed to engage in open digital governance, this is not the case for millions of young South Africans aged 7 to 18. Therefore, digitally-enabled education and digital literacy at school is essential for fostering an inclusive, participative future democracy, in other words, open digital governance. Yet, the resources and capacities required to prepare young learners are often lacking.

### **6.1. Systems Applications in Education: Making the Case for Communities of Knowledge and Practice (CoKPS)**

An appropriate starting point for this case study is the recognition that learner performance in South Africa is weak in language, maths and science (and other subjects). The TIMSS score for mathematics achievement for Grade 9 learners in 2019 was 389, well below the TIMSS scale centrepoint of 500 and the score of case study country Malaysia at 461. The TIMSS score for science achievement for Grade 9 learners in 2019 was 370, also below the TIMSS scale centrepoint of 500 and the score of the case study country Malaysia at 460 (Reddy et al., 2019, p. 3). Poor learner performance is often due to the fact that schools are poorly resourced in terms of the high learner-to-teacher ratio, small classrooms, limited access to high quality learning materials and resources, and poor socio-economic conditions with respect to household income and assets. This reality can be extrapolated to a future where large numbers of young school leavers increase the ranks of youth-not-in-employment-education-or-training (YNEET) and where they do not participate in civic activities or in the governance of the country. While the digital enablement of schools is not the only possible approach to building the capacity to participate in future governance, and while it is not a panacea for the many resource challenges that schools face, there is a case to be made that promoting digitally-enabled learning in schools can make a difference, even if not all the difference needed.

Many South African schools now have Internet, but insufficient broadband connectivity. Many schools have computer laboratories which are used for the subject Computer Applications Technology (CAT), offered from Grade 10 to Grade 12, but many of these labs cannot be used for more general e-learning purposes. Few schools have media centres.




Schools that do have media centres may not yet have a media centre programme, in other words, a media centre design that means that a class or a group(s) from a class can use the media centre for learning periods throughout the day.

The National Education Infrastructure Management System (NEIMS) report for April 2021 (DBE, 2021) indicates that 4,738 schools out of a total of 23,276 schools had Internet connectivity for teaching and learning (Table 11), while 7,676 schools or 41,8% of schools had a computer centre (Table 9) and 5,444 schools or 30,4% of schools had a library (Table 7). It is not known whether there are computers in school libraries and, if so, how many. Many schools, in many provinces, have provided digital tablets to learners. The relatively small number of smart classrooms in each province typically include resources such as interactive whiteboards, laptops, data projectors, and eBeams, which project images from physical objects, as well as digital tablets for learners and tablet charging trolleys. It is possible to say, based on the annual NEIMS reports, that there is a digital divide in ordinary operational schools.

The Department of Basic Education (DBE) currently recommends (from circa 2014) 111 digitally-enabled learning applications, across multiple subjects and multiple grades, to teachers. See, for example, the language learning apps listed in Figure 6.1 below, and also see

[https://www.education.gov.za/Portals/0/Documents/Publications/app\\_store\\_bundle%2014%20sept%20version/app\\_store\\_bundle/index.html?ver=2016-09-14-111840-000](https://www.education.gov.za/Portals/0/Documents/Publications/app_store_bundle%2014%20sept%20version/app_store_bundle/index.html?ver=2016-09-14-111840-000)

**Figure 6.1 DBE app store bundle: Recommended apps**

Languages					
	Multiple Languages	R, 1-3 (5-7+ years)	Language: English and 40 others	Listening, speaking, viewing and reading	+
	English First Additional Language	R, 1-3 (5-7+ years)	Language: English Home and First Additional	Listening, speaking, viewing and reading, phonics	+
	English First Additional Language	R, 1-3 (5-7+years)	Language: English Home and First Additional	Listening, reading and viewing	+
	English home language	10 - 12	Vocabulary		+
	English First Additional Language	R, 1-3 (5-7+years)	Language: English Home and First Additional	More than CAPS	+
	English	10 - 12			+
	EFAL	12	All	All	+
	English Language Literature	7-12			+

Source: DBE (no date)

This represents the beginnings of open digital governance at the national education level, where extensive information is made available to a particular community, in this case to teachers and learners, school management and education administrators, researchers and the general public. Two challenges arise: (i) the information and the learning apps are not always easy to access and download; and (ii) the capacity of teachers to effectively and progressively utilise the materials presents a challenge, partly because it takes a significant amount of time, initially, to select and consistently apply resources to specific components of the curriculum.

The DBE's schools' digital readiness policy brief (Van Greunen et al., 2021) provides a useful, though incomplete, picture of areas and indicators for ICT maturity in schools. It illustrates five critical dimensions of maturity (leadership and vision, ICT in learning and teaching, development of digital competencies, ICT culture, ICT resources and infrastructure). Additional indicators should include: (i) knowledge of digital pedagogy and instructional design; (ii) utilisation of dynamic software by teachers and learners; (iii) cybersecurity and personal data protection; (iv) communities of educational knowledge and practice; and (v) open digital governance for schools. The latter point is of particular importance because schools do want parents to participate in the learner management and school management processes, but formal meetings at inconvenient times and places have been the only means used so far.

**Figure 6.2: Applying maturity levels design thinking to ICT in schools**

**Table 1: Areas and indicators of the ICT Maturity of schools**

Area	Indicators
Leadership and Vision	<ul style="list-style-type: none"> <li>Vision, strategic guidelines and objectives of ICT integration</li> <li>Plan and programme of school development from the perspective of ICT</li> <li>Managing the integration of ICT in learning and teaching</li> <li>Managing the integration of ICT the school's business activities</li> <li>Managing data collected by means of information systems</li> <li>Regulated access to ICT resources</li> <li>Use of ICT in teaching students with special educational needs</li> </ul>
ICT in learning and teaching	<ul style="list-style-type: none"> <li>Awareness</li> <li>Planning</li> <li>Use</li> <li>Digital content</li> <li>Evaluation of students</li> <li>Students' experience</li> <li>Special educational needs</li> </ul>
Development of digital competencies	<ul style="list-style-type: none"> <li>Awareness and participation</li> <li>Planning</li> <li>Purpose of professional training</li> <li>Self-confidence in the use of ICT</li> <li>Digital competencies of students</li> <li>Digital competencies of educators</li> <li>Professional Development</li> <li>Informal learning</li> </ul>
ICT culture	<ul style="list-style-type: none"> <li>Access to ICT resources by educational staff</li> <li>Access to ICT resources by students</li> <li>Network presence</li> <li>Communication, information and reporting</li> <li>Netiquette</li> <li>Copyright and intellectual property</li> <li>Projects</li> </ul>
ICT resources and infrastructure	<ul style="list-style-type: none"> <li>Planning and procurement</li> <li>Network infrastructure</li> <li>ICT equipment in the school</li> <li>ICT equipment for educational staff</li> <li>Programme tools in schools</li> <li>Connectivity</li> <li>Technical support</li> <li>Equipment maintenance</li> <li>Central repository of digital documents and educational content</li> <li>Information security system and licensing control</li> </ul>

Source: Van Greunen et al. (2021)

The maturity level descriptors used are digitally unaware (level 1), digital beginner (level 2), digitally competent (level 3), digitally advanced (level 4) and digitally mature (level 5). Based on a self-assessment across 5,199 schools, the Van Greunen (2021) study found that the majority of schools considered themselves to be digitally competent, interpreted as an awareness of the role of digital technologies and an unspecified level of digital competency. In concluding, the authors state that “[t]he ICT readiness maturity levels and the extent to which schools and educators learn and improve their ICT readiness capabilities are largely unknown. The findings of the pilot study indicate that while some schools are at a maturity level of awareness and understanding, they have not reached the stage where ICT readiness and the use of digital technologies are entrenched in their schools and the learning and teaching processes.” This study indicates that schools have a long way to go to create and achieve open digital governance, and that awareness and understanding of approaches to open digital governance in schools may be limited or non-existent. This is an opportunity for the public service, and an opportunity that must be seized.

## **6.2. Digital Leadership for Open Digital Governance in Basic Education**

It is noted that open digital governance needs a foundation on which to evolve. In the schools’ context, this foundation is the transition to digitally-enabled teaching and learning. Where that foundation is weak or does not exist, it will be difficult or impossible to build open digitally-enabled governance.

Multiple layers of open digital governance will need to be established and strengthened at schools’ level, including: (i) the relationship between national government and schools with respect to decision-making on policy and practice for digitally-enabled teaching and learning; (ii) the relationship between provincial and district level education administrators and schools with respect to improving the quality of basic education, and learner performance in assessments; (iii) the relationship between parents/communities and school governing bodies with respect to school management and learner benefit; and (iv) the relationships of teachers with each other and with learners. While all these are matters of importance with respect to enhancing education governance for improved outcomes, it is noted that the relationships of teachers with each other and of teachers with learners can be significantly advanced by adopting a “communities of knowledge and practice (CoKP)” approach, where learning communities are formed, using digital tools and online platforms to create subject-based communities (eg. language learning community of practice) and knowledge-based communities (eg. all subjects using maths, including maths, physics and business studies).

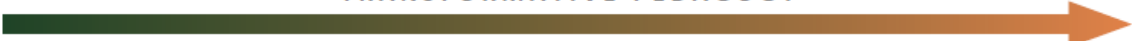
The key points at which open digital governance in basic education can begin to occur are the point at which schools are governed by education districts, and the point at which schools are governed by their governing bodies. Key role players in education districts are the subject advisors, who are responsible for, amongst other things, guidance on curriculum and assessments. Subject advisors have a major role to play in facilitating the adoption of the 111 digital applications recommended by the DBE; however, they can only do this if they have the requisite knowledge and capabilities and if the schools can access the content. Where subject advisors have the knowledge and capabilities, they can create open lines of communication, enabled by basic mobile messaging technologies, to engage in interactive

communities of knowledge and practice with teachers, enabling the adoption and utilisation of apps, and also hearing the particular challenges, needs and ideas of teachers. This form of approach would shift the governance interaction from bureaucratic to developmental. On the second point, engagement between the school, its governing body and its community of parents can be enhanced by introducing basic digital messaging applications, laying the early foundations for more advanced forms of digitally-enabled governance.

### 6.3. Policy and Regulatory Environment for Schools: New Operating Guidelines, Data Sharing and Cybersecurity

Key milestones in fostering digitally-enabled education include the adoption of the e-Education White Paper in 2004 (<https://www.education.gov.za/Resources/Legislation/WhitePapers.aspx>) and the publication of the Professional Development Framework for Digital Learning in 2017 (<http://www.schoolnet.org.za/wp-content/uploads/2017-12-01-Professional-Development-Framework-for-Digital-Learning-Final.pdf>). The framework translates ideas about 21st century skills and the SAMR model into a meaningful presentation for teachers and subject advisors. These important role players now need to embed the thinking enshrined in the operational guidelines presented in the digital learning framework, which shifts the focus from simply teaching to transformative pedagogy.

**Figure 6.3 Enabling transformative pedagogy**

<b>Regulation</b>			
Teacher dominates; Learners are passive (e.g. not interacting, writing notes).	Less than 50% of lesson time is learner-centred activity. Mix of individual and group work.	Learners are engaged in individual and/or group work for more than 50% of time. Activities are learner-centred.	Learners mostly engage in collaborative, self-directed and self-regulated activities; teacher facilitates learning.
<b>Information transformation</b>			
Information is presented only by the teacher verbally or in writing.	Information is gathered and processed in simple ways by learners. It is sometimes copied and pasted and not always re-stated in original words.	Information is gathered and transformed – used for skills such as analysis and evaluation and as the basis for drawing conclusions. Activities are confined to the classroom.	Knowledge is constructed by learners and applied in real life scenarios, often in collaboration with the community. Content is created/published for authentic audiences.
<b>Interactions and deep learning (Anderson)</b>			
Limited interaction – mostly one-way transfer of information by the teacher. Some teacher feedback to learners and possible learner self-study of digital content.	Teacher-class, teacher-learner (feedback and discussion) interaction. Some learner-learner interaction.	Learner-learner interaction (communication/feedback)  Learner(s) and teacher in dialogue. Learners engage independently with content.	Full range of interactions at deep level. Learner-learner interaction (collaboration dominant). Learner(s) – teacher in dialogue with each ther.
<b>TRANSFORMATIVE PEDAGOGY</b>			
			

Source: DBE (2017)



The Professional Development Framework for Digital Learning is a comprehensive guide for subject advisors and teachers, incorporating models for thinking and practice, explanations, a set of proposed minimum requirements, a lesson analysis checklist, and a diagnostic self-assessment tool for teachers.

Schools have historically been, and still are, highly regulated environments with very limited room for flexibility in learning and teaching. Teachers generally follow the textbook, rather than the curriculum, meaning that teachers generally only teach the content made available in the textbook, as they have had limited access to the knowledge resources required for creatively finding material relevant to the curriculum. Will this change fast enough? It took approximately 14 years for an initial set of clear guidelines for teachers, schools and subject advisors to be published. The process of adopting these guidelines needs to be hastened, with the scarce resource of time being used as effectively as possible to make the transition required.

Another major regulatory focus for schools relates to the digitalisation of learning activities and of learner data, which requires attention to personal data protection and cybersecurity. Very limited observation suggests that learners do not necessarily want to be on Facebook and other social media for learning purposes. They may prefer discrete, “membership-only” forms of learning media that can be restricted and managed by the school. Whichever mode of interaction is preferred, learners (and possibly their parents) would need to give informed consent for data to be shared in any public online space. Here too lies an opportunity for public service innovation, relevant to open digital governance, in the sense that clear guidelines on personal data protection for learners will need to be designed, with reference to POPIA. Similarly, a cybersecurity risk analysis for schools can be performed and updated on an ongoing basis. Personal data protection, cyber awareness and cybersecurity risk management must go hand in hand with the process of transitioning to digitally-enabled learning, and to open digital governance in schools.

## **7. Key Challenges**

The fragmented and dispersed nature of open digital governance leadership and policy coordination, characterised by discontinuity and change at the ministerial level, is a significant hindrance to the realisation of policy goals and outcomes. Several institutions play a role in exercising leadership for digital government, but the governance arrangements and structures that must ensure effective coordination do not work effectively (DPSA, 2021). Development of the requisite capacity to lead and manage the complex digital ecosystem remains a major area of concern and limits the extent to which leadership capability can be exercised.

The legislative and regulatory environment relevant to open digital governance, together with the institutions established to enforce regulations, is characterised by the development of piecemeal legislation, whereas a coherent and integrated data governance regulatory framework is required that addresses privacy, data protection and cybersecurity (NPC, 2020).

The explicit focus on data as a national resource is only now emerging in South Africa. This means that the development of the necessary institutional capacities to harness and exploit the benefits arising from the availability, processing and usage of data will take time to realise. Investments in developing the country's data capabilities need to be accelerated, including the policy positions on questions such as data sovereignty and the regulation of digital and data markets.

These factors are exacerbated by the digital divide in South Africa, with its access, geographic and demographic dimensions. Half of South Africa's population remains offline with a lack of Internet-enabled devices, with digital literacy and data prices constituting key barriers to closing the divide (Gillwald et al., 2018). Trust in government, a key enabler for open digital governance, has been in decline for several years with less than 50% of citizens having trust in state institutions (DPME, 2021).

## 8. Priorities to Unlock and Accelerate Open Digital Government

Circling back to the five overarching insights, the following closing thoughts are offered:

**A powerful sense of mission:** Open innovation and collaborative creation (co-creation) need to be interlinked in the process of establishing and strengthening open digital governance. Public servants, both generalists and specialists (teachers, health workers, front-line workers and others), need to expand their knowledge of the forms of constructive engagement that can be supported by digital technologies. More importantly, they will need to be the originators and sponsors of practices of open digital governance, some of which are alluded to in the six case studies in the South African and international experience papers for the SA–EU dialogue.

**Digital-first:** The six cases presented in the South African and international experience papers (accelerating health benefits, collaborative engagement of role players, digital identity, platform government, digital bilingualism and 21st century skills, partnering with tech hubs) all indicate that a strong mission orientation is needed. Rapid incrementalism is more desirable than a “big bang” approach. Indeed, a big bang approach is not possible. But a key lesson is that slowness and ineffectiveness have a high negative impact on development. The mindset for building open digital governance must be a mindset of asking and reflecting on how digital tools, processes and approaches can address or solve old intransigent problems, and new problems, and then innovating to produce the desired outcomes.

**Human capability for 21st century public service governance:** While many skills and capabilities are required for establishing and nurturing open digital governance, the case studies suggest that digital leadership is one of the most important capabilities, and collaborative governance is another. The levels of complexity in public service institutional environments cannot be managed by public servants working in isolation from the public that they serve. This is already widely recognised, but it must become part of everyday citizen–government interaction.

**Legislation, regulation and standards that encourage innovation:** The traditional approach to regulation is that regulation creates the frame for operation. This approach constrains innovation. The public service can move to a new reality where innovation influences the kinds of necessary regulation that would benefit the problem being addressed.

**Future orientation:** Public service innovation cannot be effected in a stop–start fashion. Therefore, open digital governance cannot be strengthened in a stop–start fashion. For the public service to adopt a future-oriented culture and practice, public service leaders will need to place innovation at the centre of their mission. This will require consistency in always looking to the “next future”, the future beyond the horizon, which we need to continually develop.

## References

- Amoore, L., & Piotukh, V. (2016). Introduction. In L. Amoore, & V. Piotukh (Eds.), *Algorithmic life: Calculative devices in the age of big data* (pp. 1–19). Routledge.
- Auditor-General South Africa. (2008). *Report of the Auditor-General to Parliament on information systems audits conducted regarding the electronic National Traffic Information Systems*. <https://static.pmg.org.za/docs/080611agsa.pdf>
- Berry, D. M. (2014). *Critical theory and the digital*. Bloomsbury Publishing Inc.
- Breckenridge, K. (2005). The biometric state: The promise and peril of digital government in the new South Africa. *Journal of Southern African Studies*, 31(2), 267–282. <http://doi.org/10.1080/03057070500109458>
- Carreira, P., & Mtshali, S. (2019). The SARS innovation journey. Version 2. Presentation at the 13<sup>th</sup> Annual Public Sector Innovation Conference on 28 and 29 November 2019. <http://cpsiregistrations.co.za/wp-content/uploads/2019/11/20191128-The-SARS-Innovation-Journey-13th-Government-Innovation-Conference-V2.pdf>
- Chuma, K., & Ngoepe, M. (2021). Security of electronic personal health information in a public hospital in South Africa. *Information Security Journal: A Global Perspective*, 31(2), 179–195. <http://doi.org/10.1080/19393555.2021.1893410>
- Cloete, F. (2003). *Strategic management support technologies in the public sector*. SUN ePress. [https://www.academia.edu/47152436/Strategic\\_Management\\_Support\\_Technologies\\_in\\_the\\_Public\\_Sector](https://www.academia.edu/47152436/Strategic_Management_Support_Technologies_in_the_Public_Sector)
- Competition Commission South Africa (CCSA). (2020). *Competition in the digital economy*. Report for public comment. <https://www.compcom.co.za/wp-content/uploads/2020/10/Competition-in-the-Digital-Economy-Report-7-September-2020.pdf>
- Cohen, J. E. (2015). The networked self in the modulated society. In W. de Been, P. Arora, & M. Hildebrandt (Eds.). *Crossroads in new media, identity and law: The shape of diversity to come* (pp. 67–79). Palgrave Macmillan.
- Coovadia, H., Jewkes, R., Barron, P., Sanders, D. & McIntyre, D. (2009). The health and health system of South Africa: Historical roots of current public health challenges. *The Lancet*, 374, 817–834. [https://doi.org/10.1016/S0140-6736\(09\)60951-X](https://doi.org/10.1016/S0140-6736(09)60951-X)
- Department of Basic Education (DBE). (no date). App store bundle. [https://www.education.gov.za/Portals/0/Documents/Publications/app\\_store\\_bundle%2014%20sept%20version/app\\_store\\_bundle/index.html?ver=2016-09-14-111840-000](https://www.education.gov.za/Portals/0/Documents/Publications/app_store_bundle%2014%20sept%20version/app_store_bundle/index.html?ver=2016-09-14-111840-000)

Department of Basic Education (DBE). (2004). *White paper on e-education: Transforming learning and teaching through information and communication technologies.*

<https://www.education.gov.za/Resources/Legislation/WhitePapers.aspx>

Department of Basic Education (DBE). (2017). *Professional development framework for digital learning.*

<http://www.schoolnet.org.za/wp-content/uploads/2017-12-01-Professional-Development-Framework-for-Digital-Learning-Final.pdf>

Department of Basic Education (DBE). (2021, April). *National education infrastructure management system report as at 12 April 2021.*

<https://www.education.gov.za/Resources/Reports.aspx>

Department of Justice and Constitutional Development (DoJ&CD). (2017). *Progress report: Integrated Justice System (IJS) programme.* Progress report to the Select Committee on Security and Justice. <https://static.pmg.org.za/170531IJSReport.pdf>

Department of Communications and Digital Technologies (DCDT). (no date). *Digital skills forum terms of reference.*

[http://www.digitalcouncil.africa/docs/Digital\\_Skills\\_Forum\\_Draft%20Terms%20of%20Reference\\_2021.pdf](http://www.digitalcouncil.africa/docs/Digital_Skills_Forum_Draft%20Terms%20of%20Reference_2021.pdf)

Department of Communication and Digital Technology (DCDT). (2021a) *Annual report 2020/21.* <https://www.dcdt.gov.za/documents/annual-reports/file/190-annual-report-2020-2021.html>

Department of Communications and Digital Transformation (DCDT). (2021b). *Draft national policy on data and cloud.*

[https://www.gov.za/sites/default/files/gcis\\_document/202104/44389gon206.pdf](https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf)

Department of Communications and Digital Technologies (DCDT). (2021c). *Implementation programme for the national digital and future skills strategy of South Africa, 2021–2025.*

[https://www.gov.za/sites/default/files/gcis\\_document/202203/digital-and-future-skillsimplementation-programmefinal.pdf](https://www.gov.za/sites/default/files/gcis_document/202203/digital-and-future-skillsimplementation-programmefinal.pdf)

Department of Telecommunications and Postal Services (DTPS). (2017). *National e-government strategy and roadmap.*

[https://www.gov.za/sites/default/files/gcis\\_document/201711/41241gen886.pdf](https://www.gov.za/sites/default/files/gcis_document/201711/41241gen886.pdf)

Department of Science and Innovation (DSI). (2021). *Annual report 2020–2021 financial year.* [https://www.dst.gov.za/images/2021/Annual\\_Report\\_2020-2021.pdf](https://www.dst.gov.za/images/2021/Annual_Report_2020-2021.pdf)

Department of Home Affairs (DHA) (2020a). *Automated biometric identification system (ABIS).* Presentation to the Portfolio Committee on Home Affairs.

[https://pmg.org.za/files/200602PRESENTATION\\_TO\\_THE\\_PC\\_ON\\_ABIS.pptx](https://pmg.org.za/files/200602PRESENTATION_TO_THE_PC_ON_ABIS.pptx)

Department of Home Affairs (DHA). (2020b). *Draft official identity management policy*. Public consultation version.

[https://www.gov.za/sites/default/files/gcis\\_document/202101/44048gon1425.pdf](https://www.gov.za/sites/default/files/gcis_document/202101/44048gon1425.pdf)

Department of Home Affairs (DHA). (2021, May 25). *Nexia SAB&T investigation*.

Presentation to the Portfolio Committee on Home Affairs.

[https://pmg.org.za/files/210525FinalPC\\_DHAPresentation\\_for\\_DG\\_1.pptx.with\\_input\\_on\\_condonation.pptx](https://pmg.org.za/files/210525FinalPC_DHAPresentation_for_DG_1.pptx.with_input_on_condonation.pptx)

Department of Planning, Monitoring and Evaluation (DPME). (2021). *Trust in government*. Policy brief.

[https://www.dpme.gov.za/publications/research/Documents/2021\\_DPME\\_Policy%20Brief\\_Trust%20in%20Government.pdf](https://www.dpme.gov.za/publications/research/Documents/2021_DPME_Policy%20Brief_Trust%20in%20Government.pdf)

Department of Public Service and Administration (DPSA). (no date). *Open Government Partnership: South Africa: Department of Public Service and Administration (ZA0021)*.

<https://www.opengovpartnership.org/members/south-africa/commitments/ZA0021/>

Department of Public Service and Administration (DPSA). (1997). *White paper on transforming public service delivery (Batho Pele)*.

[https://www.gov.za/sites/default/files/gcis\\_document/201409/183401.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/183401.pdf)

Department of Public Service and Administration (DPSA). (2001). *Electronic government, The digital future. A public service IT policy framework*.

[https://www.gov.za/sites/default/files/gcis\\_document/201409/it0.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/it0.pdf)

Department of Public Service and Administration (DPSA). (2002). *Information technology planning guidelines South African Government year 2002*.

<https://www.dpsa.gov.za/dpsa2g/documents//ogcio/2007/Adopted%20IT%20Plan%20Guideline%20Rev%202.1%2002-11-19.pdf>

Department of Public Service and Administration (DPSA). (2003). *The machinery of government: Structures and functions of government*.

<http://www.dpsa.gov.za/dpsa2g/documents/lkm/mog.pdf>

Department of Public Service and Administration (DPSA). (2006). *Policy on free and open-source software use for South African government*.

[https://www.gov.za/sites/default/files/gcis\\_document/201409/fosspolicy0.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/fosspolicy0.pdf)

Department of Public Service and Administration (DPSA). (2007). *Minimum information security standards*. <https://www.dpsa.gov.za/dpsa2g/documents//ogcio/2007/miss.pdf>

Department of Public Service and Administration (DPSA). (2017). *Minimum interoperability standards (MIOS) framework for government information systems*. Revision 6.0.

<https://www.dpsa.gov.za/dpsa2g/documents//egov/2018/MIOS%20V6.0%20SIGNED.pdf>

Department of Public Service and Administration (DPSA). (2018a, May). *Integrated Financial Management System* [PowerPoint slides]. Presentation by DPSA, National Treasury and SITA to the Portfolio Committee on Public Service and Administration/Planning, Monitoring and Evaluation. <https://pmg.org.za/file/180523IFMS.ppt>

Department of Public Service and Administration (DPSA). (2018b). *ICT security incident management guidelines*. Version 1.2. <https://www.dpsa.gov.za/dpsa2g/documents//egov/2018/Public%20Service%20ICT%20Security%20Incident%20Management%20Guidelines.pdf>

Department of Public Service and Administration (DPSA). (2018c). *Information and communication technology service continuity management sub-guidelines*. Version 0.1. [https://www.dpsa.gov.za/dpsa2g/documents//egov/2018/ogcio\\_19\\_01\\_2018\\_Guidelines.pdf](https://www.dpsa.gov.za/dpsa2g/documents//egov/2018/ogcio_19_01_2018_Guidelines.pdf)

Department of Public Service and Administration (DPSA). (2019a). *Electronic signature guidelines*. <https://www.dpsa.gov.za/dpsa2g/documents//egov/2019/Electronic%20Signature%20Guidelines%20for%20the%20Public%20Service%20%20final.pdf>

Department of Public Service and Administration (DPSA). (2019b). *Information and communication technology security guidelines*. Version 1. [https://www.dpsa.gov.za/dpsa2g/documents//egov/2017/ogcio\\_02\\_06\\_2017\\_Guidelines.pdf](https://www.dpsa.gov.za/dpsa2g/documents//egov/2017/ogcio_02_06_2017_Guidelines.pdf)

Department of Public Service and Administration (DPSA). (2020a). *Portfolio Committee presentation on e-government plan and implementation to digitalise the public service*. Presentation to the Public Service and Administration, Performance Monitoring and Evaluation Portfolio Committee. [https://pmg.org.za/files/200826e-GOVERNMENT\\_STRATEGY\\_AND\\_IMPLEMENTATION\\_PLAN\\_08142020\\_pptx\\_ver2.pptx](https://pmg.org.za/files/200826e-GOVERNMENT_STRATEGY_AND_IMPLEMENTATION_PLAN_08142020_pptx_ver2.pptx)

Department of Public Service and Administration (DPSA). (2020b). *Strategic Plan 2020–2025*. <https://www.dpsa.gov.za/dpsa2g/documents/institutional/2020-2025%20DPSA%20Strategic%20Plan.pdf>

Department of Public Service and Administration (DPSA). (2021). *2020/2021 annual report*. <https://www.dpsa.gov.za/dpsa2g/documents/institutional/DPSA%20ANNUAL%20REPORT%202020-2021.pdf>

Department of Public Service and Administration (DPSA). (2022). *Determination and directive on the usage of cloud computing services in the public services*. [https://www.dpsa.gov.za/dpsa2g/documents/egov/2022/egovernment\\_02\\_02\\_2022.pdf](https://www.dpsa.gov.za/dpsa2g/documents/egov/2022/egovernment_02_02_2022.pdf)

- Department of Telecommunications & Postal Services (DTPS). (2016). *National Integrated ICT Policy White Paper*.  
[https://www.dtps.gov.za/images/phocagallery/Popular\\_Topic\\_Pictures/National\\_Integrated\\_ICT\\_Policy\\_White.pdf](https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/National_Integrated_ICT_Policy_White.pdf)
- Edwards, P., & Hecht, G. (2010). History and the technopolitics of identity: The case of apartheid South Africa. *Journal of Southern African Studies*, 36(3), 619–639.  
<https://www.jstor.org/stable/20790048>
- Ensor, L. (2021, October 5). Finance management system project sullies Treasury's audit report. *Business Day*. <https://www.businesslive.co.za/bd/national/2021-10-05-finance-management-system-project-sullies-treasurys-audit-report/>
- Garrib, A., Stoop, N., McKenzie, A., Dlamini, L., Govender, T., Rohde, J., & Herbst, K. (2008). An evaluation of the District Health Information System in rural South Africa. *South African Medical Journal*, 98(7), 549–552.  
[http://www.scielo.org.za/scielo.php?script=sci\\_arttext&pid=S0256-95742008000700027](http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S0256-95742008000700027)
- Gillwald, A., Mothobi, O., & Rademan, B. (2018). *The state of ICT in South Africa*. [https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report\\_04.pdf](https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf)
- Health Systems Trust. (2014). South African health review 2014/15.  
[https://www.hst.org.za/publications/South%20African%20Health%20Reviews/Complete\\_SAHR\\_2014\\_15.pdf](https://www.hst.org.za/publications/South%20African%20Health%20Reviews/Complete_SAHR_2014_15.pdf)
- Information Regulator. (2021). *Annual performance plan 2020/21*.  
<https://www.inforegulator.org.za/docs/pptr/InfoRegSA-2021-2022-APP.pdf>
- Klaaren, J., Breckenridge, K., Cachalia, F., Fonn, S., & Veller, M. (2020). South Africa's COVID-19 tracing database: Risks and rewards of which doctors should be aware. *South African Medical Journal*, 110(7), 617–620.  
<https://doi.org/10.7196/SAMJ.2020.v110i7.14852>
- Leonard, R. (1978). *Computers in South Africa: A survey of US companies*. New York: The Africa Fund.
- Lindgren, I., & Jansson, G. (2013). Electronic services in the public sector: A conceptual framework. *Government Information Quarterly*, 30(2), 163–172.  
<https://doi.org/10.1016/j.giq.2012.10.005>
- Lindgren, I., Madsen, C., Hofmann, S., & Melin, U. (2019). Close encounters of the digital kind: A research agenda for the digitalization of public services. *Government Information Quarterly*, 36(3), 427–436. <https://doi.org/10.1016/j.giq.2019.03.002>



- Lindner, R., & Aichholzer, G. (2020). E-Democracy: Conceptual foundations and recent trends. In L. Hennen, I. van Keulen, I. Korthagen, G. Aichholzer, R. Lindner & R. Øjvind Nielsen (Eds.), *European e-democracy in practice* (pp. 11–45). Springer.  
<https://doi.org/10.1007/978-3-030-27184-8>
- Lips, M., Taylor, J., & Organ, J. (2009). Identity management, administrative sorting and citizenship in new modes of government. *Information, Communication & Society*, 12(5), 715–734. <https://doi.org/10.1080/13691180802549508>
- McLoughlin, I., Garrety, K., & Wilson, R. (2017). *The digitalisation of healthcare*. Oxford: Oxford University Press.
- Myllyoja, J., Toivanen, H., Herselman, M., Botha, A., Alberts, R., & Fogwill, T. (2016). *Conceptualising of a South African digital health innovation ecosystem*. Technical report. CSIR.
- NARMIC. (1984). *Automating apartheid: U.S. computer exports to South Africa and the arms embargo*. American Friends Service Committee, USA.
- National Department of Health (NdoH). (1997). *White paper for the transformation of the health system in South Africa*.  
[https://www.gov.za/sites/default/files/gcis\\_document/201409/17910gen6670.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/17910gen6670.pdf)
- National Department of Health (NDoH). (2012). *eHealth strategy South Africa*.  
<https://www.knowledgehub.org.za/system/files/elibdownloads/2019-07/South%2520Africa%2520eHealth%2520Strategy%25202012-2017.pdf>
- National Department of Health (NdoH). (2017). *National health insurance policy*.  
[https://www.gov.za/sites/default/files/gcis\\_document/201707/40955gon627.pdf](https://www.gov.za/sites/default/files/gcis_document/201707/40955gon627.pdf)
- National Department of Health (NDoH). (2019). *National digital health strategy for South Africa, 2019–2024*. <https://www.health.gov.za/wp-content/uploads/2020/11/national-digital-strategy-for-south-africa-2019-2024-b.pdf>
- National Department of Health (NdoH). (2020). *Strategic plan 2020/21–2024/25*.  
<https://www.health.gov.za/wp-content/uploads/2020/11/depthealthstrategicplanfinal2020-21to2024-25-1.pdf>
- National Department of Health (NDoH). (2021). *Annual report 2020/21*.  
<https://www.health.gov.za/wp-content/uploads/2021/11/Annual-Report-2020-2021.pdf>
- National Department of Health (NDoH) and Council for Scientific and Industrial Research (CSIR). (2014). *National health normative standard framework for interoperability in e-health*. <https://www.colleaga.org/sites/default/files/attachments/hnsf-complete-version%201.pdf>

- National Planning Commission (NPC). (2012). *National development plan 2030*.  
[https://www.gov.za/sites/default/files/gcis\\_document/201409/ndp-2030-our-future-make-it-workr.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/ndp-2030-our-future-make-it-workr.pdf)
- National Planning Commission (NPC). (2020). *Digital futures: South Africa's readiness for the Fourth Industrial Revolution*.  
<https://www.nationalplanningcommission.org.za/assets/Documents/DIGITAL%20FUTURES%20-%20SOUTH%20AFRICA%27S%20READINESS%20FOR%20THE%20FOURTH%20INDUSTRIAL%20REVOLUTION.pdf>
- Nicol, E., Hanmer, L. A., Mukumbang, F. C., Basera, W., Zitho, A., & Bradshaw, D. (2021). Is the routine health information system ready to support the planned national health insurance scheme in South Africa? *Health Policy and Planning*, 36(5), 639–650.  
<https://doi.org/10.1093/heapol/czab008>
- Odeyemi, T. I., & Abioro, T. (2019). Digital technologies, online engagement and parliament-citizen relations in Nigeria and South Africa. In O. Fagbadebo & F. Ruffin (Eds.), *Perspectives on the legislature and the prospects of accountability in Nigeria and South Africa*. Springer [https://doi.org/10.1007/978-3-319-93509-6\\_12](https://doi.org/10.1007/978-3-319-93509-6_12)
- Okeke-Uzodike, O., & Dlamini, B. (2019). Citizen e-participation at local municipal government in South Africa. *Journal of Reviews on Global Economics*, 8, 458–468.  
<https://www.lifescienceglobal.com/pms/index.php/jrge/article/view/6047/3355>
- Owings, L. (2021, July 7). How safe is your data on the Covid-19 vaccine registration system? *Health24*. <https://www.news24.com/health24/medical/infectious-diseases/coronavirus/how-safe-is-your-data-on-the-evds-20210707>
- Paterson, A., Visser, M., Arends, F., Mthethwa, M., Twalo, T., & Nampala, T. (2015). *High-level audit of administrative datasets*. Labour Market Intelligence Partnership.  
<https://lmip.org.za/document/high-level-audit-administrative-datasets>
- Pillay, Y., & Motsoaledi, P. A. (2018). Digital health in South Africa: Innovating to improve health. *BMJ Global Health*, 3 (Suppl 2), e000722. <https://doi.org/10.1136/bmjgh-2018-000722>
- Reddy, V., Winnaar, L., Juan, A., Arends, F., Harvey, J., Hannan, S., Namome, C., Sekhejane, P., & Zulu, N. (2019). *TIMSS 2019: Highlights of South African Grade 9 results in mathematics and science*.  
<https://www.education.gov.za/Resources/Reports.aspx>
- Republic of South Africa (RSA). (1995). *White paper on the transformation of the public service*. [https://www.gov.za/sites/default/files/gcis\\_document/201409/168380.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/168380.pdf)

- Republic of South Africa (RSA). (2020). *Diagnostic report of the Presidential Commission on the Fourth Industrial Revolution*. Government Gazette 43834, pp. 181–347.  
<https://www.gov.za/documents/report-presidential-commission-4th-industrial-revolution-23-oct-2020-0000>
- Smith, K., & Nicol, E. (2020). Process evaluation of the central chronic medicines dispensing and distribution programme in Namakwa district, Northern Cape province protocol: A multimethod approach. *BMJ Open*, 10(2). <https://bmjopen.bmj.com/content/10/2/e032530>
- State Information Technology Agency (SITA). (2021). *Annual report 2020/2021*.  
<https://www.sita.co.za/sites/default/files/Annual%20Report%202020-2021.pdf>
- South African Medical Research Council (SAMRC). (2021, December 08). *Access to EVDS health data significant for evaluating vaccine efficacy*. Press release.  
<https://www.samrc.ac.za/media-release/access-evds-health-data-significant-evaluating-vaccine-efficacy>
- South African Police Service (SAPS). (2003, June 9). *Automated fingerprint identification system (AFIS)*. South African Police Service: Progress report.  
[www.pmg.org.za/docs/2003/appendices/030609afis.ppt](http://www.pmg.org.za/docs/2003/appendices/030609afis.ppt)
- State Security Agency (SSA). (2012). *National Cybersecurity Policy Framework for South Africa*. [https://www.gov.za/sites/default/files/gcis\\_document/201512/39475gon609.pdf](https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf)
- Tredger, C. (2021, June 04). GITOC toasts digital future as it marks 20th anniversary. *ITWeb Africa*. <https://www.itweb.co.za/content/xnklOvzLDO6M4Ymz>
- Townsend, B. (2022). The lawful sharing of health research data in South Africa and beyond. *Information & Communications Technology Law*, 31(1), 17–34.  
<http://doi.org/10.1080/13600834.2021.1918905>
- Van Greunen, D., Kativu, K., Veldsman, A., & Botha, J. (2021, June). Enhancing ICT readiness of schools in South Africa. Policy brief.  
[https://www.dst.gov.za/images/Policy\\_Brief\\_June\\_2021.pdf](https://www.dst.gov.za/images/Policy_Brief_June_2021.pdf)
- Vial, G. (2019). Understanding digital transformation: A review and research agenda. *Journal of Strategic Information Systems*, 28(2), 118–114.  
<https://doi.org/10.1016/j.jsis.2019.01.003>