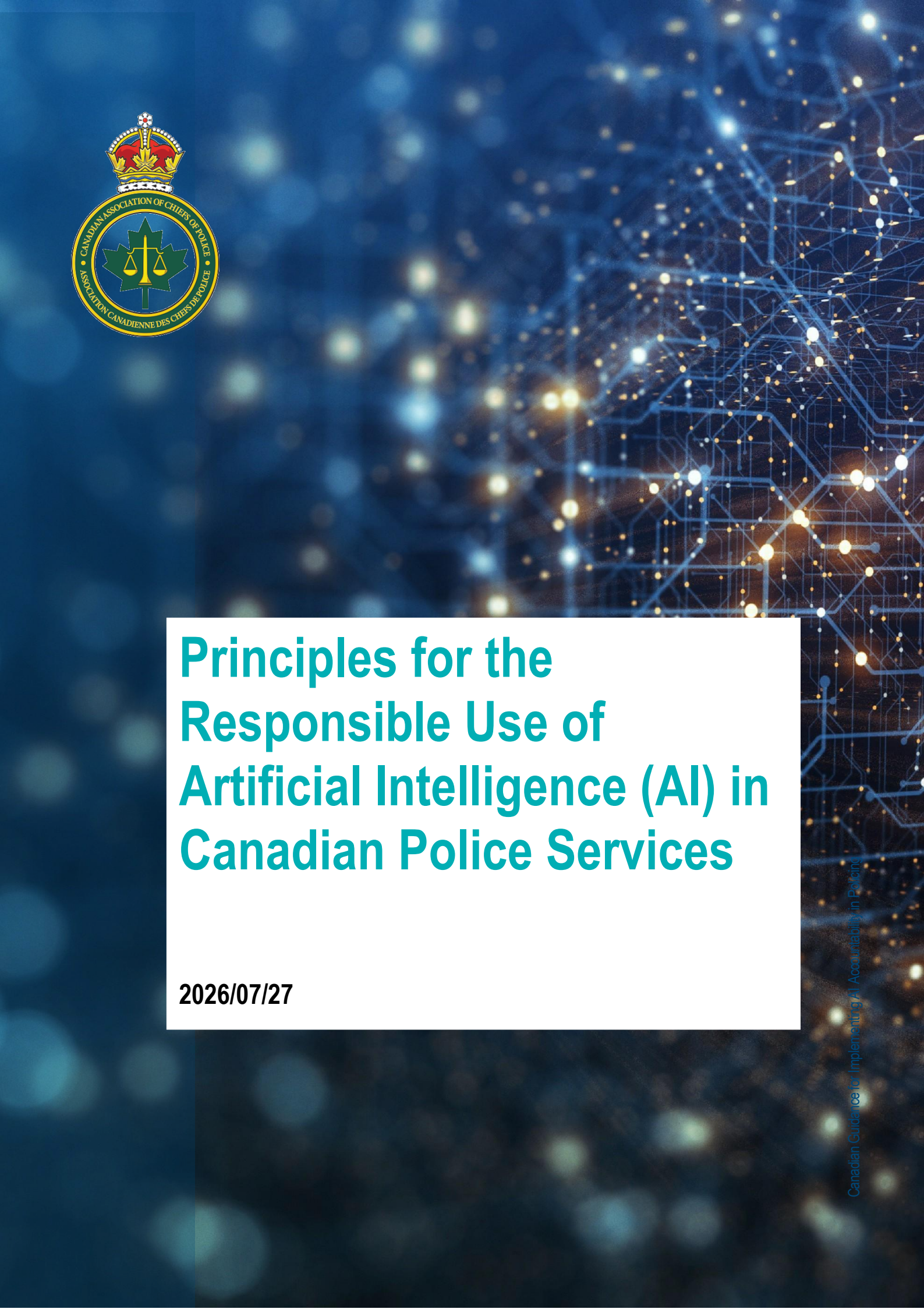


Principles for the Responsible Use of Artificial Intelligence (AI) in Canadian Police Services

2026/07/27

Introduction

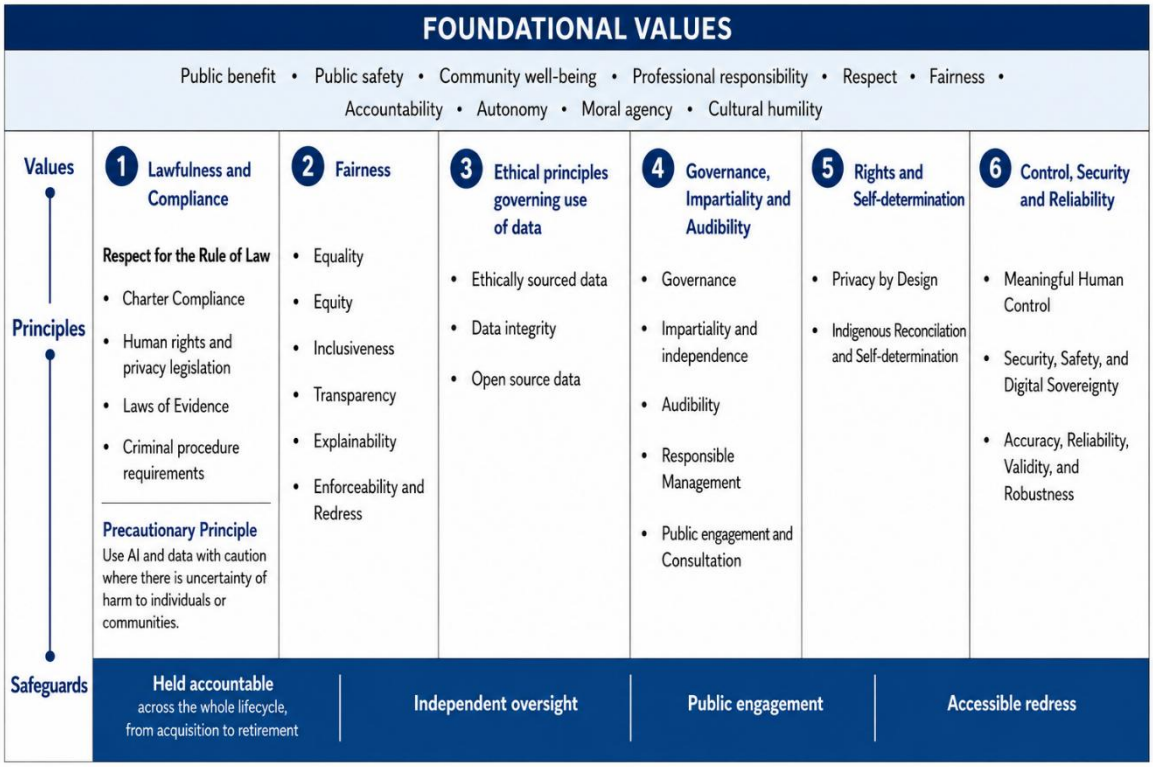
Artificial intelligence integration is necessary in Canadian policing to protect our communities from existing and evolving threats. For policing, the strategic question is no longer whether AI will be used, but whether it will be governed in a way that preserves public trust and the rule of law while improving public safety. Recognizing this challenge, the CACP has developed ethical principles to guide the use of AI tools and promotes the use of a commonly shared rigorous documentation and risk assessment tool that monitors and follows operational AI tools through all stages of its life cycle.

Although Canadian police services operate under municipal, provincial, and federal jurisdictions with differing expectations, they share common commitments; upholding the rule of law, respect for human rights, preventing crime, ensuring public safety, fostering community well-being, consulting with their communities, professional development, and earning public trust.

Canadian police also share common values; public service, professionalism, accountability, respecting the autonomy and moral agency of others, cultural humility, and fairness in its many iterations — equality, equity, impartiality, objectivity, transparency, and procedural justice. From these values follow ethical AI principles, applying at every stage of an AI tool's life, from determining need and purpose, design, testing, procurement, implementation, monitoring, auditing to decommissioning.

As a profession Canadian police understand the importance of innovation in improving operations and service delivery. Used legally and ethically AI tools can help solve serious crimes, find missing people, support victims, and spare officers repeated exposure to traumatic material. Without appropriate guidance and oversight, however, AI can entrench bias, erode privacy, undermine human rights, compromise the rule of law, and diminish public trust in policing.

The principles described in this document serve two purposes. Lawfulness and Compliance and ethical principles establish guidance for how police adopt and use AI, balancing public with fundamental rights and freedoms, while stipulating police responsibilities to their communities. Secondly, these principles demonstrate our commitment to transparency and accountability.



Lawfulness and Compliance

Respect for the Rule of Law

Use of AI tools must comply with the Canadian Charter of Rights and Freedoms, the laws of evidence, federal and provincial human rights and privacy legislation, criminal procedure requirements, international laws, and organizational policies.

Where applicable, AI tools must comply with tort, administrative, contract law, and laws governing police and law enforcement.

Precautionary Principle

An AI tool should be assessed to consider compliance with the rule of law before it is adopted. The AI tool should be treated with caution and an appropriate risk level applied before it is relied on, having due regard to the AI tool's scope, purpose, impact. A precautionary approach recommends that tools are screened for compliance with the rule of law before deployment.[1]

[1] We are grateful to the Law Commission of Ontario for recommending a precautionary principle regarding adoption of AI. See their forthcoming report *Artificial Intelligence in Criminal Justice: Final Report and Recommendations (Toronto: Forthcoming August 2026)*

Ethical Principles

These ethical principles complement the rule of law and align with operational principles developed and validated by the Centre of Excellence in Research in Terrorism, Resilience, Intelligence, Organized Crime (CENTRIC).

The principles also align with the CACP/CENTRIC Canadian AI Accountability for Policing and Security (C-AIPAS) documentation and risk assessment tool and C-AIPAS operational principles.

The ethical principles fall into five groups:

1. Fairness
2. Ethical principles governing use of data
3. Governance, impartiality, and auditability
4. Rights and self-determination
5. Control, Security and Reliability

These principles set a standard higher than what is required by law, and they will sometimes need to be balanced against one another. When they do, this document is explicit about how the tension is addressed. Some protections cannot be compromised. Risks are balanced through reasoned, documented, and independently reviewable judgment, with the more protective option preferred where the outcome is uncertain. The whole framework operates under independent oversight and public engagement, so that AI in policing remains lawful, accountable, and worthy of public trust.

Guiding ethical principles are not sufficient to avoid negative impacts. The use of C-AIPAS operational principles and the C-AIPAS documentation and risk assessment tool is recommended as best practice in policing.

Ethical Principles Governing the use of AI Tools

In the absence of law these ethical principles offer guidance to police. The principles of fairness provide guidance on balancing competing interests. AI tools satisfy these principles before deployment. In-use AI tools are screened to align with these principles.

1. Fairness

The principles of fairness require that AI tools treat people without harmful bias, and that benefits and burdens fall equitably across affected communities. They cover equality in treatment, equity that corrects rather than entrenches disadvantage, inclusiveness so that no affected group is left out, and data that is ethically sourced and representative of the populations affected by an AI tool.

1.a Equality

Human rights legislation requires all people to be treated equally without prejudice. AI tools must be free of biases resulting in unequal and harmful treatment.

1.b Equity

Treating people equally may result in inequalities. The principle of equity arose to correct inequalities by treating people in accordance with different situational needs. The principle of equity requires identifying, analyzing, and correcting inequalities through outreach and collaboration with racialized communities.

1.c Inclusiveness

The principle of inclusiveness ensures no one is left out in consultations, data collection, communications, protection of rights, and redress.[2]

1.d Transparency

Transparency refers to the importance of having access to information to ensure fairness in agreements and decision making.

Transparency enables AI accountability when clear, accurate and meaningful information is open to scrutiny, allowing the public to make informed judgements of police use, responsible management, and governance of AI tools. Police have a right to non-disclosure of specific AI tools if transparency prepares bad actors to avoid detection.

Police must be transparent concerning how human rights are protected through the entire AI ecosystem, including design, development, procurement, implementation, use, operational updates, data storage, decommissioning, and governance.

[2] CENTRIC. (2025). *AIPAS: AI accountability for policing and security: Guidance for implementing AI accountability in policing*.

1.e Explainability

Explainability is a fundamental attribute of transparency, ensuring that transparent communication regarding the purpose, scope, data source, data security and storage, operation, use, risk level, risk mitigation measures, and public benefit of AI tools is clear and easily understood.

Use of adaptive or continually learning AI tools, where internal operation cannot be easily explained, must be explained in terms of constant monitoring of consistent outputs, updating of risk assessments, and public benefit that justifies use.

1.f Enforceability and redress

Appealing decisions to remedy unfair outcomes is an important part of procedural justice. Appealing decisions or complaining about adverse outcomes is only possible if a clear process for appeals or complaints, whether external or internal, is easily accessible, understood, and complete.[3]

2. Ethical principles governing use of data

2.a. Ethically sourced data

Legally sourced data requires protection of personal information under federal and provincial privacy acts. Ethically sourced data involves communicating the purpose of the proposed research project, voluntary agreement to participate, and ensuring anonymity of participants.

Consideration should also be given to whether the data's use aligns with the circumstances under which it was originally collected and the reasonable expectations of affected individuals and communities.

2.b. Data Integrity

Data integrity requires training data that is legally and ethically sourced; obtained from identifiable and documented sources; representative of affected populations; large enough to provide valid results; coded and analyzed without stigmatizing or revictimizing racialized or equity-seeking groups; and securely stored consistent with Canadian data sovereignty. Training data must be tested under real world conditions.

Police services should assess whether training data is lawful, accurate, reliable, relevant, representative, and appropriate for the intended purpose.

2.c. Open-source data

Open-source data refers to publicly available information newspaper and academic articles, the internet, social media platforms, public records, and other easily accessible online resources. Criminals use open-source data for a wide variety of unlawful purposes: fraud, human trafficking, organized crime, terrorism, even war crimes. Police use open-source data to ensure public safety and security. In doing so police must respect licenses and copyright where applicable and conform with the principles of data integrity, training data, and privacy impact assessments. Use of open-source data must be open to reasonable considerations of privacy.[4]

[3] CENTRIC. (2025). *AIPAS: AI accountability for policing and security: Guidance for implementing AI accountability in policing*.

[4] Consistent with RCMP use of open source data - https://rcmp.ca/en/corporate-information/access-information-and-privacy/privacy-impact-assessments/collection-and-use-open-source-information-internet. Retrieved July 27, 2026.

3. Impartiality, Governance, and Auditability

These principles establish the structures that ensure AI use is accountable. They cover oversight by an impartial body independent of the units that deploy the tools, systems whose operation and use can be audited, responsible management of each tool across its life, and engagement with our communities, who have a stake in the knowledge that AI tools benefit public safety while possible harms have been considered and addressed.

3.a Governance

In addition to already established oversight boards, police services should establish an AI Governance Committee drawn from community representatives including members from academia, law, private sector, and racialized community members.

3.b Impartiality and Independence

Oversight of AI use must rest with an impartial body independent of the units deploying the tools. It should have authority to confirm that tools align with these principles and to require corrective action or withdrawal where they do not. Independence and impartiality establish credibility and eliminate conflicts of interest. Oversight bodies must be free to publicly communicate their decisions.

3.c Auditability

AI tools, and the decisions they inform, must be auditable. A tool should keep enough record of its inputs, outputs, and operation to reconstruct how a result was reached and confirm it was used within authority. These records are what make oversight, review, and redress possible.

3.d Responsible Management

Police services must manage each AI tool responsibly across its whole life, from acquisition to decommissioning. This means clear lines of responsibility, AI training and competencies, and routine reporting on the tool's use, performance, and any errors or incidents.

3.e Public Engagement and Consultation

While transparency lets the public see how AI is used, public engagement gives them a voice in its use. Services should consult affected communities before a tool is acquired to provide meaningful input into whether the tool is adopted and how it is used., Where it touches First Nations, Inuit, and Métis peoples, it should follow the Indigenous-led approach under Rights and Self-determination. Public engagement is also a safeguard, surfacing harms a service may not foresee.

4. Rights and self-determination

These principles require that AI use respect fundamental rights and the self-determination of the communities it touches. They cover privacy protected by design rather than added after deployment, and full respect for Indigenous rights, data sovereignty, and community-led approaches to public safety.

4.a Privacy by Design

Privacy is fundamental to human autonomy, identity, and dignity. AI tools must be designed to protect privacy and sensitive information by default, across training data, databases, inputs, and use. This protection extends beyond information that individuals disclose to the inferences that AI tools draw about them and their communities. Privacy and public safety should be balanced rather than traded away, and privacy protections should be built in at the planning stage rather than added after deployment.

4.b Indigenous Reconciliation and Self-determination

When engaging with First Nations, Inuit, and Métis communities, police services must support self-determination, prioritize trust-building, and commit to meaningful and sustained systemic change. The use and governance of artificial intelligence must respect Indigenous rights, perspectives, data sovereignty, and community-led approaches to public safety. While the principles of Ownership, Control, Access, and Possession (OCAP) provide important guidance, police services must recognize the diversity of Indigenous communities and remain open to distinct voices, priorities, and governance approaches. Meaningful engagement requires ongoing collaboration, transparency, cultural humility, and respect for Indigenous-led public safety initiatives.

5. Control, security and reliability

These principles require that AI remain under human control and fit for a high-stakes setting. They cover meaningful human control over the tasks a tool performs, the security of the system and of Canadian data under Canadian law, and accuracy, reliability, and robustness confirmed through independent testing.

5.a Meaningful human control

The ethical values of human autonomy and moral agency require meaningful human control of AI tools. Autonomy should be granted to AI tools only to the extent that the delegated tasks, conditions for effective oversight, and interpretability of system behavior have been explicitly specified.

Meaningful human control refers to a competent human in the loop who has training required to monitor, evaluate, and audit an AI system to ensure that it is achieving its intended goal and who has authority to stop the system if necessary. Meaningful human control also refers to supervisory responsibility to oversee AI systems, as well as a human command authority who ensure AI systems are consistent with these guidelines and is accountable for the use of AI systems in the police service.

5.b Security, Safety, and Digital Sovereignty

AI tools used in policing must be secure against unauthorized access, misuse, and disclosure, and safe in both ordinary operation and foreseeable failure. When using vendors outside Canada, police services must keep three distinct concerns separate: the operational security of the system, the residency and jurisdictional control of Canadian data, and control over the inferences drawn about people in Canada. Sensitive policing data should remain governed by Canadian law and protected from improper foreign interference.

5.c Accuracy, Reliability, Validity, and Robustness

AI tools must be accurate in their outputs, reliable across time and conditions, valid for what they are intended to measure, and robust under real world conditions. These are prerequisites for use in a high stake's domain. AI tools should be confirmed through independent testing before deployment and monitored continuously thereafter. Where outputs may become evidence, tools should meet the recognized requirements for admitting novel scientific evidence: testing, peer review, a known rate of error or established standards, and general acceptance.

6. Applying principles in conflict

These principles are not tick boxes. In practice they will sometimes conflict. Transparency can sit in tension with the confidentiality of an active investigation. Public safety can press against privacy. The convenience of automation can erode meaningful human control. A set of principles silent on how such tensions are resolved becomes either an obstacle quietly set aside, or a justification for a decision already made. Neither serves the public.

The framework therefore treats the principles as two kinds. A small number are floors that cannot be traded away under any claim of efficiency or public safety – lawful authority and Charter compliance, human dignity and freedom from discrimination. The rest are weighed against one another through structured judgment rather than open discretion. That judgment asks three questions: is the use necessary for a legitimate policing purpose, is it the least intrusive means available, and are its benefits proportionate to its costs to rights and freedoms. Where real uncertainty remains, given the imbalance of power between the state and the individual, the more protective and precautionary option should prevail.

How a trade-off is reached matters as much as the result. The C-AIPAS tool incorporates human rights and privacy impact assessments, recorded with reasons, disclosed so far as operational sensitivity allows, and left open to challenge and redress. Private vendors must disclose algorithmic impact assessments.

Public engagement should inform every difficult trade-off, rather than providing feedback after a decision. When a decision may have significant or contested effects on a community, its legitimacy depends in part on whether those most affected had a meaningful voice beforehand. Engagement can also reveal harms and concerns that impact assessments and oversight bodies may miss. The deploying service should not make these judgments alone. An independent body must provide oversight, supported by the auditable records these principles require.

Finally, arbitration is continuous. A trade-off acceptable when a tool is adopted may not be acceptable if the tool, its data, or its context changes. Responsible use means returning to these judgments across the whole life of the system from procurement to decommissioning.

Acknowledgements

The Co-leaders of the CACP AI initiative, Dr. Stephen Maguire Carleton University, CS Larry Montgomery RCMP, and Maria McDonald, Co-Chair of the CACP CTNS National Working Group Supporting Victims of Terrorism and Mass Violence gratefully acknowledge current and former members of the CACP Ethics Sub-Committee on AI Ethical Principles for their commitment and generosity sharing their time to develop a Canadian version of AI principles.

Dr. Jean-Christophe Belisle-Pipon, Greg Stanisci, Alpha Chan, Jordan Whitesell, Dr. Jordan Schoenherr, Brendan Dodd, Dr. Maxime Bérubé, Dave Cobey, Dan Despatie, Tracey Bednarczyk, Amy Moore, Dr. Keira Stockdale, Cameron Hopgood

References

Abril, D. (2022, March 9). *Drones, robots, license plate readers: Police grapple with community concerns as they turn to tech for their jobs*. *The Washington Post*. https://www.washingtonpost.com/technology/2022/03/09/police-technologies-future-of-work-drones-ai-robots/

Andrew, J., & Baker, M. (2019). The General Data Protection Regulation in the age of surveillance capitalism. *Journal of Business Ethics, 168*(3), 565–578. https://doi.org/10.1007/s10551-019-04239-z

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review, 82*(5), 977–1008. https://doi.org/10.1177/0003122417725865

Cabinet Office. (n.d.). *Data ethics framework*. GOV.UK. https://www.gov.uk/government/publications/data-ethics-framework

European Commission for the Efficiency of Justice. (2018). *European ethical charter on the use of artificial intelligence in judicial systems and their environment*. Council of Europe. https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

Hill, K. (2022, May 26). *A face search engine anyone can use is alarmingly accurate*. *The New York Times*. https://www.nytimes.com/2022/05/26/technology/pimeyes-facial-recognition-search.html

John-Mathews, J.-M., Cardon, D., & Balagué, C. (2022). From reality to world: A critical perspective on AI fairness. *Journal of Business Ethics*. Advance online publication. https://doi.org/10.1007/s10551-022-05055-8

Lauer, D. (2020). You cannot have AI ethics without ethics. *AI and Ethics, 1*(1), 61–62. https://doi.org/10.1007/s43681-020-00013-4

Université de Montréal. (n.d.). *Montreal declaration for a responsible development of artificial intelligence*. Retrieved August 1, 2022, from https://recherche.umontreal.ca/english/strategic-initiatives/montreal-declaration-for-a-responsible-ai/

Murder Accountability Project. (n.d.). *Who we are*. Retrieved August 2, 2022, from https://www.murderdata.org/p/who-we-are.html

Prox, R. (2020). Lessons learned on implementing big data machine learning. *Police Chief Magazine*, 48–50.

Russell, C., Kusner, M. J., Loftus, J., & Silva, R. (2017). *When worlds collide: Integrating different counterfactual assumptions in fairness*. In *Advances in Neural Information Processing Systems 30 (NeurIPS 2017)*. https://papers.nips.cc/paper/6995-when-worlds-collide-integrating-different-counterfactual-assumptions-in-fairness

Treasury Board of Canada Secretariat. (2019, June 5). *Directive on service and digital*. Government of Canada. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601

Shah, H. (2018). Algorithmic accountability. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376*(2128), Article 20170362. https://doi.org/10.1098/rsta.2017.0362

Sullivan, Y. W., & Fosso Wamba, S. (2022). Moral judgments in the age of artificial intelligence. *Journal of Business Ethics*. Advance online publication. https://doi.org/10.1007/s10551-022-05053-w

The Ditchley Foundation. (n.d.). *The future of policing in the digital age*. Retrieved August 2, 2022, from https://www.ditchley.com/programme/past-events/2010-2019/2018/future-policing-digital-age