Draft Digital Principles

Digital solutions are being proposed to advance objectives for improving quality of life in waterfront neighbourhoods. When considering and evaluating solutions, Waterfront Toronto is focused on:

- Ensuring that personal privacy, civil liberties and human dignity are protected;
- Providing shared benefits, including an economic catalyst for open innovation;
- Informing the broader public policy dialogue on digital technology and data;
- Determining whether technology is the right answer to the challenge or opportunity; and
- Future-proofing emerging neighbourhoods, ensuring resiliency and adaptability.

These draft principles have been developed through our recent Civic Labs and are informed by the work of cities around the world, including the efforts of the *Cities Coalition for Digital Rights*. They also incorporate feedback from a public consultation on a prior version. We will next engage our Digital Strategy Advisory Panel for their expertise and guidance.

It is important to note that any projects or proposals made for the waterfront would need to fully comply with all applicable legislative and regulatory requirements, including:

- Canadian Charter of Rights and Freedoms
- Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada)
- Privacy Act (Canada)
- Municipal Freedom of Information and Protection of Privacy Act (Ontario)
- Freedom of Information and Protection of Privacy Act (Ontario)
- Any new legal/regulatory requirements which may be introduced or amended.

The core foundation of these draft Principles is that any project proposed to Waterfront Toronto must represent **ethically responsible innovation that reflects public values and preserves or enhances the public good.**

Principle #1: Everyone will have access to, and benefit equally from, digital solutions

This includes:

- Universal access to affordable internet, inclusive design of digital solutions on equitable terms, and the digital literacy efforts to promote the skills to use these resources.
- Creating opportunities for individuals and groups to engage with their community through open, participatory and transparent digital processes.
- Identifying and, to the extent possible, mitigating any potential bias against or marginalization of an individual or group.
- Sharing, as appropriate, non-personal and de-identified data collected with government-provided open data portals, the research community or other third-party organizations who are contributing to the advancement of the public good.
- Designing digital solutions and accompanying commercial terms to minimize the impacts of information asymmetry.

Principle #2: Digital solutions will be open, ethical, and resilient

This includes:

- Use of protocols, standards and operating agreements that do not foster monopolies, barriers to entry, vendor lock-in, or dependency on a sole vendor to provide related products or services.
- Providing digital solutions through open and ethical digital service standards.
- Ensuring digital solutions are developed and operate using only ethically sourced data.
- Requiring that solutions – particularly those related to infrastructure – be secure and resilient, including the implementation of measures allowing for safe failure.

Principle #3: Everyone will be able to understand how their data is being collected and used, and how organizations can and will be held accountable for their practices

This includes:

- Specific measures to ensure transparency of collection, use, retention and disclosure of personal data.
- Mechanisms to proactively address concerns about the potential misuse of data by fulfilling individuals' rights to access, review and correct their data.
- Access to understandable and accurate information about the digital solutions (including underlying algorithms or artificial intelligence) that are proposed or adopted, and the ability to question and change unfair, biased or discriminatory systems.
- Ability to override automated decisions that are inconsistent with the public good.
- Review of any proposed project that could have a significant impact on a person or group by the Waterfront Toronto Digital Strategy Advisory Panel prior to implementation.
- Active monitoring of compliance with these principles to ensure the objectives are achieved and maintained, and public access to the results of these compliance reviews.
- Requiring that the organization responsible for any proposed project must demonstrate knowledge of, and adherence to, any applicable guidance published by a relevant regulator (such as the Privacy Commissioner of Canada or the Information and Privacy Commissioner of Ontario).

- Requiring that organizations be willing to comply with any investigation, audit or other compliance action by an applicable regulator, including where such cooperation is "voluntary" under the regulation.

Principle #4: Strong privacy protections will be in place at all times

This includes:

- All initiatives and products that use personal data will be the subject of a published Privacy Impact Assessment to identify privacy risks and corresponding mitigation strategies before implementation.
- Embedding privacy in any initiative or product development through Privacy by Design.
- Collection of personal data by, or on behalf of, government agencies must be accompanied by a demonstration of necessity and appropriate notice to individuals. Collection of personal data by businesses requires informed consent, full identification of purposes (in a contextually appropriate form), and clear options to not provide, and to later withdraw, consent.
- Minimization of collection, use, retention and disclosure to what is necessary for the provision of identified and approved services that demonstrate benefit to individuals. This includes limiting collection through, among other measures, the use of non-identifying technology (e.g. motion sensors rather than cameras) and automatic deletion of identifiable data when no longer required.
- De-identification of personal data at source, unless the collecting organization has obtained consent – or, in the case of government, demonstrated necessity – to store the data in identifiable form.
- Prohibiting profiling, without demonstrated necessity or informed consent by government or without informed consent by business, for any purpose.
- Prohibiting data collected within waterfront projects from being used for advertising purposes without express positive consent.
- Protecting data through appropriate security measures, mandatory breach notification, and prohibitions against disclosure without consent (except where explicitly permitted by law).

Principle #5: Data and systems will remain under local control and be subject to local laws

This includes:

- Granular policies regarding data residency and routing that are informed by legislative requirements, global best practices and project objectives (e.g., potential research and development exemptions, support escalation requirements, etc.), which policies would be adopted and made public.
- As a first principle, data collected in waterfront neighbourhoods will remain in Canada.
- Decision-makers (including individuals) have the freedom to use the technologies of their choice, and expect the same level of interoperability, inclusion and opportunity in their digital services.
- Adaptability of solutions to new legislative or regulatory conditions that may emerge.