

Digital Policy

The Green Party supports equitable access to digital technologies, services, and data. We will take a harm-based approach to digital technology, including social media, AI, and quantum computing, policy that upholds Te Tiriti o Waitangi and protects people's privacy and online safety.

Vision

Digital environments are secure, support our well-being, connect people, and respect sovereignty.

Values and Principles

- *Whanaungatanga*: Data and digital systems should empower secure, meaningful, and mutually beneficial connections between people. Digital management must be accountable, transparent, and responsible.
- *Rangatiratanga*: Data and digital systems honour Te Tiriti o Waitangi, tikanga Māori, and mātauranga Māori, with decisions made by those affected. Data sovereignty is paramount. Data is a taonga and people must have control and ownership over their data.
- *Manaakitanga*: Digital systems offer innovative ways to foster community and enable communities to build social cohesion. Everyone is brought together, whether online or not.
- *Akoranga*: All communities should be able to participate digitally. Digital systems can help us learn and build our capacity. They must be accessible, understandable, and responsive to the needs of connected people and the environment.
- *Kotahitanga*: Data and digital systems must be designed and operated to benefit and respect people, communities, individuals, and the environment. Digital infrastructure is a public good and must be reliable and available for all people to use if they want to.
- *Kaitiakitanga*: Digital systems can negatively affect people and the environment and require protection from misuse and exploitation. Digital systems should reduce waste and pollution, not contribute to it.

Strategic Priorities

The Green Party's strategic goals include:

"As a Party we strive to create a more connected, compassionate, and equal Aotearoa, free from structural biases that discriminate against groups and individuals."

"All people will be empowered to shape the systems that affect them through community engagement enabled by good evidence, co-design, and adequate resourcing."

Actions in this policy that work towards these goals include:

- Use a harm-based approach to regulating autonomous decision-making software. [...] (1.1.3)
- Limit the use of automated or mass surveillance by government and strengthen regulations for surveillance done by individuals. (2.4.2)
- Establish standards for data quality in public decision-making. (3.1.1)
- Provide free internet access in appropriate places, including marae and public spaces such as schools, hospitals, libraries, and public transit. (4.1.2)
- Require digital items manufactured or used domestically to be repairable and require retailers to support the right to repair, including by providing component parts. (5.2.1)
- Refine public data collection systems to reflect tikanga and mātauranga Māori. (6.2.1)

Connected Policies

Our [Research, Science and Technology](#) explores the development and regulation of technologies in general. Digital technologies are an integral part of [Business](#) innovation, supported by digital [Education](#).

Policy Positions

1. Autonomous decision-making systems

Issues

Algorithms can be biased black boxes that increasingly shape our thinking, lives, and decision-making. Whilst they have many potential benefits and uses, they are also difficult to challenge or scrutinise and can potentially amplify misinformation, cause harm to people, society, compromise privacy, create dehumanising outcomes, and diminish livelihoods. When organisations hide responsibility behind an algorithm, people are abused without accountability.

Actions

- 1.1. Ensure that accountability and oversight of software that autonomously makes decisions are transparent and independent, including by:
 - 1.1.1. Requiring providers of autonomous decision-making software to demonstrate that they have minimised harmful biases and provided a means of appealing decisions to a human decision-maker;
 - 1.1.2. Requiring algorithmically generated content (often referred to as artificial intelligence (AI) content) to be easily identifiable, e.g., watermarked, so that it can be isolated; and
 - 1.1.3. Using a harm-based approach to regulating autonomous decision-making software, including prohibiting uses for the purpose of:
 - 1.1.3.1. Subliminal or deceptive manipulation;
 - 1.1.3.2. Exploiting vulnerable people or groups;
 - 1.1.3.3. Social scoring and tracking;
 - 1.1.3.4. Predicting criminality;
 - 1.1.3.5. Emotion recognition; and/or

- 1.1.3.6. Remote Biometric Identification, including remote facial and emotion recognition (FRT).

2. Digital privacy and information security

Issues

Digital technologies make constant, widespread, and long-term data collection and correlation both routine and easy. Their increased use by the public and private sectors, for security, convenience, and identity verification, is making personal surveillance ever more pervasive and persistent, undermining privacy.

Actions

- 2.1. Support anonymity online, including by:
 - 2.1.1. Encouraging digital systems to allow anonymous use;
 - 2.1.2. Removing trackers from publicly funded digital services; and
 - 2.1.3. Limiting ID verification for digital services outside government without strong security protections for ID documents.
- 2.2. Strengthen digital privacy protections, including by:
 - 2.2.1. Providing for a right to privacy and meaningful privacy protection within data regulation;
 - 2.2.2. Regulating all data brokers and all sales or commercial exchange of information about people; and
 - 2.2.3. Supporting end-to-end encryption and opposing all “backdoors” or other weaknesses for state access.
- 2.3. Limit digital surveillance, including by:
 - 2.3.1. Developing a framework for consistently sharing information between agencies that reduces the need for state surveillance and only uses information for the purpose and consented reasons for which it was collected;
 - 2.3.2. Limiting the use of automated or mass surveillance by the government and strengthening regulations for surveillance done by individuals; and
 - 2.3.3. Prohibiting tracking in the home through digital devices, such as by landlords and employers.
- 2.4. Ensure that the Privacy Commissioner can effectively protect everyone’s privacy, including by:
 - 2.4.1. Empowering the Privacy Commission to investigate and enforce privacy protections for people living in Aotearoa New Zealand and overseas New Zealanders; and
 - 2.4.2. Empowering the Privacy Commissioner to audit publicly funded digital systems, including designs before they are built, to ensure privacy by design.
- 2.5. Ensure that critical digital systems are resilient and well protected, including by:
 - 2.5.1. Regulating digital surveillance devices, including home surveillance, to require strong security and encryption;

- 2.5.2. Expanding consumer protection laws to include all digital products; and
- 2.5.3. Requiring commercial subscription software to promptly correct defects and security vulnerabilities, and disclose security breaches.

3. Data governance

Issues

Users of digital tools, platforms, and systems are often required to sign away personal information and privacy as part of the platform's terms of service. Poor data quality is a source of great expense to everyone and of harm to people.

Actions

- 3.1. Ensure that public decision-making is supported by high-quality data and analysis, including by:
 - 3.1.1. Establishing standards for data quality in public decision-making;
 - 3.1.2. Regularly and transparently assessing the quality of data that is used in public decision-making, and appropriately explaining why poor-quality data is used when it is used; and
 - 3.1.3. Supporting public servants to be digitally literate and requiring agencies to maintain internal digital expertise.
- 3.2. Maximise the accessibility and availability of data without putting privacy at risk, including by:
 - 3.2.1. Ensure that the public service has the resourcing and capability to maintain comprehensive archives of Government data that is managed according to the Public Records Act;
 - 3.2.2. Require publicly funded agencies to adopt the open contracting data standard; and
 - 3.2.3. Publish digital material and open data funded by the government where permitted under the OIA.

4. Digital inclusion

Issues

Due to the increasing reliance on digital technologies across many core aspects of society, groups that are less able to access digital systems are increasingly disadvantaged. Furthermore, experiences in digital systems can be inequitable due to design choices, policy decisions, and digital structures that do not account for diverse users and serve to entrench the digital divide.

Actions

- 4.1. Enable people to participate equitably in digital services, including by:
 - 4.1.1. Ensuring all communities have access to the internet and telecommunications through publicly provided infrastructure;
 - 4.1.2. Providing free internet access in appropriate places, including marae and public spaces such as schools, hospitals, libraries, and public transit;

- 4.1.3. Ensuring digital government services are accessible to end users, work well on older devices and software, and load efficiently on low-speed internet connections;
- 4.1.4. Requiring digital services and platforms to provide accessibility tools, such as text-to-speech and subtitles, in easy-to-access formats; and
- 4.1.5. Protecting net neutrality by requiring network companies to provide equal standards of digital services to all users.
- 4.2. Ensure that accessible alternatives to digital services remain available for core aspects of society, including by:
 - 4.2.1. Requiring essential services, whether provided by the public or private sector, to provide offline access; and
 - 4.2.2. Requiring vendors to accept cash for payments, including government services, without exception.
- 4.3. Localise the benefits of digital systems, including by:
 - 4.3.1. Requiring Government agencies to, when procuring digital products and services:
 - 4.3.1.1. Report digital expenditure going to overseas and domestic digital companies;
 - 4.3.1.2. Use a procurement system that enables domestic providers to bid for the work;
 - 4.3.1.3. Prioritise local providers in procurement, including enabling small providers to achieve individual pieces of work; and
 - 4.3.1.4. Comply with relevant open standards.
 - 4.3.2. Requiring publicly funded agencies to use free and open-source software to the greatest extent possible; and
 - 4.3.3. Improving Aotearoa New Zealand's data sovereignty by strengthening local digital infrastructure.

5. Environmental impacts

Issues

Although digital spaces can provide a range of benefits to human experience, the environmental impact of providing those spaces is increasing. Recent research highlights that emissions from digital infrastructure are likely significantly higher than is reported by large technological industry representatives, and other issues such as waste production and water consumption associated with data management and digital infrastructure are increasing in prevalence and awareness.

Actions

- 5.1. Ensure that Aotearoa New Zealand plays its part in reducing the environmental impacts of digital systems, including by:

- 5.1.1. Requiring all publicly funded agencies to optimise digital systems to reduce energy intensity and waste production as well as report on their emissions and environmental impacts;
 - 5.1.2. Requiring domestic manufacturers, producers, and retailers of digital systems to meet waste diversion and environmental efficiency standards, and to report on their compliance; and
 - 5.1.3. Ratifying the UN Convention on Access to Information, Public Participation in Decision-making, and Access to Justice in Environmental Matters.
- 5.2. Maximise the useful life of digital items, including by:
- 5.2.1. Requiring digital items manufactured or used domestically to be repairable and requiring retailers to support the right to repair, including by providing component parts; and
 - 5.2.2. Prohibiting manufacturers from remotely disabling domestically sold physical goods and ensuring they function offline wherever possible.

6. Te Tiriti and digital systems

Issues

Māori are increasingly losing control and sovereignty over their collective cultural knowledge, data, and technology. This is through systems that include patent, copyright, and trademark laws that favour exploitation and profiteering.

Actions

- 6.1. Ensuring that data about Māori is produced and held by Māori wherever possible, including by:
 - 6.1.1. Resource and support Māori-designed and -led data infrastructure systems to hold Māori data; and
 - 6.1.2. Holding individuals and organisations handling Māori data accountable to the Māori communities, groups, and individuals it comes from.
- 6.2. Establish and support Māori rights and interests in relation to data collected by the government and data derived from research, including by:
 - 6.2.1. Refining public data collection systems to reflect tikanga and mātauranga Māori.