Trial or adoption of new policing technology

Table of Contents

Policy statement and principles

What

All proposals to trial or adopt either a new technology-based policing capability, or a new use of an existing technology, must first receive approval under this policy. The Policy purpose and scope statement below contains further detail as to the policy's intended scope and should be consulted in every case.

Trial or adoption of a technology without the necessary approvals will be considered unauthorised.

Why

Our system of policing by consent is based on public trust and confidence in the way New Zealand Police delivers its services. Loss of public trust and confidence could undermine the effectiveness of our efforts to keep the community safe, and erode the trust placed in us by Government and other justice and social institutions.

Trust and confidence can be threatened if Police trial or adopt policing technologies or capabilities that may be viewed as unjustifiably intrusive, or incompatible with the wider community's perceptions of what it is fair and justified for Police to do.

Community concerns are often highest when technology is perceived to enable surveillance, to use facial images or other biometric or personal data without consent, or to use artificial intelligence or algorithms to make decisions which affect them. However, Police also has an obligation to the public to ensure we do not ignore opportunities to use technology appropriately to deliver better policing services and keep the community safe. Being clearer about the basis on which New Zealand Police engages with new technologies can help dispel any unfounded concerns.

Ensuring decisions to trial or adopt new technology are made transparently, and in a principled way, means we will be acting in a way that is consistent with Our Values and Our Business; and will enhance public trust and confidence that the policing technologies we use strike the right balance between enabling better policing, and respecting and protecting individual rights and freedoms.

How

There are several ways that you may discover a new technology capability that could be helpful to deliver Our Business. For example, this may be through the work you do day to day, or as part of a programme or project. This could be as a response to improve the way we deliver our service with new technology available; identifying a gap or opportunity in our technology capabilities; or a response to a legislative change.

From time to time, external suppliers, or colleagues from other agencies (including from overseas), may extend an offer to New Zealand Police staff to test or trial a new policing technology, or new functionality within an existing technology. Such offers will likely be well-intentioned, and consistent with the goal of sharing knowledge and being open to new and promising approaches.

It is important any ideas or offers are appropriately scrutinised, with the possible policing value balanced against the possible real, or perceived, risks to other values such as privacy and fairness.

There is high public interest in ensuring this balance is struck appropriately in every case, and for that reason it is important there is senior (Executive governance-level) oversight in every case.

Important: If you are approached with an offer to trial a new or enhanced policing technology, or you propose to trial or adopt a new technology you have identified could be beneficial, seek advice from your manager or supervisor in the first instance. If it is decided that the opportunity is worthy of pursuing, this policy is likely to apply and the process it describes should be followed prior to beginning any trial or adoption.

Approval is required before any proposed trials or adoption be undertaken

The Police Executive agreed to strengthen the governance and oversight around technology-enabled capabilities in July 2020, with a particular emphasis on any technologies which enable a core policing function. There was also seen to be a chance to better align with the Government Chief Data Steward's and Privacy Commissioner's Principles for the safe and effective use of data and analytics, and Statistics New Zealand's Algorithm Charter for Aotearoa New Zealand.

Before any trial or adoption of new technology commences, or extra functionality within an existing technology is switched on, formal approval must be sought from Police's Security and Privacy Reference Group (SPRG) and endorsed by the Organisational Culture Governance Group (OCGG). Such submissions are expected to have taken into account any relevant ethical and human rights considerations, including public expectations and legal obligations surrounding the right to privacy.

Important: Any trial or adoption of new technology, or added functionality in an existing technology, that has not been approved and endorsed by the SPRG and OCGG will be considered unauthorised.

Policy purpose and scope

Purpose

The purposes of this policy are to:

- ensure decisions to trial or adopt new and evolving policing technologies and technology-enabled capabilities are made ethically and proportionately with individual and community interests
- ensure Police's approach aligns with wider New Zealand Government ethical standards and expectations, including the Government Chief Data Steward's and Privacy Commissioner's Principles for the safe and effective use of data and analytics, and Statistics New Zealand's Algorithm Charter for Aotearoa New Zealand
- ensure decisions reflect Police's obligations to Te Tiriti o Waitangi including by seeking and taking account of a te ao Māori perspective
- enhance public trust and confidence by ensuring decisions and the reasons for them are transparent, and decision-makers are accountable
- enable Police to innovate safely, so that opportunities offered by technology to deliver safer communities and better policing outcomes for New Zealanders are not lost.

Scope

The policy applies to any proposed trial or adoption of new technology. It extends to situations where extra functionality is being added or turned on to an existing technology.

The policy may apply to any type of technology. The scope includes novel technologies such as artificial intelligence (AI), including generative AI tools, drones, machine learning or algorithm-based software, and 'new tech' capabilities, such as use of chat bots or other digitally-enabled management tools, and 3D photogrammetry. It also includes more established technologies which allow for images to be captured (such as use of Closed Circuit Television Cameras [CCTV]) and/or matched (such as Automatic Number Plate Recognition [ANPR]).

The policy applies:

- where new or enhanced policing capability is proposed, whether or not the technology itself is new ('new capability'); **OR**
- where existing technology is proposed to be used for a new or evolved policing purpose ('new use'); **AND**
- it is proposed by Police either to trial or adopt the new capability or new use (whether or not a trial has previously been approved under this policy); **OR**
- the new capability or new use has been, or will be, passively acquired by Police (for example, because of vendor-initiated product enhancement).

The policy **does not** apply where:

- existing technology (software or hardware) is subject to end-of-lifecycle replacement, iterative version upgrades, security patching or other minor enhancements (such as new user interface), if the replacement or upgrade does not add significant new policing capability or enable its use for a new policing purpose; **OR**
- the proposed new capability, or new use, is not a core policing function, because:
  - it will not affect Police interactions with the public in any way (either directly or indirectly); **AND**
  - it will not gather new, additional or improved data from or about members of the public including offenders or victims.

As transparency and accountability are key objectives of this policy, where there is any room for doubt, the policy should be assumed to apply.

Refer to the Technology Assurance Framework for more details on scope, including a policy assessment tree diagram. If in doubt, contact the Technology Assurance Team for advice.

Scope of approvals

Any governance approvals gained under this policy are limited by the relevant governance group's mandate: that is, to assess whether a technology proposal is justified and compatible with privacy, security, legal, and ethical principles. Such approval does not replace or remove the need for a business owner to comply with any other applicable policies including obtaining appropriate financial authorisations.

Process for obtaining approvals

All proposals to trial or adopt a new technology-based policing capability, or new use of an existing technology, should be assessed to determine whether they fall within the intended scope of this policy.

All proposals which are within the intended scope must follow the five-step process described below to receive the appropriate governance approvals, prior to proceeding to trial or adoption.

Any proposal which is assessed to be outside the scope of this policy must still be notified to the Chief Advisor: Technology Assurance by email, so that a complete central record of policing technologies can be maintained.

Trial or adoption of a technology without the necessary governance approvals will be considered unauthorised.

Five step approval process

Step	Who	What
1. Does this policy apply?	Business owner (proposer) in consultation with Technology Assurance Team	Consider whether the policy applies. Consult the initial assessment decision tree diagram and complete the Initial Assessment Form to assist in making this judgment. If the policy does not apply, advise the Technology Assurance Team in writing of the existence of the technology proposed and the business owner's determination that the policy does not apply. This is required to ensure complete records are maintained of the organisation's use of technology tools. No further steps are required.
2. Develop Proposal	Business owner	Develop a brief Technology Proposal document. The document template contains guidance to assist in completing this step. Proposal document is sent to the Technology Assurance Team.
3: Contact the Technology Assurance Team	Business Owner	Provide Technology Proposal to the Technology Assurance Team. The Technology Assurance Team will review the proposal and confirm the proposal is within scope of the policy, is sufficiently well-developed to advance, if the proposed technology relies substantively on an algorithm and provide advice whether the NZ Police Guidelines for algorithm life-cycle management is required to be adhered to, and/or other expert input (such as a te ao Māori perspective) are required.
4. Consider the proposal and develop a Policy Risk Assessment (and Privacy Impact Assessment, Information Security Risk Assessment if required)	Technology Assurance Team and New Technology Working Group	Consider the proposal at a New Technology Working Group meeting, with input from the Business Owner and complete required documentation. The Technology Assurance Team produce a Policy Risk Assessment (PRA) conducted against the Principles. If it is necessary to commission any further specialist advice to support the PRA (for example, to consider a te ao Māori perspective) this may be done at this stage. The Governance Group cover paper make clear recommendation on the proposal and may also recommend that the proposal be referred to the Expert Panel on Technology Assurance for independent advice to inform further consideration by the SPRG (with approval deferred), or as supplementary advice to inform OCGG's consideration of endorsement. The cover paper should provide specific advice on the two special considerations (te ao Māori perspective; and whether algorithm guideline adherence should be mandated) and may recommend conditions be attached to governance approvals as appropriate. The paper should include as attachments: - The Policy Risk Assessment - Privacy Impact Assessment / Information Security Risk Assessment (if conducted) - Any specialist or Expert Panel advice received on the proposal or other relevant supporting information as required - The Algorithm Questionnaire (as required) - Internal - External

4a. Contact other experts as required	Chief Privacy Officer (CPO) / Chief Information Security Officer (CISO) / other subject-matter expert (as appropriate)	Produce Privacy Impact Assessment / Information Security Risk Assessment /other expert assessment (as appropriate) in consultation with business owner. Adjustments to the proposal may be made to address issues, for example by refining the use-case or introducing new controls to the proposal.
5. Two-step Governance approval Step 1: Approval decision by Security and Privacy Reference Group (SPRG)	SPRG	Receive advice and recommendations from the Technology Assurance Team and decide whether or not to approve the proposal. This decision will be based on the proposal meeting security and privacy requirements. SPRG may refer the proposal to the Expert Panel on Technology Assurance or any other key stakeholders for independent advice. **Note:** Should a request be required in an emergency situation; it can be raised to the Executive Lead for Organisational Culture Governance Group via the Chief Advisor: Technology Assurance.
5a. Two-step Governance approval: Step 2: Endorsement decision by Organisational Culture Governance Group (OCGG)	Delegated Executive Lead for OCGG	Review and decide whether or not to endorse the SPRG decision. The Executive Lead should be informed by the same material presented to the SPRG and any further relevant material produced since (for example, a description of new controls or proposal revisions made in response to SPRG comment or approval conditions). The Executive Lead may also refer the proposal to the Expert Panel, if it has not already been previously referred. The Executive Lead makes decision on whether proposals are referred to the whole OCGG for consideration of endorsement. This decision should be minuted, along with any conditions that the Executive Lead may attach to the approval (for example, narrowing the approved use-case or requiring additional controls to be implemented). The Executive Lead (or OCGG) will decide whether NZP will proceed with trialling or adopting the technology. If endorsed by the Executive Lead (or OCGG), the proposal may proceed within the approved parameters subject to any other necessary approvals having been gained (such as financial authorisation) under any other applicable policies. **Note:** It is anticipated that, in most cases, there will be a four-week period between the receipt of the proposal and an approval decision.

Approvals to trial technology

If a proposal to trial a technology is approved under this policy, the trial is authorised to proceed subject to appropriate financial approvals and any applicable requirements of other policies being met. Approval under this policy does not grant authority to proceed to trial without financial and other requirements being met.

The trial must follow the parameters and evaluation plan approved by Executive Lead and any conditions imposed as part of the approval.

The Chief Advisor: Technology Assurance maintains records of technologies being trialled. The Chief Advisor must be kept informed of trial progress, conclusion of the trial, and evaluated outcomes.

Any proposal to adopt a technology after a trial must seek further governance approval under this policy.

The process of seeking further approval will require updating of materials that were produced to support the trial proposal: in particular, to ensure that decisions on final adoption are cognisant of evaluated trial outcomes and any adjusted use parameters or controls.

Approvals to adopt a technology

If a proposal to adopt (or operationally deploy) a technology is approved under this policy, that approval is subject to appropriate financial approvals and any applicable requirements of other policies being met. These may include preparation of a business case and following appropriate procurement process. Approval under this policy provides the authority to proceed to the next steps.

Deployment of a technology must follow the approved use parameters and controls, and any other conditions imposed as part of the governance approvals.

The Chief Advisor: Technology Assurance maintains records of technologies in use by Police. The Chief Advisor must be kept informed of any changes in use, withdrawal of the technology, or other developments.

Any proposal to alter the way in which technology is used, after it has been adopted, must seek further governance approval under this policy.

Guidance for developing a technology proposal

Completing the Technology Proposal template will ensure that sufficient information is available to begin the process of seeking approval for a new technology use.

The process mandated by this policy is based on assessing technology proposals for compatibility with ten principles. This ensures Police can demonstrate in a transparent and defensible way that any new policing capability trialled or adopted has been robustly considered and fairly balances competing interests.

It will be helpful for business owners considering the possibilities of new technology to be cognisant of the ten principles from the outset. This will help ensure that proposals are scoped and developed in a way that is less likely to raise issues of concern and maximise the likelihood of approval.

Principles

The ten Principles which guide decisions on trial or adoption of new policing technologies are described in detail in theTechnology Assurance Framework. In summary, they are:

1. **Necessity -** there is a demonstrable need for Police to acquire the capability
2. **Effectiveness -** there is good reason to believe the technology will meet the need
3. **Lawfulness -** the proposed use is lawful
4. **Partnership -** a te ao Māori perspective, as well as the perspectives of Pacific, and other communities have been considered and affected communities consulted
5. **Fairness -** possible data or use biases have been considered and risks mitigated
6. **Privacy -** impacts have been considered and risks mitigated
7. **Security -** data and information security risks have been considered and risks mitigated
8. **Proportionality -** individual, group and wider community impacts have been considered and any negative impacts are proportionate to the necessity and benefits
9. **Oversight and accountability -** policy, audit and reporting controls will assure that the technology is only used as intended
10. **Transparency -** appropriate information about the technology, its use, and how to challenge adverse outcomes will be publicly available

The need for alignment with the Principles should be incorporated into early design decisions or product selection criteria. In much the same way as 'privacy by design' should apply, designing for alignment with the Principles could be considered 'ethical by design'.

The Principles should be considered when determining the parameters of the trial proposal, and its proposed evaluation. For example, where judgments as to alignment with certain principles may be unclear, these may be issues that need to be explicitly investigated through the trial and evaluation.

The advice provided to the Governance Groups to inform their decision (process Step 4) should include a structured assessment of the proposal against each of the statements contained in the Principles. This is the point at which formal alignment with the Principles is comprehensively assessed. The Policy Risk Assessment is the advice of the Technology Assurance Team. It represents the analysis and judgment of the Group and will usually be based on the information presented in the Technology Proposal, PIA/ISRA (if commissioned), and any other relevant information. This template contains guidance to assist in completing the Policy Risk Assessment.

Refer to the Technology Assurance Framework for more details and resources on the principles, assessments, and groups that support this process.

Further advice and support

For further advice and support regarding this policy, please contact the Technology Assurance Group, Police National Headquarters.

The following Police Instructions contain additional information and guidance relevant to this policy:

- SELF CHECK
- Police governance and leadership
- ICT projects and service delivery
- Information security roles and responsibilities
- Information security

Printed on : 23/07/2024

Printed from : https://tenone.police.govt.nz/pi/police-manual/s-u/trial-or-adoption-new-policing-technology