IPS Working Papers

MEASURING DIGITAL TRUST: AN EMPIRICAL FRAMEWORK FOR INSTITUTIONAL TRUST

CHEW HAN EI
CAROL SOON
KAM TAI TONG
HARKIRAN KAUR
and
CHIN SHUEN LIN

February 2026
IPS Working Papers No. 72

Institute of Policy Studies

About Institute of Policy Studies (IPS)

The Institute of Policy Studies (IPS) was established in 1988 to promote a greater awareness of policy issues and good governance. Today, IPS is a think-tank within the Lee Kuan Yew School of Public Policy (LKYSPP) at the National University of Singapore. It seeks to cultivate clarity of thought, forward thinking and a big-picture perspective on issues of critical national interest through strategic deliberation and research. It adopts a multi-disciplinary approach in its analysis and takes the long-term view. It studies the attitudes and aspirations of Singaporeans which have an impact on policy development and the relevant areas of diplomacy and international affairs. The Institute bridges and engages the diverse stakeholders through its conferences and seminars, closed-door discussions, publications, and surveys on public perceptions of policy.

IPS Working Papers No. 72

MEASURING DIGITAL TRUST:
AN EMPIRICAL FRAMEWORK FOR INSTITUTIONAL TRUST

Chew Han Ei
Senior Research Fellow
Institute of Policy Studies
National University of Singapore
han.chew@nus.edu.sg

Carol Soon
Associate Professor (Practice)
Deputy Head, Department of Communications and New Media
National University of Singapore
carol.soon@nus.edu.sg

Kam Tai Tong
Research Fellow
Institute of Policy Studies
National University of Singapore

Harkiran Kaur
Research Assistant
Institute of Policy Studies
National University of Singapore
harkiran@nus.edu.sg

and

Chin Shuen Lin
Research Intern
Institute of Policy Studies
National University of Singapore

February 2026

AUTHORS’ NOTE

This working paper builds on ***Digital Trust and Why it Matters*** (CTIC Working Paper 05/2023), which outlined the conceptual landscape and the competing definitions that shape current discussions on digital trust. It updates the literature on material developments since 2023 and focuses on the empirical validation of the conceptual model introduced earlier.

While the previous paper clarified what digital trust encompasses and why it matters for policy and governance, this study examines whether the proposed framework holds when translated into measurable constructs. Using structural equation modelling, we assess the influence of both mechanical and relational dimensions of digital trust on trust formation.

Together, the two papers establish a conceptual framework for digital trust and assess its empirical robustness through data and modelling. The emphasis on empirical validation reflects a deliberate effort to develop a measurement approach that is analytically robust and suitable for application at scale.

We would like to thank Mr Henry Ho for executing the structural equation modelling under the guidance of the research team.

CONTENTS

EXECUTIVE SUMMARY **4**

1. INTRODUCTION **7**

1.1. Establishing a Common Definition of Digital Trust 8

1.2. Measuring Digital Trust 12

2. CONCEPTUAL FRAMEWORK **14**

2.1. Mechanical Dimensions of Digital Trust 16

2.2. Relational Dimensions 24

2.3. Trust in Institutions 28

3. METHODS **30**

3.1. Bivariate Relationships 31

3.2. Analysis 32

4. RESULTS **33**

5. DISCUSSION **36**

5.1. Policy Implications 38

6. CONCLUSION **40**

REFERENCES **42**

APPENDICES **49**

Appendix A: Methodology 49

Appendix B: About the Authors 53

MEASURING DIGITAL TRUST: AN EMPIRICAL FRAMEWORK FOR INSTITUTIONAL TRUST

EXECUTIVE SUMMARY

As digital systems become deeply embedded in institutional operations, the public's trust in institutions' ability to govern and manage these systems has become increasingly consequential. This working paper empirically validates a conceptual model of digital trust to examine which dimensions of digital systems and user capability are most strongly associated with institutional trust.

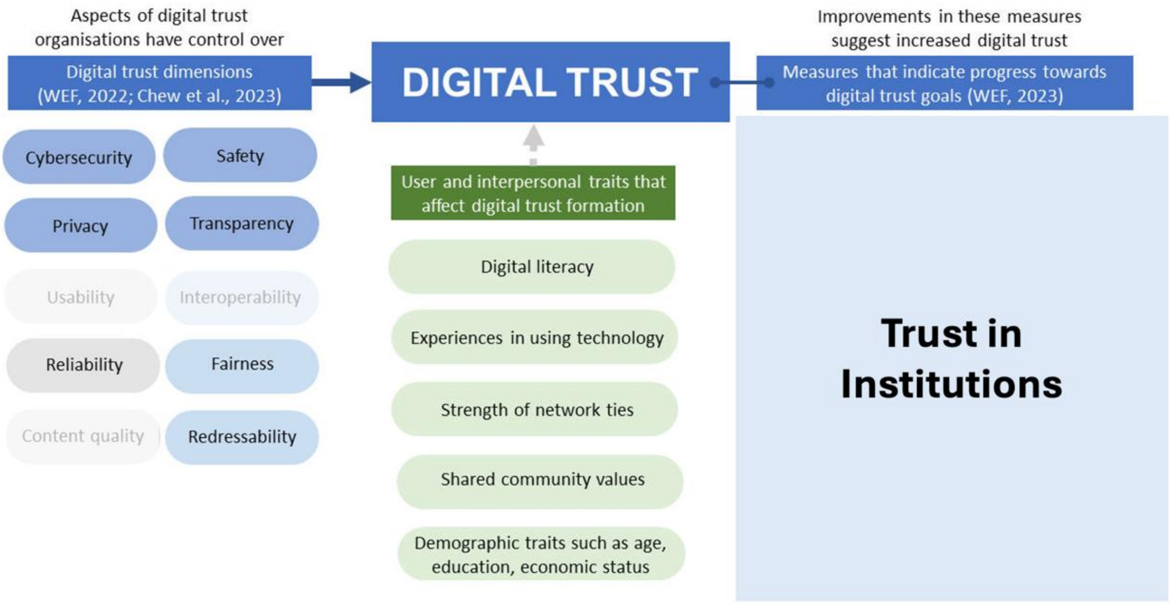
In Singapore, sustained exposure to cybercrime, data breaches and online harms has heightened public attention to how digital systems are designed and governed. While policymakers and practitioners frequently emphasise the importance of strengthening digital trust, existing approaches are often conceptual or focused on isolated dimensions of trust (e.g., trust in technology companies). A coherent and empirically grounded measurement framework is therefore necessary to assess how different dimensions of digital systems and user attributes relate to institutional trust over time.

Against this backdrop, this working paper empirically validates a conceptual model for measuring digital trust that was first introduced in earlier conceptual work. Existing definitions of digital trust often exhibit conceptual ambiguity and overlap. The definition by the World Economic Forum (WEF) is comparatively coherent and inclusive. WEF defines digital trust as **"individuals' expectation that digital technologies and services — and the organisations providing them — will protect all stakeholders' interests and uphold societal expectations and values"** (WEF,

2022). The conceptual model (see Figure 1) draws on the WEF digital trust framework and established academic research, and incorporates individual-level traits relevant to trust formation.

The analysis draws on survey data from a nationally representative sample of 1,008 respondents in Singapore. The results show that five mechanical dimensions under organisational control — cybersecurity, fairness, transparency, reliability and redressability (CFTRR), together with digital literacy, are significant predictors of institutional trust. Among these, fairness and redressability emerge as particularly salient dimensions through which individuals evaluate digital systems and the institutions that govern them. Overall, the model demonstrates good fit and explains a substantial proportion of variation in institutional trust.

Figure 1: Conceptual Framework for Measuring Digital Trust


Aspects of digital trust organisations have control over
Digital trust dimensions (WEF, 2022; Chew et al., 2023)
Cybersecurity
Safety
Privacy
Transparency
Usability
Interoperability
Reliability
Fairness
Content quality
Redressability
DIGITAL TRUST
User and interpersonal traits that affect digital trust formation
Digital literacy
Experiences in using technology
Strength of network ties
Shared community values
Demographic traits such as age, education, economic status
Improvements in these measures suggest increased digital trust
Measures that indicate progress towards digital trust goals (WEF, 2023)
Trust in Institutions

This study provides has several implications for policymakers:

1. **Considering Digital Trust as a Smart Nation Indicator**

   The validated conceptual model provides a basis for incorporating digital trust into national measurement systems to track public confidence in digital systems and inform responsible innovation.

2. **Recognising Digital Literacy as a Strategic Capability**

   The positive association between digital literacy and institutional trust suggests value in tiered digital literacy approaches — spanning foundational digital safety, intermediate information evaluation, and more advanced algorithmic and data rights literacy — to support informed trust across proficiency levels.

3. **Strengthening Transparency and Accountability in Institutional Design**

   The significant association between CFTRR and institutional trust underscores the importance of transparent, accountable and user-centred institutional practices. Clear privacy policies, greater disclosure of cybersecurity practices and accessible redress mechanisms may contribute to public confidence in digital systems.

Together, these implications highlight system-level and user-level considerations relevant to sustaining institutional trust in an increasingly digital society.

MEASURING DIGITAL TRUST:
AN EMPIRICAL FRAMEWORK FOR INSTITUTIONAL TRUST

1. INTRODUCTION

As digital services become embedded across everyday activities, trust in digital systems and the institutions that govern them is increasingly central to economic, social and institutional functioning (WEF, 2024). However, digital trust has been declining, driven by the growing prevalence of online harms such as cybersecurity breaches, system failures and ethical misconduct (Dobrygowski, 2022). In Singapore, the persistent surge in scams and cyberattacks has contributed to a steady erosion of digital trust. Despite enforcement efforts, scam activity has continued, with reported cases reaching 51,501 in 2024 — an increase of 10.6 per cent from 2023 (Singapore Police Force, 2025). As breaches and scams become more frequent, users increasingly question whether the digital environment is capable of safeguarding their interests.

This decline in trust is reflected in the 2025 Thales Digital Trust Index Report, which reported a broad decline in trust in digital services across most sectors compared to the previous year (Thales, 2025). Similarly, the 2024 Consumer Survey by Ping Identity[1] found that 86 per cent of respondents in Singapore did not fully trust organisations that managed their identity data (Ping Identity, 2024). Together, these findings point to declining confidence among Singaporean users in terms of reliability, security and accountability of digital technologies. While these surveys do not measure

[1] Ping Identity is an American software company that specialises in identity management solutions (Ping Identity, n.d.).

digital trust directly, they signal a broader erosion of confidence that warrants closer empirical examination.

Declining digital trust has tangible consequences for user behaviour and institutional legitimacy. It can deter users from engaging fully in online transactions, limiting their ability to benefit from the convenience and efficiency of digital services (Chew, 2023). More broadly, weakened trust may constrain innovation by discouraging adoption and investment, with potential implications for technological competitiveness and economic growth (SGS, 2025). Ensuring that digital trust remains robust alongside technological advancement is therefore essential for sustaining public confidence and supporting a resilient digital economy.

This working paper contributes to this effort by validating a conceptual framework for measuring digital trust and its relationship to institutional trust.

1.1. Establishing a Common Definition of Digital Trust

Addressing digital trust requires a clear and commonly accepted definition of the term. However, there is no consensus on what constitutes digital trust. At the Singapore International Cyber Week 2024 Opening Ceremony, then Senior Minister and Coordinating Minister for National Security Mr Teo Chee Hean described trust in technology as resting on several core requirements:

> "… I think these are questions which you ask yourselves too whenever you receive a call or a message on your mobile device. You want confidence that:

> a. Your data is *secure* [emphasis added], and will not be lost or corrupted;
>
> b. What you see and hear online is *reliable* [emphasis added], not fake or surreptitiously altered;
>
> c. When you transact online, you are not going to be cheated or scammed; and
>
> d. The digital services you use are *resilient* [emphasis added], and will not break down when you need them."
>
> — Prime Minister's Office Singapore, 2024a, para. 7

This framing emphasises security, reliability and system resilience as central components of trust in digital technologies. A related but distinct emphasis appears in the definition offered by Prime Minister and Minister for Finance Mr Lawrence Wong at the launch of Smart Nation 2.0 in 2024, where he stated:

> "To achieve Growth and Community, Singaporeans must be able to go online with confidence — confident that digital systems and services are *secure and reliable* [emphasis added]; that their *safety and well-being* [emphasis added] will not be compromised; and that there is effective help and *recourse* [emphasis added] if they encounter harms."
>
> — Prime Minister's Office Singapore, 2024b, para. 45

Here, trust extends beyond system performance to include user safety and the availability of recourse when harm occurs.

The private sector offers another perspective, often framing digital trust around cybersecurity, data privacy and user experience. The Thales Digital Trust Index Report (2025) reflects this emphasis, noting that “more than four in five consumers expect some level of *data-privacy rights* [emphasis added].” The report also emphasised that “consumers’ confidence in a brand would significantly increase if they adopted emerging or advanced technologies that improves *security and data protection* [emphasis added].” Additionally, it highlights the necessity for organisations to “offer a good *customer experience* [emphasis added].” This framing place particular weight on an institution’s data protection, security practices and users’ experience with its service as drivers of trust.

In *Digital Trust and Why It Matters*, we identified several recurring terms across definitions of digital trust, most notably confidence, beliefs and faith (Chew et al., 2023). Table 1 summarises selected definitions from the literature, illustrating the prominence of these recurring terms.

Table 1: Examples of Definitions of Digital Trust from the Literature

Definition	**Source**
An evolution of traditional trust models to cover the additional requirements of digital business — deriving levels of **measurable confidence** to make risk-based decisions	Gaehtgens and Allan (2017) as cited in Kożuch (2021)
The **belief** that a brand is reliable, capable, safe, transparent and truthful in its digital practices	Lynch et al. (2016)

The level of **confidence** in people, processes and technology to build a secure digital world	PwC (2018)
Consumer **faith** in cybersecurity, data privacy, and responsible AI	McKinsey & Company (2022)

The diversity of definitions reflect both conceptual ambiguity and overlaps, complicating efforts to operationalise digital trust for measurement and policy use. The one commonality which they share is the emphasis on the source that delivers the service.

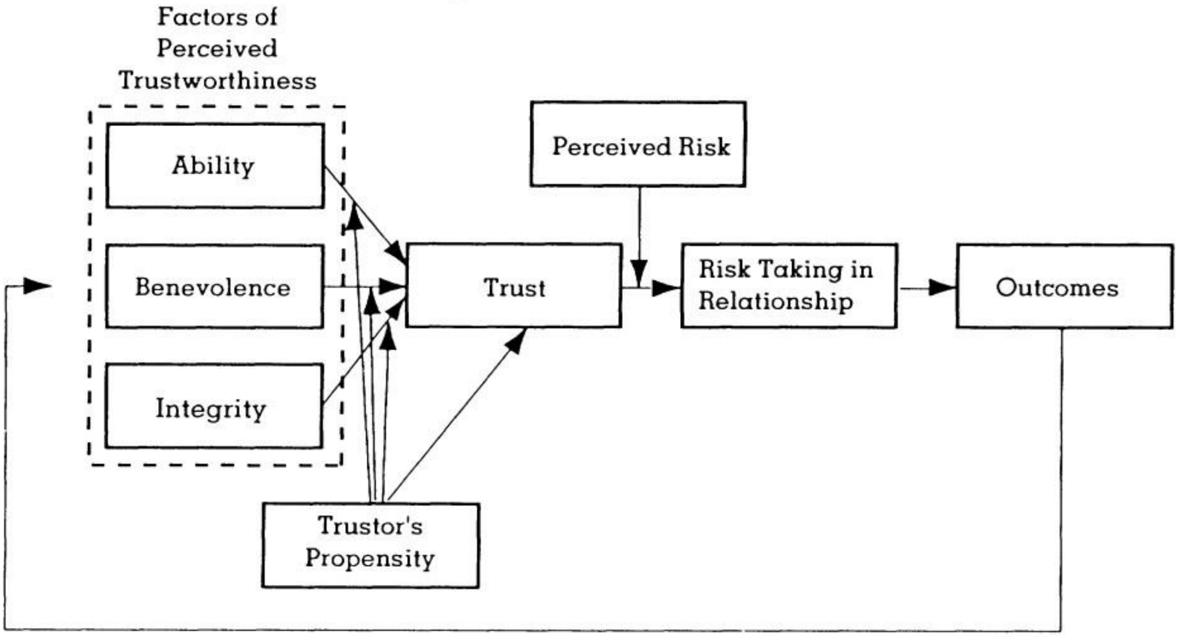
To address this definitional ambiguity, the WEF released a 2022 report titled *Earning Digital Trust: Decision Making for Trustworthy Technologies* (WEF, 2022). This report attempts to bring conceptual coherence to digital trust and introduces a structured framework informed by government officials, consumer representatives and leaders from major technology and consumer-oriented firms. It defines digital trust as **"individuals' expectation that digital technologies and services — and the organisations providing them — will protect all stakeholders' interests and uphold societal expectations and values"** (WEF, 2022). The framework identifies three core pillars underpinning digital trust: security and reliability; accountability and oversight; and inclusive, ethical and responsible use. It further outlines eight dimensions through which the trustworthiness of digital technologies can be operationalised and assessed: cybersecurity, safety, privacy, auditability, transparency, interoperability, redressability and fairness (WEF, 2022).

This definition highlights that trust is fundamentally a human disposition, and technologies can only be designed, deployed and governed by institutions or organisations in ways that inspire user confidence. Importantly, this framework also distinguishes between normative expectations and dimensions that can be operationalised and assessed.

1.2. Measuring Digital Trust

A central challenge in measuring digital trust lies in identifying constructs that are meaningful and comparable across contexts. The Integrative Model of Organisational Trust, known as the ABI model, developed by Mayer et al. (1995) remains one of the most influential frameworks in trust research (see Figure 2). It conceptualises trust as emerging from perceived trustworthiness, shaped by assessments of ability, benevolence and integrity, alongside an individual's general propensity to trust others (Fricker et al., 2014). Its parsimony and broad applicability have led to extensive validation and application across organisational and relational contexts (Colquitt et al., 2007; Dirks & de Jong, 2022).

Figure 2: Integrative Model of Organisational Trust



Source: Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review, 20*(3), 709–734. https://doi.org/10.2307/258792

However, the ABI framework was developed primarily to explain interpersonal trust within organisational settings rather than institutional trust in digital systems at national scale. In particular, the construct of "benevolence" — defined as the extent to which a trustee is perceived act in the trustor's interest beyond self-interest (Mayer et al., 1995) — presents significant challenges for standardised national measurement. As a perception-based and inherently normative construct, benevolence is shaped by individual interpretations, prior experiences and contextual framing (Saveljeva & Volkova, 2025). Establishing stable and consensus-based benchmarks for benevolence across diverse populations is therefore difficult.

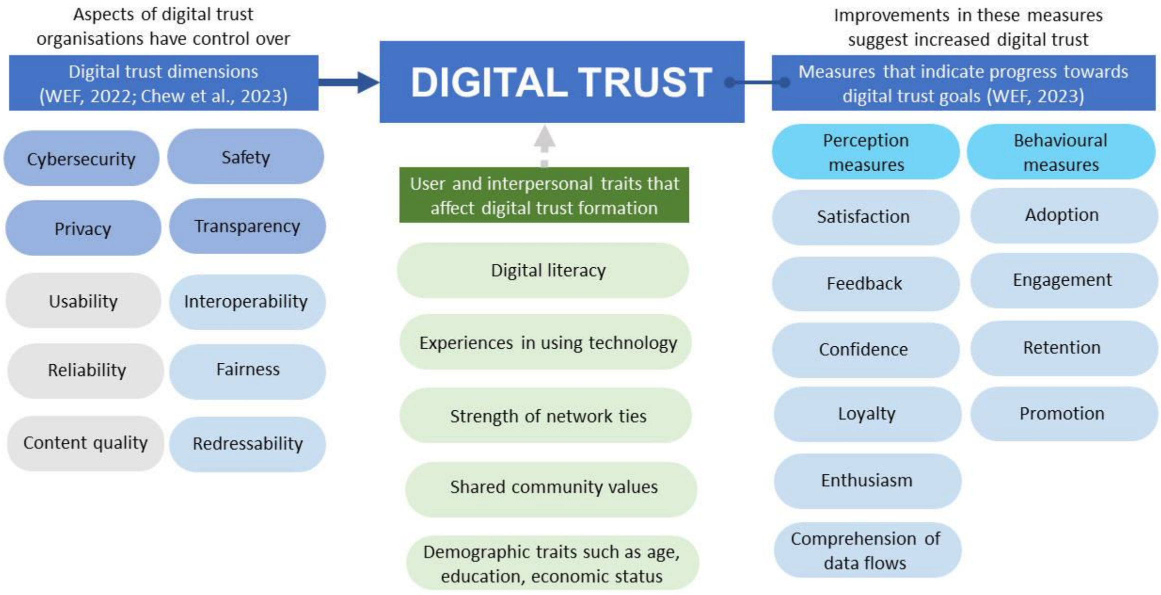
Operationalising “benevolence” in a national digital trust index also introduces risks of politicised interpretation. Fluctuations in benevolence indicators may be interpreted as evidence of institutional bad faith, even when driven by methodological adjustments or isolated events. This susceptibility to contextual framing constrains its reliability as a stable indicator in public policy settings.

For these reasons, this paper builds on an alternative conceptual model of digital trust introduced in earlier work (Chew, 2023), integrating insights from the WEF digital trust framework and existing academic research. The model incorporates system-level dimensions and selected individual traits, including digital literacy, that are empirically examined in this study (Dutton & Shephard, 2006; Jones-Jang et al., 2021; Walther & Bunz, 2005).

2. CONCEPTUAL FRAMEWORK

Trust in institutions is a cornerstone of social stability and effective governance. In an era of rapid technological, economic and political change, understanding the factors that shape institutional trust has become increasingly important. Drawing on *Digital Trust and Why it Matters* (Chew et al., 2023), Figure 3 illustrates the conceptual framework that this study validates.

Figure 3: Conceptual Framework for Measuring Digital Trust


Aspects of digital trust organisations have control over
Digital trust dimensions (WEF, 2022; Chew et al., 2023)
DIGITAL TRUST
Improvements in these measures suggest increased digital trust
Measures that indicate progress towards digital trust goals (WEF, 2023)
Cybersecurity
Safety
Privacy
Transparency
Usability
Interoperability
Reliability
Fairness
Content quality
Redressability
User and interpersonal traits that affect digital trust formation
Digital literacy
Experiences in using technology
Strength of network ties
Shared community values
Demographic traits such as age, education, economic status
Perception measures
Behavioural measures
Satisfaction
Adoption
Feedback
Engagement
Confidence
Retention
Loyalty
Promotion
Enthusiasm
Comprehension of data flows

Source: Chew, H. (2023). *To stop the erosion of digital trust, measure it.* Tech for Good Institute. https://techforgoodinstitute.org/blog/perspectives/to-stop-the-erosion-of-digital-trust-measure-it/

Dobrygowski and Hoffman (2019) distinguish digital trust into two core types: mechanical and relational trust. Mechanical digital trust refers to the “means and mechanisms that deliver predefined outputs reliably and predictably” (Dobrygowski & Hoffman, 2019, para. 5). In this study, the independent variables correspond to the dimensions of mechanical digital trust — aspects of digital trust that organisations have control over.

In contrast, relational trust concerns user-level and interpersonal traits that shape digital trust formation. Dobrygowski and Hoffman (2019) described relational digital trust as the societal norms and expectations that constitute a “shared agreement on when, where, why and how technologies are used” (para. 6). These traits are incorporated as moderating variables in this study. Their inclusion reflects the understanding that digital trust is shaped by individuals' perceptions, experiences and social context.

The dependent variable consists of indicators used to measure progress towards digital trust goals. These goals are defined as "the extent to which an organisation's relationship with an actor (whether an individual or an organisation) is strong and resilient" (WEF, 2023, p. 4). WEF recommends incorporating both perceptual measures — such as satisfaction, feedback, confidence, loyalty, enthusiasm and comprehension of data flow — and behavioural measures, such as adoption, engagement, retention and promotion (WEF, 2023). Together, these indicators capture the level of trust individuals or organisations place in an entity, with improvements reflecting stronger institutional digital trust (Chew, 2023).

A fuller conceptual discussion of the dimensions is provided in *Digital Trust and Why it Matters*.

2.1. Mechanical Dimensions of Digital Trust

This section examines the mechanical dimensions of digital trust. To ensure a parsimonious and interpretable measurement model, the dimensions of usability, interoperability and content quality were excluded from the current phase of analysis following exploratory factor analysis. Future research can revisit these dimensions to examine their relationship to institutional trust once measurement properties are better specified. In the current study, greater emphasis is placed on the emerging dimensions of fairness and redressability, reflecting their growing significance in the digital ecosystem and their centrality to the empirical validation undertaken here (see Subsections 2.1.1 and 2.1.2). The remaining mechanical dimensions are presented according to their established definitions. Table 2 outlines each dimension, its definition and the operationalised statements used in this study.

.

Table 2*:* Mechanical Dimensions of Digital Trust

Mechanical Dimension	Definition	Operationalisation	Response Options
Cybersecurity (Spearman-Brown coefficient = 0.69)	Cybersecurity focuses on the security of digital systems, including data, technologies and processes; and is crucial for maintaining the confidentiality, integrity and availability of data and systems (National Institute of Standards and Technology, 2020).	• Digital technologies have strong security measures to protect my personal data (Acharya & Mekker, 2022). • Digital technologies have sufficient security measures to ensure that data cannot be modified by a third party (Acharya & Mekker, 2022).	1 - Strongly disagree 2 - Disagree 3 - Agree 4 - Strongly agree 5 - I can't decide
Safety	Efforts to prevent harm (e.g., emotional, physical, psychological) to people or society from technology uses and data processing (WEF, 2021).	• There will always be new solutions to address any harmful consequences of developments in digital technologies (European Commission, 2021).#	1 - Strongly disagree 2- Disagree 3 - Agree 4 - Strongly agree 5 - I can't decide
Privacy (Cronbach's alpha = 0.70)	The expectation of control over or confidentiality of their personal or personally identifiable information (WEF, 2022).	• Digital technologies collect too much information about me (Parasuraman, 2000).# • New digital technologies make it too easy for governments to spy on people (Parasuraman, 2000).	1 - Strongly disagree 2 - Disagree 3 - Agree 4 - Strongly agree 5 - I can't decide

		• New digital technologies make it too easy for companies to spy on people (Parasuraman, 2000).	
Transparency (Cronbach's alpha = 0.76)	Availability of information about an actor that allows other actors to monitor the workings or performance of the first actor (Meijer, 2013, p. 430).	• Digital technology providers disclose sufficient information to the public on how their products and services work (Park & Blenkinsopp, 2011). • Digital technology providers disclose sufficient information to the public on how their data would be used (Park & Blenkinsopp, 2011). • Digital technology providers are honest to the public about how their products and services work.	1 - Strongly disagree 2 - Disagree 3 - Agree 4 - Strongly agree 5 - I can't decide
Reliability (Cronbach's alpha = 0.67)	The accessibility to a technology when needed as assessed by digital users (Lippert, 2001).	• I feel confident that digital technologies will follow through with what I instructed them to do (Parasuraman, 2000). • Digital services are available and work without disruption when I need them (Parasuraman, 2000).[#]	1 - Strongly disagree 2 - Disagree 3 - Agree 4 - Strongly agree 5 - I can't decide

		• I can rely on digital tools to perform as expected when I use them (Parasuraman, 2000).	
Fairness	Fairness requires organisations to strive for just and equitable outcomes for all stakeholders, considering the relevant circumstances and expectations (WEF, 2021).	• Help will be available for those who are negatively impacted by digital technologies (Edelman Trust Institute, 2024a).	1 - Strongly disagree 2 - Disagree 3 - Agree 4 - Strongly agree 5 - I can't decide
Redressability (Cronbach's alpha = 0.70)	Represents the possibility of obtaining recourse where individuals, groups or entities have been negatively affected by technological processes, systems or data uses (Shell & Buell, 2019).	• It is easy to reach out to digital technology providers if I have any issues while using their products and services. • Digital technology providers will fix any issues I have when using their products and services. • Digital technology providers make improvements based on user feedback.	1 - Strongly disagree 2 - Disagree 3 - Agree 4 - Strongly agree 5 - I can't decide

# indicates items that were reverse-coded.

For dimensions assessed using the Spearman-Brown coefficient, all values exceeded the commonly cited minimum reliability threshold of 0.60 (George & Mallery, 2016; Royal, 2017). Similarly, dimensions evaluated using Cronbach’s alpha either met or closely approached the conventional threshold of α ≥ 0.70 (van Griethuijsen et al., 2015). These findings indicate that the instruments demonstrate acceptable reliability for the constructs examined.

2.1.1. Fairness

Fairness refers to the extent to which organisations strive for just and equitable outcomes for all stakeholders, taking relevant circumstances and expectations into account (WEF, 2021). As digital systems increasingly inform decisions across multiple domains, ensuring equitable operation has become increasingly important. Users’ perceptions of fairness in digital systems strongly influence their acceptance and trust in automated decisions. Research indicates that trust increases when algorithms are perceived as fair and explainable (Kuang et al., 2025). Users also respond to incremental improvements in fairness, which can lead to meaningful gains in trust (Zhou et al., 2021). Taken together, these findings suggest that perceived fairness is a key determinant of digital trust.

However, achieving fairness in digital systems presents well-documented challenges. Digital systems can replicate and amplify existing societal biases and inequalities. Biased or incomplete data can produce skewed outputs, while algorithms developed without consideration of biases may reinforce or exacerbate injustices (Hasan et al., 2023). Opaque systems can further constrain users' ability to scrutinise or challenge decisions perceived as unfair (Hasan et al., 2023).

Transparency plays an important role in mitigating these risks. Clear explanations and visible decision-making mechanisms, as observed in ridesharing and food delivery platforms, enable users to better assess fairness and foster stronger digital trust (Chong et al., 2024). Advancing fairness therefore requires a structured and transparent approach. Organisations can demonstrate fairness by being transparent about data collection, use and retention policies, and consider multiple user personas to account for differing fairness expectations across groups. In these processes, standardisation helps ensure decision-making remains consistent and aligned with ethical and responsible use norms (Microsoft, 2022). As such, organisations should document and justify their fairness-related decisions, particularly when defining and implementing fairness within technology and data processing.

2.1.2. Redressability

Redressability refers to the availability of recourse when individuals, groups or entities are negatively affected by technological processes, systems or data uses (Shell & Buell, 2019). Even with state-of-the-art technology and robust deployment plans, unintentional technical errors and unforeseen circumstances are inevitable. Security breaches or significant system downtime can undermine the trustworthiness of a technology or organisation. The impact is further amplified when there is a failure to provide adequate compensation or a reluctance to rectify the losses suffered by partners, customers, or other affected individuals (WEF, 2022). Transparent and accessible redress mechanisms allow users to report harms while enabling technology providers to respond effectively, thereby mitigating further erosion of trust.

The importance of redressability in maintaining trust is well established in the literature. Pi and Proctor (2025) argue that effective redress mechanisms are essential for addressing AI-related harms. Internal complaint systems, which are often the first point of contact for consumers, play an important role in building trust. When designed well, these mechanisms provide clear avenues for compensation, correction or human review of algorithmic decisions. In doing so, they protect individual rights, foster a culture of responsibility and generate insights into how AI systems may cause harm, all of which contribute to stronger digital trust (Pi & Proctor, 2025). Similarly, research on complaints management shows that fair compensation, transparent procedures and empathetic treatment are central to restoring trust and encouraging positive user engagement (Rosli, 2025).

This shift towards institutionalising redressability is reflected in Singapore's Online Safety (Relief and Accountability) Act (OSRA), passed in November 2025 (Lee, 2025). The OSRA establishes the Online Safety Commission (OSC), which administers a statutory reporting mechanism allowing victims to seek timely remedies for online harms. It also introduces statutory torts, providing a clear legal basis for victims to hold perpetrators accountable and enhancing oversight of platforms and actors responsible for such harms. Covering 13 categories of online harms — including harassment, doxxing, online stalking, and intimate image abuse — the Act embeds accessible and enforceable pathways for redress. By signalling a commitment to user protection and meaningful remedy, the Act contributes to a digital environment that is fair, responsive and trustworthy, thereby strengthening overall digital trust.

Given that the remaining mechanical dimensions have been extensively discussed in earlier work and are included in Table 2 for completeness, the analysis now turns to the relational dimensions of digital trust.

2.2. Relational Dimensions

This section examines the relational dimensions that moderate digital trust formation. Table 3 summarises the theoretical relationships between each relational dimension and digital trust, as supported by existing research, and outlines how these dimensions are operationalised in the current study.

To ensure measurement reliability, the operationalised statements used to assess each relational dimension draw on instruments validated in prior studies. For measures evaluated using the Spearman-Brown coefficient, all reported values meet the commonly cited minimum reliability threshold of 0.60 (George & Mallery, 2016; Royal, 2017). Measures assessed using Cronbach’s alpha exceed the conventional threshold of $\alpha \geq 0.70$ (van Griethuijsen et al., 2015), indicating acceptable internal consistency.

Table 3: Relational Dimensions of Digital Trust

Relational Dimension	Key Findings	Operationalisation	Response Options
Digital Literacy (Spearman-Brown coefficient = 0.60)	Digital literacy enables users to better identify misinformation and avoid negative online experiences that may otherwise diminish relational trust (Jones-Jang et al., 2021).	• Overall, I am comfortable with using digital technology (Ministry of Digital Development and Information, n.d.). • I can usually figure out new digital products and services without help from others (Parasuraman, 2000).	5-point agreement scale
Experiences in Using Technology (Cronbach's alpha = 0.85)	More experience using the internet is generally associated with greater confidence in technology and higher levels of trust, as increased familiarity leads to ease of use, comfort and reduced perceived risk (Dutton & Shepherd, 2006).	• During the last 12 months, how often, if at all, did you experience online harassment or online hate speech, or heard of someone experiencing it? (International Social Survey Programme, 2023). • During the last 12 months, how often, if at all, did you receive a security alert, like a login attempt from an unfamiliar device, but found that your account was not compromised? (International Social Survey Programme, 2023)	1 - Almost all the time 2 - Several times a day 3 - Once a day 4 - Several times a week 5 - Several times a month 6 - Less often 7 - Never

		• During the last 12 months, how often, if at all, did you turn to online resources (forums, guides or videos) and quickly found solutions to a technical or personal problem that saved you time and effort?	
Strength of Ties in Digital Network Relationship	Strong ties support "thick" interpersonal trust through frequent interaction and familiarity (Ferlander, 2007; Putnam, 2000). High levels of trust cultivated within close-knit, localised networks can generalise outward to broader social networks, allowing trust to extend even to strangers (Burt, 1992; Freitag & Traunmüller, 2009; Glanville & Paxton, 2007; Khodyakov, 2007; Putnam et al., 1993).	• I have a person to contact if I have problems with digital technologies.	5-point agreement scale
Shared Community Values	Wu et al. (2010) found that shared values within virtual communities increased members' trust in one another, with trust deepening as common values and goals developed.	• My friends and family are generally positive about using digital technologies in their lives (Niehaves et al., 2012).	5-point agreement scale

Demographic Factors	Age Studies found clear generational differences in digital trust and readiness to adopt digital technologies, with adolescents demonstrating higher scores than the older age groups (Dmitrii, 2025; Noah & Sethumadhavan, 2019).	Age	Based on year of birth
	Income Income has been shown to influence traditional relational trust. Individuals with higher income levels report higher levels of trust (Alesina & La Ferrara, 2002; Putnam, 2000).	Household Monthly Income	Income bands ranging from below S$1000 to S$20,000 and above
	Education Education is also positively correlated with trust as education as education allows people to make informed decisions (Keefer & Knack, 2005).	Highest Education Level	Categories ranging from below primary to degree and above

2.3. Trust in Institutions

The dependent variable, *trust in institutions*, reflects individuals' confidence in both public and private institutions. This form of trust has important implications for social cohesion and institutional legitimacy. Institutional trust shapes political attitudes and behaviours and influences cooperation among individuals and groups (Justino & Samarin, 2025). It also affects the capacity of societies to mobilise around shared norms and collective goals (Justino & Samarin, 2025). Given its central role in sustaining the social contract, institutional trust is a critical outcome variable in this study. Table 4 presents the definition of this variable and its operationalisation.

Table 4: Operationalisation of Trust in Institutions

Outcome	Definition	Operationalisation	Response Options
Trust in Institutions (Cronbach's alpha = 0.86)	The trust users have in institutions to do what is right when it comes to managing the introduction of new digital technologies and innovations — ensuring they are safe, understood by the public, beneficial to society and accessible to the people who need them (Edelman Trust Institute, 2024b).	• Digital technology providers in general (Edelman Trust Institute, 2024b). • Businesses in non-technology industries (Edelman Trust Institute, 2024b). • Non-governmental organisations (Edelman Trust Institute, 2024b). • Government in general (Edelman Trust Institute, 2024b).	1 - Do not trust them at all 9 - Trust them a great deal

Institutional trust was measured using four items, each demonstrating strong standardised loadings ranging from 0.67 to 0.87, exceeding the commonly cited minimum threshold of 0.50 (Cheung et al., 2024). The scale also meets the recommended minimum reliability threshold α ≥ 0.70 (van Griethuijsen et al., 2015), indicating acceptable internal consistency.

It is, however, important to situate these results within Singapore's broader trust context. Singapore is generally characterised as a high-trust society, particularly with respect to government institutions. According to the Edelman Trust Barometer (2024c), 77 per cent of Singaporeans report trusting the government, substantially above the global average of 51 per cent. Consistent with this broader context, 65 per cent of respondents in this study rated their trust in the government between 7 and 9 on a nine-point scale, ranging from 1 ("Do not trust them at all") to 9 ("Trust them a great deal"). Trust levels were lower for other actors: 50 per cent of respondents reported high trust in technology providers; 42 per cent in non-governmental organisations; and 38 per cent in businesses in non-technology sectors. These differences highlight the relatively higher levels of trust placed in government institutions compared to other organisations in Singapore.

3. METHODS

Data were collected through an online survey administered to a panel-based respondent database (see Appendix A). This approach enabled broad reach and efficient recruitment across key demographic segments. To ensure data quality, an initial screening process was conducted to remove responses displaying irregularities or internal inconsistencies. Following data cleaning, 1,008 valid responses were retained for analysis. The resulting sample closely mirrors the demographic profile of Singapore's population in terms of citizenship, gender, race, age group, and housing type (see Figures A1 to A5 in Appendix A). However, the sample is skewed towards individuals with higher educational attainment (see Figure A6 in Appendix A), reflecting the online mode of administration.

Before model estimation, several steps were applied to improve data consistency and accuracy. Missing values were imputed using mean substitution, negatively worded items were reverse-coded for consistency, and all variables were standardised to align measurement scales across constructs. These steps enhanced data comparability and prepared the dataset for structural equation modelling (SEM).

3.1. Bivariate Relationships

Prior to estimating the SEM, bivariate correlations were examined between each mechanical and relational dimension and institutional trust (see Table 5). Most mechanical dimensions demonstrated positive and statistically significant correlations with institutional trust. Several relational traits were also correlated at the bivariate level. These results suggest that multiple dimensions are associated with institutional trust when considered independently.

Table 5: Bivariate Correlations with Trust in Institutions

Dimension	r
Cybersecurity	.461***
Safety	.257***
Privacy	.020
Transparency	.487***
Reliability	.463***
Fairness	.360***
Redressability	.462***
Digital Literacy	.363***
Experiences in Using Technology	.379***

Note: n = 1,008. ***p < .001. Constructs retained in the final SEM model include cybersecurity, transparency, reliability, fairness, redressability and digital literacy. All other inter-construct correlations are available on request.

While several dimensions demonstrate positive bivariate associations with institutional trust, only a subset retains independent explanatory power when entered simultaneously into the structural model.

3.2. Analysis

This study adopted an SEM approach, implemented using the Latent Variable Analysis (*lavaan*) package in R version 4.5.1, alongside IBM SPSS Statistics 28 for preliminary data cleaning and descriptive analyses. Starting from the conceptual model in Figure 3, an iterative modification process was undertaken to improve model fit while maintaining theoretical coherence. Through systematic adjustments, latent constructs exhibiting high intercorrelations were combined where theoretically justified, and observed variables with low factor loadings were removed to enhance measurement validity. These refinements were made incrementally to preserve the conceptual integrity of the model.

When entered simultaneously into the structural model, only cybersecurity, fairness, transparency, reliability, redressability and digital literacy retained significant predictive power. This indicates that while several dimensions correlate with institutional trust at the bivariate level, only a subset exerts independent explanatory influence once shared variance across constructs is accounted for.

The final set of constructs used in the refined SEM model is presented in Table 6. This refined model served as the foundation for subsequent analysis and interpretation.

Table 6: Latent Variables Included in the Final SEM Model

Endogenous variable	Exploratory variables	Estimate
Trust in Institutions	CFTRR = Cybersecurity + Fairness + Transparency + Reliability + Redressability	0.442
	Digital Literacy	0.314

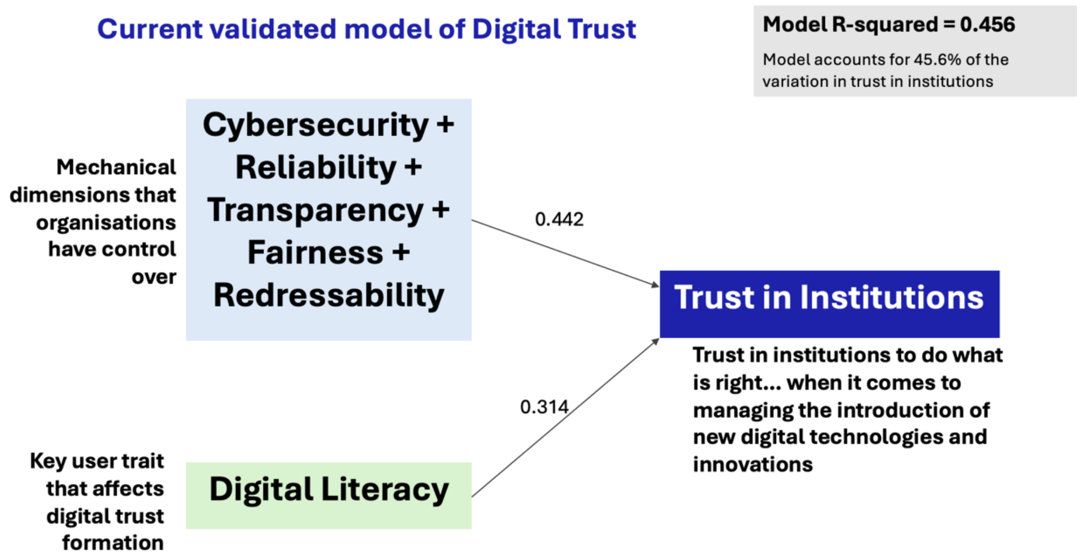
4. RESULTS

Results from the SEM indicated good overall model fit, suggesting that the simplified model (see Figure 4) provides a parsimonious representation of the data. The comparative fit indices[2] (CFI = 0.970; TLI = 0.966) exceeded

[2] The Comparative Fit Index (CFI) and Tucker–Lewis Index (TLI) assess how well the specified model fits the observed data relative to a baseline model, with values above 0.95 generally indicating good fit.

conventional thresholds for good fit, while the root mean square error of approximation value of 0.039 (90% CI = 0.034–0.044) and standardised root mean square residual of 0.030 indicate close approximation to the observed covariance structure.[3] Taken together, these indices suggest that the model captures the underlying relationships among the constructs adequately. Additionally, the predictors accounted for approximately 45.6 per cent of the variance in institutional trust, indicating that the model explains a meaningful proportion of observed variation in trust outcomes.

Figure 4: Final SEM Model


Current validated model of Digital Trust
Model R-squared = 0.456
Model accounts for 45.6% of the variation in trust in institutions
Mechanical dimensions that organisations have control over
Cybersecurity + Reliability + Transparency + Fairness + Redressability
0.442
Trust in Institutions
Trust in institutions to do what is right... when it comes to managing the introduction of new digital technologies and innovations
0.314
Key user trait that affects digital trust formation
Digital Literacy

Within the structural model, both CFTRR and digital literacy were significant predictors of institutional trust. CFTRR emerged as the stronger predictor, with a standardised coefficient of 0.442 (p < .001).

[3] The root mean square error of approximation estimates how closely the model approximates the population covariance structure per degree of freedom; values below 0.05 indicate close fit. The standardised root mean square residual reflects the average discrepancy between observed and predicted correlations, with values below 0.08 considered acceptable.

This result suggests that **individuals who perceive digital systems as secure, reliable, transparent, fair and supported by effective channels for redress tend to report higher levels of trust in the institutions operating those systems**. Digital literacy also exhibited a positive association with institutional trust, with a standardised coefficient of 0.314 (p < .001). This suggests that **individuals with greater digital competence and understanding of online systems are more likely to place confidence in digital institutions**, possibly because they feel better equipped to navigate, evaluate and manage digital processes.

The two predictors, digital literacy and CFTRR, were moderately correlated (r = 0.582), indicating that users with higher digital literacy also tend to perceive digital systems as more trustworthy. Despite this association, each variable contributed unique explanatory power to institutional trust, suggesting that system-level qualities and user-level competencies are independently associated with trust outcomes.

The mechanical dimensions of safety and privacy were not significant predictors of institutional trust. Similarly, the relational dimensions of demographic factors, experience using technology, strength of ties in digital network relationships and shared community values did not have a significant effect on institutional trust. However, this does not mean that these factors were not important, but that taken together, they were weaker than CFTRR and digital literacy in predicting one's trust in the institutions which provide the product and/or service.

5. DISCUSSION

All in all, the findings suggest that trust in digital institutions is shaped primarily by perceptions of system integrity and by individuals' digital capabilities. The dominant role of CFTRR underscores the importance of designing and maintaining digital systems that are secure, transparent, procedurally fair and reliable. When individuals believe that systems protect their data, operate consistently, and offer avenues for redress, they are more likely to trust the institutions responsible for them. This highlights the central role of system design and governance practices in shaping public trust.

These findings are broadly consistent with definitions of digital trust proposed by major consultancy firms, as discussed in our earlier working paper. These definitions primarily emphasised dimensions such as cybersecurity, transparency and user confidence in digital platforms. Consistent with these definitions, the present study demonstrates that dimensions such as **cybersecurity and transparency** are important contributors to digital trust. However, the results also extend beyond existing industry definitions. A key contribution of this study is the identification of additional dimensions — **redressability and fairness** — as significant predictors of trust. These findings suggest that digital trust extends beyond technical safeguards to include users' expectations of fair treatment and meaningful avenues for recourse.

At the same time, the positive association between digital literacy and institutional trust suggests that users' ability to understand and navigate digital environments contributes to their evaluations of institutional trustworthiness.

Individuals with higher digital skills may feel more empowered and less vulnerable when interacting with digital services, which may in turn fosters trust (Hussain & Phulpoto, 2024). This finding points to the potential value of public digital education initiatives, as efforts to improve digital literacy may indirectly support institutional legitimacy and confidence.

Overall, the results indicate that both system qualities and user competencies work in tandem to shape trust in digital institutions. The model's fit and explanatory power reinforce the importance of these factors in understanding how individuals evaluate and place trust in institutions that provide digital services. This study also provides empirical validation for the conceptual framework presented previously in Figure 3. This empirical support strengthens the framework's utility as a foundation for future research and as a reference point for policymakers seeking to monitor digital trust at a national level.

Several limitations should be noted. First, the data were collected through an online, panel-based sample. While this approach enables efficient recruitment, it may limit the generalisability. Future research could validate the model using broader population samples.

Second, although the conceptual model demonstrates empirical support, further testing is needed to assess its robustness. Developed and refined using a single dataset, the model would benefit from replication across diverse contexts to assess stability and wider applicability.

Third, while this study draws on validated measures from prior literature, there remain alternative ways to operationalise certain dimensions of digital trust. The dimensions can be conceptualised through multiple lenses, and different item formulations may yield richer or more nuanced insights. Further refinement and experimentation in operationalisation could help ensure that each dimension is captured with greater precision while retaining conceptual coherence.

5.1. Policy Implications

The findings of this study have implications for Singapore policymakers seeking to foster institutional trust in an increasingly digital society.

First, the findings suggest that digital trust could be considered as a Smart Nation indicator. Incorporating the validated digital trust conceptual model into national measurement frameworks could enable policymakers to monitor public confidence in institutions systematically and over time. Such an indicator would allow government agencies to detect changes in digital trust and identify areas where trust may be weakening. This could support the design of more targeted responses where necessary. Further research would also be needed to validate additional dimensions of digital trust before their integration into national frameworks. Expanding measurement beyond the current set of indicators could offer more comprehensive guidance for responsible innovation and institutional accountability.

Second, the findings underscore the importance of digital literacy. The government, through the Infocomm Media Development Authority’s Digital for

Life movement and National Library Board's S.U.R.E campaign, has ramped up efforts in public education to strengthen people's ability to navigate the online space competently, safely and responsibly.

Consistent with extant literature on digital literacy (Akello, 2024; Hargittai et al., 2019; Mancino, 2023), the descriptive analysis indicates that digital literacy levels vary by age and educational attainment, with younger and more highly educated respondents reporting higher literacy scores. These patterns suggest potential value in tiered digital literacy approaches tailored to different proficiency levels. Entry-level modules could equip individuals with foundational skills in digital safety and privacy management. Intermediate content should focus on evaluating digital information and detecting misinformation. At the advanced level, digital literacy programmes should promote algorithmic awareness, data rights education, and critical evaluation of digital platforms and institutional content. Such a graduated structure may help support public resilience and informed trust.

Third, the significant association between CFTRR and institutional trust highlights the value of investments in transparency, accountability, and user support systems. Governments and institutions should prioritise ensuring that privacy policies are clear and accessible and that users are well-informed about how data is collected and used. They could also consider establishing visible and reliable support services through which individuals can raise concerns and obtain redress. Strengthening responsive communication channels and providing timely, transparent updates on data practices and safeguards may further enhance user confidence in digital systems.

6. CONCLUSION

As digital systems become more deeply embedded in institutional operations, trust is no longer a peripheral concern. It has become a strategic consideration, shaping social cohesion, economic participation and governance legitimacy. In this context, establishing a reliable framework to measure digital trust has become increasingly important. This working paper addresses this challenge by providing an empirically validated framework for measuring digital trust.

The findings also underscore the role of digital literacy in shaping how individuals across diverse backgrounds navigate digital systems. Greater understanding of digital processes and risk assessment can reduce vulnerability and support trust in digital systems.

At the same time, safeguards such as robust cybersecurity measures, reliable system performance and clear accountability structures help protect users from harm while signalling institutional competence and responsibility. Enhancing transparency complements these efforts by enabling users to understand how digital systems operate, how decisions are made, and how data is collected and used.

Together, these findings point to a digital environment in which trust is shaped by both sound system design and user capabilities. By providing tools to assess digital trust empirically, the validated framework offers a basis for future research and for policy discussion on trust in institutions.

REFERENCES

Acharya, S., & Mekker, M. (2022). Public acceptance of connected vehicles: An extension of the technology acceptance model. *Transportation Research Part F: Traffic Psychology and Behaviour, 88*, 54–68. https://doi.org/10.1016/j.trf.2022.05.002

Alesina, A., & La Ferrara, E. (2002). Who trusts others? *Journal of Public Economics, 85*(2), 207–234. https://doi.org/10.1016/S0047-2727(01)00084-6

Akello, T. (2024). Digital Literacy and Media Consumption among Different Age Groups. *Journal of Communication, 5*(2), 14–27. https://doi.org/10.47941/jcomm.1973

Burt, R. S. (1992). Structural holes: The social structure of competition (1st ed.). *Harvard University Press*. https://doi.org/10.4159/9780674029095

Chew, H. (2023). *To stop the erosion of digital trust, measure it*. Tech for Good Institute. https://techforgoodinstitute.org/blog/perspectives/to-stop-the-erosion-of-digital-trust-measure-it/

Chew, H. E., Tan, J., Soon, C. (2023). *Digital Trust and Why It Matters.* NUS-CTIC Working Paper Series. https://ctic.nus.edu.sg/resources/CTIC-WP-05(2023).pdf

Cheung, G. W., Cooper-Thomas, H. D., Lau, R. S., & Wang, L. C. (2024). Reporting reliability, convergent and discriminant validity with structural equation modeling: A review and best-practice recommendations. *Asia Pacific Journal of Management, 41*(2), 745–783. https://doi.org/10.1007/s10490-023-09871-y

Chong, A., Yoo, J. S., & Cheshire, C. (2024). Perceptions of fairness in technology-mediated marketplaces. *In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). Association for Computing Machinery.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of Their Unique Relationships With Risk Taking and Job Performance. *Journal of Applied Psychology*, *92*(4), 909–927. https://doi.org/10.1037/0021-9010.92.4.909

Dirks, K. T., & de Jong, B. (2022). Trust Within the Workplace: A Review of Two Waves of Research and a Glimpse of the Third. *Annual Review of Organizational Psychology and Organizational Behavior, 9*(1), 247–276. https://doi.org/10.1146/annurev-orgpsych-012420-083025

Dmitrii, I. D. (2025). The Problem of Digital Trust and Readiness to Use Digital Technologies among Adolescents and Parents in Russia. *Naselenie i Èkonomika, 9*(4), Article e150814. https://doi.org/10.3897/popecon.9.e150814

Dobrygowski, D. (2022). *Losing digital trust will harm technological innovation: Here's how to earn it again.* World Economic Forum. https://www.weforum.org/stories/2022/12/losing-digital-trust-will-harm-technological-innovation/

Dobrygowski, D., & Hoffman, W. (2019, May 28). *We need to build up "digital trust" in tech.* WIRED. https://www.wired.com/story/we-need-to-build-up-digital-trust-in-tech/

Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an experience technology. *Information, Communication & Society, 9*(4), 433–451. https://doi.org/10.1080/13691180600858606

Edelman Trust Institute. (2024a). *2024 Edelman Trust Barometer supplemental report: Insights for the tech sector.* Edelman. https://www.edelman.com/sites/g/files/aatuss191/files/2024-03/2024%20Edelman%20Trust%20Barometer%20Supplemental%20Report%20Insights%20for%20Tech.pdf

Edelman Trust Institute. (2024b). *2024 Edelman Trust Barometer Global Report.* Edelman. https://www.edelman.com/sites/g/files/aatuss191/files/2024-02/2024%20Edelman%20Trust%20Barometer%20Global%20Report_FINAL.pdf

Edelman Trust Institute. (2024c). *2024 Edelman Trust Barometer Singapore Report.* Edelman. https://www.edelman.com/sites/g/files/aatuss191/files/2024-03/2024%20Edelman%20Trust%20Barometer_Singapore%20Report.pdf

European Commission. (2021). *Special Eurobarometer 516: European citizens' knowledge and attitudes towards science and technology.* European Commission. https://europa.eu/eurobarometer/surveys/detail/2237

Mancino, D. (2023, December 6). *Digital literacy in the EU: An overview.* European Union. https://data.europa.eu/en/publications/datastories/digital-literacy-eu-overview

Ferlander, S. (2007). The importance of different forms of social capital for health. *Acta Sociologica, 50*(2), 115–128. https://doi.org/10.1177/0001699307077654

Freitag, M., & Traunmüller, R. (2009). Spheres of trust: An empirical analysis of the foundations of particularised and generalised trust. *European Journal of Political Research, 48*(6), 782–803. https://doi.org/10.1111/j.1475-6765.2009.00849.x

Fricker Jr, R. D., Kulzy, W. W., & Combs, D. J. (2014). *The integrative model of organizational trust as a framework for understanding trust in government.* Naval Postgraduate School.

George, D., & Mallery, P. (2016). *IBM SPSS Statistics 23 step by step: A simple guide and reference* (Fourteenth edition). Routledge. https://doi.org/10.4324/9781315545899

Glanville, J. L., & Paxton, P. (2007). How Do We Learn to Trust? A Confirmatory Tetrad Analysis of the Sources of Generalized Trust. *Social Psychology Quarterly, 70*(3), 230–242. https://doi.org/10.1177/019027250707000303

Hargittai, E., Piper, A. M., & Morris, M. R. (2019). From internet access to internet skills: Digital inequality among older adults. *Universal Access in the information Society, 18*, 881–890. https://doi.org/10.1007/s10209-018-0617-5

Hasan, M. Z., Hussain, M. Z., Fatima, H., Ayub, M., Nosheen, S., Mubarak, Z., Chuhan, S. H., & Mustafa, M. (2023). Explain Ability, Fairness and Trust in Data Systems and Analysis. *In 2023 Computer Applications & Technological Solutions (CATS)* (pp. 1–11). IEEE. http://dx.doi.org/10.1109/cats58046.2023.10424267

Hussain, N., and S. Phulpoto. (2024). Digital Literacy: Empowering Individuals in the Digital Age. *Assyifa Learning Journal, 2*(2), 70–83. https://doi.org/10.61650/alj.v2i2.231

International Social Survey Programme. (2023*). Final source questionnaire: 2024 Digital societies I.* ISSP. https://issp.org/wp-content/uploads/2023/09/ISSP-2024-Digital-Societies-Source-Questionnaire-Aug-2023_FINAL.pdf

Jones-Jang, S. M., Mortensen, T., & Liu, J. (2021). Does Media Literacy Help Identification of Fake News? Information Literacy Helps, but Other Literacies Don’t. *The American Behavioral Scientist (Beverly Hills), 65*(2), 371–388. https://doi.org/10.1177/0002764219869406

Justino, P., & Samarin, M. (2025). *Trust in a changing world: Social cohesion and the social contract in uncertain times (*No. 34/25). United Nations University World Institute for Development Economics Research (UNU-WIDER). https://social.desa.un.org/sites/default/files/inline-files/World%20Social%20Report_Dec2024.pdf

Keefer, P., & Knack, S. (2008). Social capital, social norms and the new institutional economics. In C. Ménard & M. M. Shirley (Eds.), *Handbook of New Institutional Economics* (pp. 701–725). Springer. https://doi.org/10.1007/978-3-540-69305-5_28

Khodyakov, D. (2007). Trust as a Process: A Three-Dimensional Approach. *Sociology (Oxford), 41*(1), 115–132. https://doi.org/10.1177/0038038507072285

Kożuch, B. (2021). The Dimensions of Trust in the Digital Era. In J. Paliszkiewicz & K. Chen (Eds.), *Trust, Organizations and the Digital Economy* (1st ed., pp. 15–26). Routledge. https://doi.org/10.4324/9781003165965

Kuang, Y., Zheng, J., Sun, M., & Xu, X. (2025). The Role of Algorithmic Fairness, Accountability, and Transparency in Shaping User Satisfaction on Digital Platforms: A Quantitative Study in China. *International Journal of Human–Computer Interaction*, 1–17. https://doi.org/10.1080/10447318.2025.2546663

Lee, L. Y. (2025, November 5). Singapore Parliament passes online harms Bill after more than eight hours of debate. *The Straits Times*. https://www.straitstimes.com/singapore/politics/singapore-parliament-passes-online-harms-bill-after-more-than-eight-hours-of-debate

Lippert, S. K. (2001). *An exploratory study into the relevance of trust in the context of information systems technology.* ProQuest Dissertations & Theses.

Lynch, H., Bartley, R., Metcalf, J., Petroni, M., Ahuja, A., & David, S. L. (2016). *Building digital trust: The role of data ethics in the digital age* [Slideshare]. https://www.slideshare.net/AccentureTechnology/building-digital-trust-the-role-ofdata-ethics-in-the-digital-age

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review, 20*(3), 709–734. https://doi.org/10.2307/258792

McKinsey & Company. (2022). *Why digital trust truly matters.* https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trusttruly-matters#/

Meijer, A. (2013). Understanding the Complex Dynamics of Transparency. *Public Administration Review*, *73*(3), 429–439. https://doi.org/10.1111/puar.12032

Microsoft. (2022). *Microsoft Responsible AI Standard, v2.* Microsoft. https://msblogs.thesourcemediaassets.com/sites/5/2022/06/Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf

Ministry of Digital Development and Information. (2021). *MDDI digital readiness survey* [Unpublished raw data].

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organisations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Niehaves, B., Gorbacheva, E., & Plattfaut, R. (2012). Social Aspects in Technology Acceptance: Theory Integration and Development. *2012 45th Hawaii International Conference on System Sciences*, Article 6149206. https://doi.org/10.1109/HICSS.2012.532

Noah, B., & Sethumadhavan, A. (2019). Generational differences in trust in digital assistants. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63*(1), 206–210. https://doi.org/10.1177/1071181319631029

Online Safety (Relief and Accountability) Bill (SG). https://www.parliament.gov.sg/docs/default-source/bills-introduced/online-safety-(relief-and-accountability)-bill-18-2025.pdf?sfvrsn=4cda5d08_1

Parasuraman, A. (2000). Technology Readiness Index (Tri): A Multiple-Item Scale to Measure Readiness to Embrace New Technologies. *Journal of Service Research*, 2(4), 307–320. https://doi.org/10.1177/109467050024001

Park, H., & Blenkinsopp, J. (2011). The roles of transparency and trust in the relationship between corruption and citizen satisfaction. *International Review of Administrative Sciences*, *77*(2), 254–274. https://doi.org/10.1177/0020852311399230

Pi, Y., & Proctor, M. (2025). Toward empowering AI governance with redress mechanisms. *Cambridge Forum on AI Law and Governance, 1*, Article e24. https://doi.org/10.1017/cfl.2025.9

Ping Identity. (2024). *2024 Consumer Survey Singapore Findings*. https://hub.pingidentity.com/surveys/4077-2024-consumer-survey-executive-summary-sg

Ping Identity. (n.d.). *Get to Know Ping Identity.* https://www.pingidentity.com/en/company/about-us.html

Prime Minister's Office. (2024a, October 1). *PM Lawrence Wong at the launch of Smart Nation 2.0* [Press release]. https://www.pmo.gov.sg/newsroom/pm-lawrence-wong-at-the-launch-of-smart-nation/

Prime Minister's Office. (2024b, October 15). *SM Teo Chee Hean at the SICW 2024 opening ceremony* [Press release]. https://www.pmo.gov.sg/newsroom/sm-teo-chee-hean-at-the-opening-of-sicw-2024/

Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community.* Simon & Schuster.

Putnam, R. D., Leonardi, R., & Nanetti, R. (1993). *Making democracy work: Civic traditions in modern Italy.* Princeton University Press. https://doi.org/10.1515/9781400820740

PwC. (2018). *The journey to digital trust.* https://www.pwc.com/sg/en/publications/assets/the-journey-to-digital-trust-2019.pdf

Rosli, N. N. (2025). From service failures to customer loyalty: A holistic review of service recovery performance. *International Journal of Entrepreneurship and Management Practices, 8*(29), 163–175. https://doi.org/10.35631/ijemp.829012

Royal, K. (2017). Using the Spearman–Brown prophecy formula to improve medical school examination quality. *Journal of Contemporary Medical Education, 5*(2), 51–53. https://doi.org/10.5455/jcme.20170705091608

Saveljeva, J., & Volkova, T. (2025). A Survey on Digital Trust: Towards a Validated Definition. *Digital*, *5*(2), Article 14. https://doi.org/10.3390/digital5020014

SGS. (2025). *The dimensions of digital trust.* https://www.sgs.com/-/media/sgscorp/documents/corporate/white-papers/sgs-ba-digital-trust-assurance-white-paper-en.cdn.en.pdf

Shell, M. A., & Buell, R. W. (2019). Why anxious customers prefer human customer service. *Harvard Business Review*. https://hbr.org/2019/04/why-anxious-customers-prefer-human-customer-service

Singapore Police Force. (2025). *SPF Annual Report 2024*. https://www.police.gov.sg/-/media/SPF/Files/Publications/PDF/SPF-Annual-Report-2024.pdf

Thales. (2025). *Digital Trust Index: Understanding How Digital Experiences Affect Consumer Trust*. https://cpl.thalesgroup.com/digital-trust-index#form-download

van Griethuijsen, R. A. L. F., van Eijck, M. W., Haste, H., den Brok, P. J., Skinner, N. C., Mansour, N., Savran Gencer, A., & BouJaoude, S. (2015). Global Patterns in Students' Views of Science and Interest in Science. *Research in Science Education, 45*(4), Article A005. https://doi.org/10.1007/s11165-014-9438-6

Walther, J. B., & Bunz, U. (2005). The rules of virtual groups: Trust, liking, and performance in computer-mediated communication*. Journal of Communication*, *55*(4), 828–846. https://doi.org/10.1111/j.1460-2466.2005.tb03025.x

WEF. (2021). *Advancing Digital Safety: A Framework to Align Global Action.* World Economic Forum. https://www3.weforum.org/docs/WEF_Advancing_Digital_Safety_A_Framework_to_Align_Global_Action_2021.pdf

WEF. (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies.* World Economic Forum. https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf

WEF. (2023). *Measuring Digital Trust: Supporting Decision-Making for Trustworthy Technologies.* World Economic Forum. https://www3.weforum.org/docs/WEF_Measuring_Digital_Trust_2023.pdf

WEF. (2024). *Digital Trust: Supporting Individual Agency.* World Economic Forum. https://www3.weforum.org/docs/WEF_Digital_Trust_Supporting_Individual_Agency_2024.pdf

Wu, J.-J., Chen, Y.-H., & Chung, Y.-S. (2010). Trust factors influencing virtual community members: A study of transaction communities. *Journal of Business Research, 63*(9 10), 1025–1032.

Zhou, J., Verma, S., Mittal, M., & Chen, F. (2021). *Understanding Relations Between Perception of Fairness and Trust in Algorithmic Decision Making.* arXiv. https://doi.org/10.48550/arxiv.2109.14345

APPENDICES

Appendix A: Methodology

The survey data was collected by IPS Social Lab online panel. Only Singapore Citizens and Permanent Residents aged 21 years and above were eligible to participate in the online survey. The self-administered survey was available in English only. The fieldwork took place from October to November 2024.

Figure A1: Representation by Citizenship

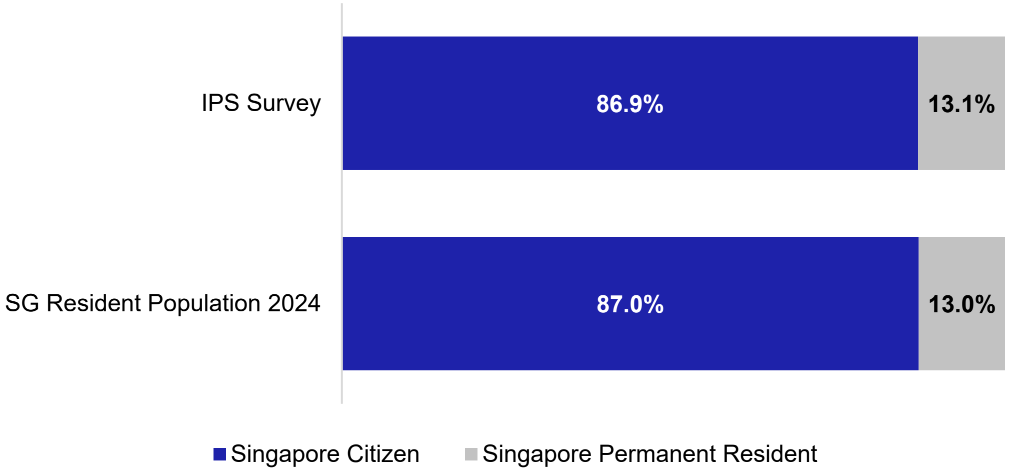


Figure A2: Representation by Gender

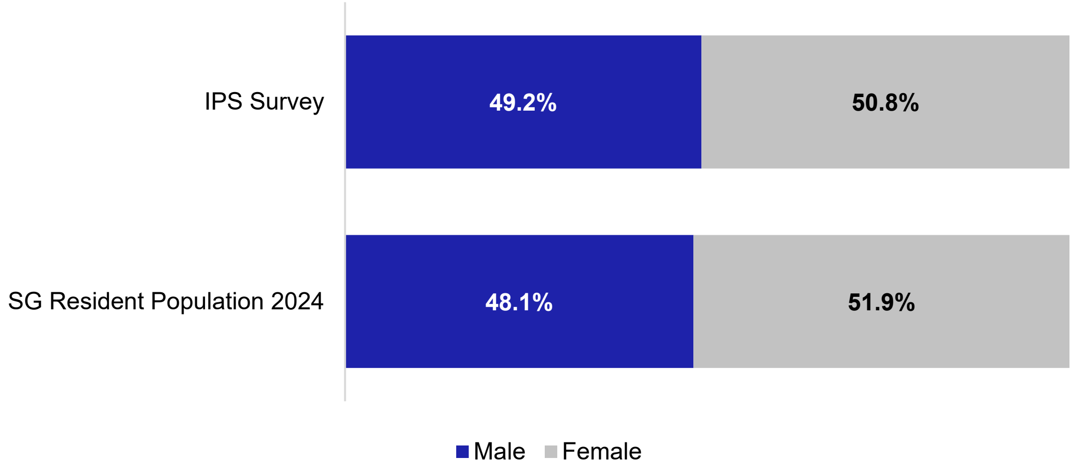


Figure A3: Representation by Race

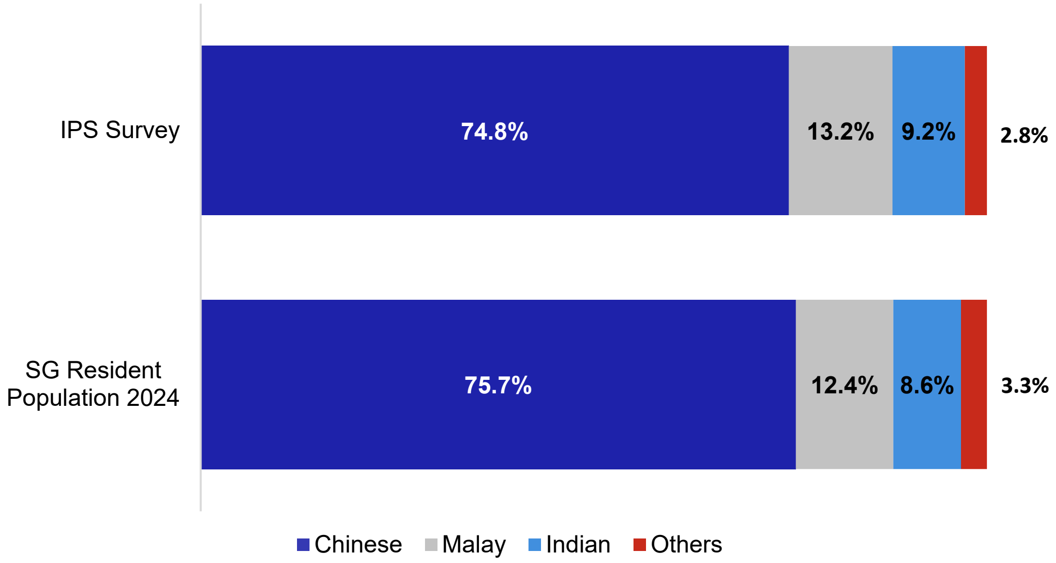


Figure A4: Representation by Age

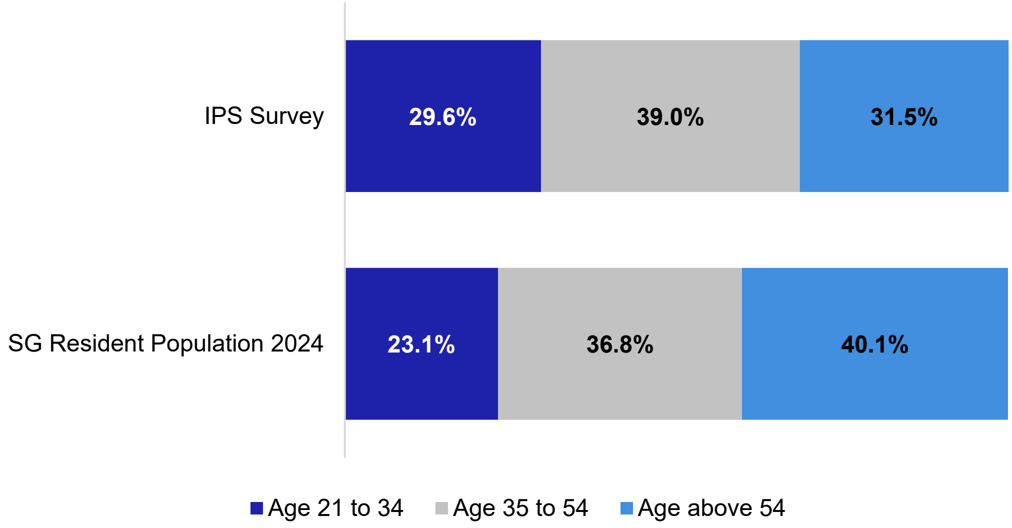


Figure A5: Representation by Housing

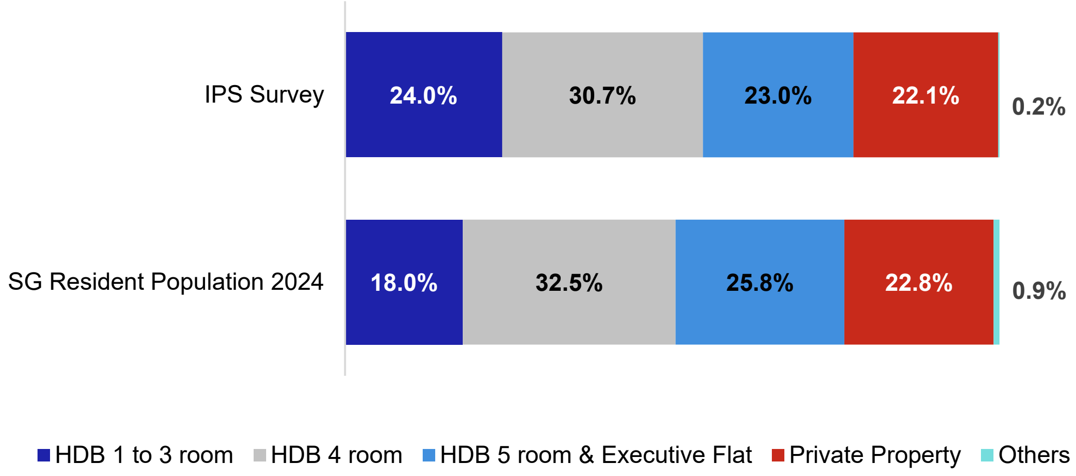
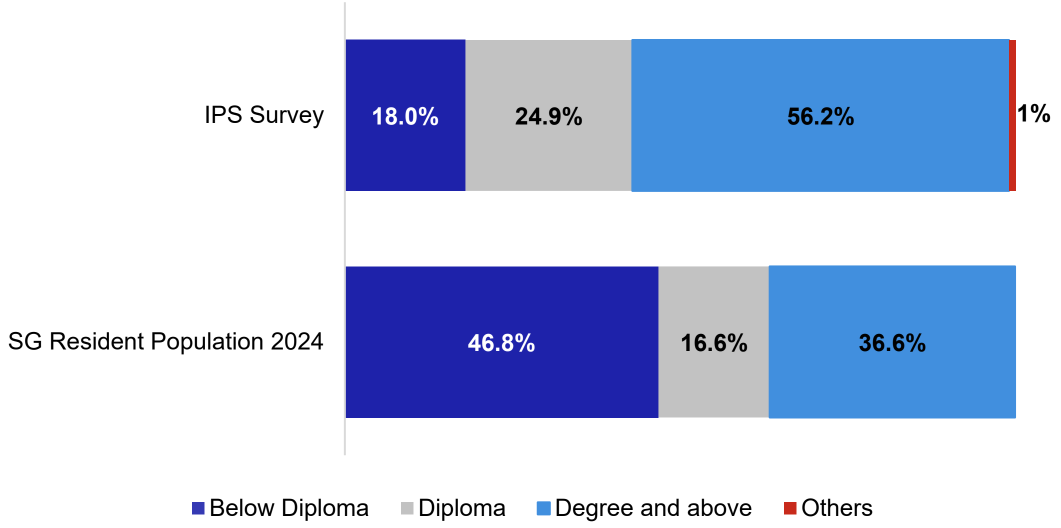


Figure A6: Representation by Education Attainment



Appendix B: About the Authors

CHEW Han Ei leads the Governance & Economy cluster at the Institute of Policy Studies (IPS). His work focuses on quantitative policy research, with a strong interest in online harms, digital trust and technology adoption.

He has served as Principal Investigator for multiple large-scale research grants and collaborates closely with public agencies to inform decision-making and policy development. His approach is empirically grounded and hands-on — from designing social science research projects to leading data analyses that shape real-world outcomes.

Outside of IPS, Han Ei serves on the board of SG Her Empowerment and is a pro bono Research Consultant to UNESCO. Some of his key international projects for UNESCO include "Reading in the Mobile Era: A Study of Mobile Reading in Developing Countries" and "I'd Blush If I Could: Closing Gender Divides in Digital Skills through Education".

Han Ei earned his PhD in Media and Information Studies from Michigan State University. He also writes *The Chart Doctor Has Issues* — a Substack newsletter on data storytelling, visual best practices and the occasional chart takedown.

Carol **SOON** is Deputy Head and Associate Professor (Practice) at the Department of Communications and New Media in the National University of Singapore (NUS). She is a member of the World Economic Forum's Global

Future Council on Information Integrity (2025 to 2026) and Principal Investigator at the NUS Centre for Trusted Internet and Community. She is also Adjunct Principal Scientist at the Centre for Advanced Technologies in Online Safety (CATOS) that is set up by Singapore's Ministry of Digital Development and Information.

Her research interests are in media regulation and digital policy, social media governance, digital literacy and policy communication. Dr Soon has written over 50 media commentaries on the impact of technology, media regulation, digital literacy and digital upskilling of citizens and workers, and public communication. She has single-authored and co-authored more than 80 research reports, journal articles, book chapters and conference papers. Her book, *Mobile Communication and Online Falsehoods: Trends, Impact and Practice*, published by Springer Nature in 2023, addresses existing gaps in research and practice in the management of online falsehoods on instant messaging platforms in Asia.

Dr Soon is currently Vice Chair of Singapore's Media Literacy Council. She is also a member of the Ministry of Culture, Community and Youth's Co-Governance Community of Practice, and serves on the National Crime Prevention Council.

KAM Tai Tong was Research Fellow at the Institute of Policy Studies from August 2024 to January 2025, when he worked on the paper.

Harkiran **KAUR** is a research assistant at the Institute of Policy Studies (Lee Kuan Yew School of Public Policy, National University of Singapore). Her research focuses on the social and policy impacts of digital media and the internet, covering topics like digital literacy, online safety and artificial intelligence. She holds a Bachelor's degree in Social Sciences from Singapore Management University.

CHIN Shuen Lin was a research intern at the Institute of Policy Studies.

About IPS Working Paper Series

The IPS Working Papers Series is published in-house for early dissemination of works-in-progress. This may be research carried out by IPS researchers, work commissioned by the Institute or work submitted to the Institute for publication.

The views expressed in the Working Papers are strictly those of the author(s) alone and do not necessarily reflect the views of the IPS.

Comments on the Working Papers are invited. Please direct your comments and queries to the author(s).

IPS Working Papers are available from the IPS at $7.00 each (before GST). Postage and handling charges will be added for mail orders.

For more information, please visit www.lkyspp.nus.edu.sg/ips or
contact email: ips@nus.edu.sg.

Institute of Policy Studies
Lee Kuan Yew School of Public
Policy National University of
Singapore
1C Cluny Road House 5
Singapore 259599

Web: www.lkyspp.nus.edu.sg/ips
Registration Number: 200604346E