NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

# Technology Assurance Framework

## *Contents*

Document history

| Version | Date | Description |
|---|---|---|
| 1.0 | 31/03/2021 | Initial version |
| 2.0 | 12/04/2021 | Internal review feedback incorporated |
| 3.0 | 30/11/2021 | External review feedback incorporated from Expert Panel and external expert advisors |
| 3.1 | 12/01/2024 | Updating governance processes and entity names, adding further considerations and direct references to the principles |
| **4.0** | 27/09/2024 | Updating process descriptions in line with Review of New Technology Proposal findings and recommendations |

Document Approval:

V2.0 Approved by Organisational Capability Governance Group on 13/07/2021
V3.1 Approved by Chief Assurance Officer on 25/03/2024
V4.0 Approved by Chief Assurance Officer on 29/09/2024

## 1. *Overview*

The Technology Assurance Framework has been developed to assist decision-making on new technology. The Framework aligns with our **SELF CHECK** tool to help make the best decisions possible:

- Would it withstand **S**crutiny? (Community, Police service, Media and Online)
- Is it in line with our **E**thics? (Our Code, Our Values, High performing culture)
- Is the decision **L**awful? (Laws, Regulation, Policies and guidelines)
- Is the decision **F**air to all? (Community, Colleagues and whānau, People's individual circumstances)

## 2. *Trial or Adopt New Policing Technology Policy purpose and scope*

### Why do we have this policy?

Our system of policing by consent is based on trust and confidence in the way New Zealand Police delivers its services, and the social license granted by the community to police in the way that we do. Concerns about overly wide access to certain technologies, or a lack of clarity around how certain policing decisions are made, can undermine public trust and confidence and Police's social license. Police also needs to ensure the use of new technology is lawful.

Being clearer about the basis on which New Zealand Police engages with new technologies can help dispel any unfounded concerns, and reinforce Police's commitment to carefully weigh privacy, legislative, security and ethical considerations before making decisions about new technology. The policy can also support an ongoing conversation about the role of technology-enabled capabilities in policing, set in the particular context of Aotearoa/New Zealand.

**Purpose and scope**

***Trial or Adoption of New Policing Technology Policy*** *purposes*

The purposes of the policy on trial or adoption of new policing technologies 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.

All business units and groups under the Police Budget allocation are subject to the policy, including the Next Generation Critical Comms (NGCC) programme and the Firearms Safety Authority / Te Tari Pūreke.

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]). It includes both "online" tools accessed through the internet and a web browser, as well as "standalone" tools that are physically managed by Police.

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, as a result of vendor-initiated product enhancement).

The policy <u>does not apply</u> 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), <u>if</u> 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, would not enable 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.

**If in doubt, contact the Technology Assurance Team for advice.**

*Examples of core policing functions:*

Examples of technology capabilities or uses which would be considered to affect Police interactions with the public, and are therefore **in scope** of the policy as core policing functions, would include technologies that:

- might influence or change public-facing deployment or response decisions
- help to detect offending
- assist in investigations
- generate leads or influence targeting or prioritising of investigations

- identify suspects or discover potential evidence
- use of equipment, like Remotely Piloted Aircraft Systems (RPAS), to survey scenes and provide situational awareness
- analytics and reporting, for example to inform operational resource allocation

Examples that would most likely not be considered as enabling core policing functions and therefore **not within scope** include technologies that:

- work only with Police's own internal corporate organisational information (such as HR systems to support personnel)
- assist decision-making on resource allocation only at an internal-facing, non-operational level
- affect only internal, non-operational, and non-investigative workflows.

*Further guidance on scope*

An **initial policy assessment decision tree diagram** is contained in the Technology Assurance Framework to assist in determining whether or not the policy applies in a specific case. Particular attention should be focussed on technologies that are significantly based on:

- artificial intelligence or machine learning
- algorithm-based risk assessment or decision support or predictive modelling
- gathering or analysing data which relates to members of the public, including individual offenders
- biometrics: the fully or partially automated recognition of individuals based on biological or behavioural characteristics
- the possibility of public place or online surveillance perceived or otherwise (irrespective of whether the provisions of the Search and Surveillance Act are considered to apply) including Open Source INTelligence (OSINT).

These technologies are likely to be inherently higher-risk and so application of the policy to them should be considered the default position.

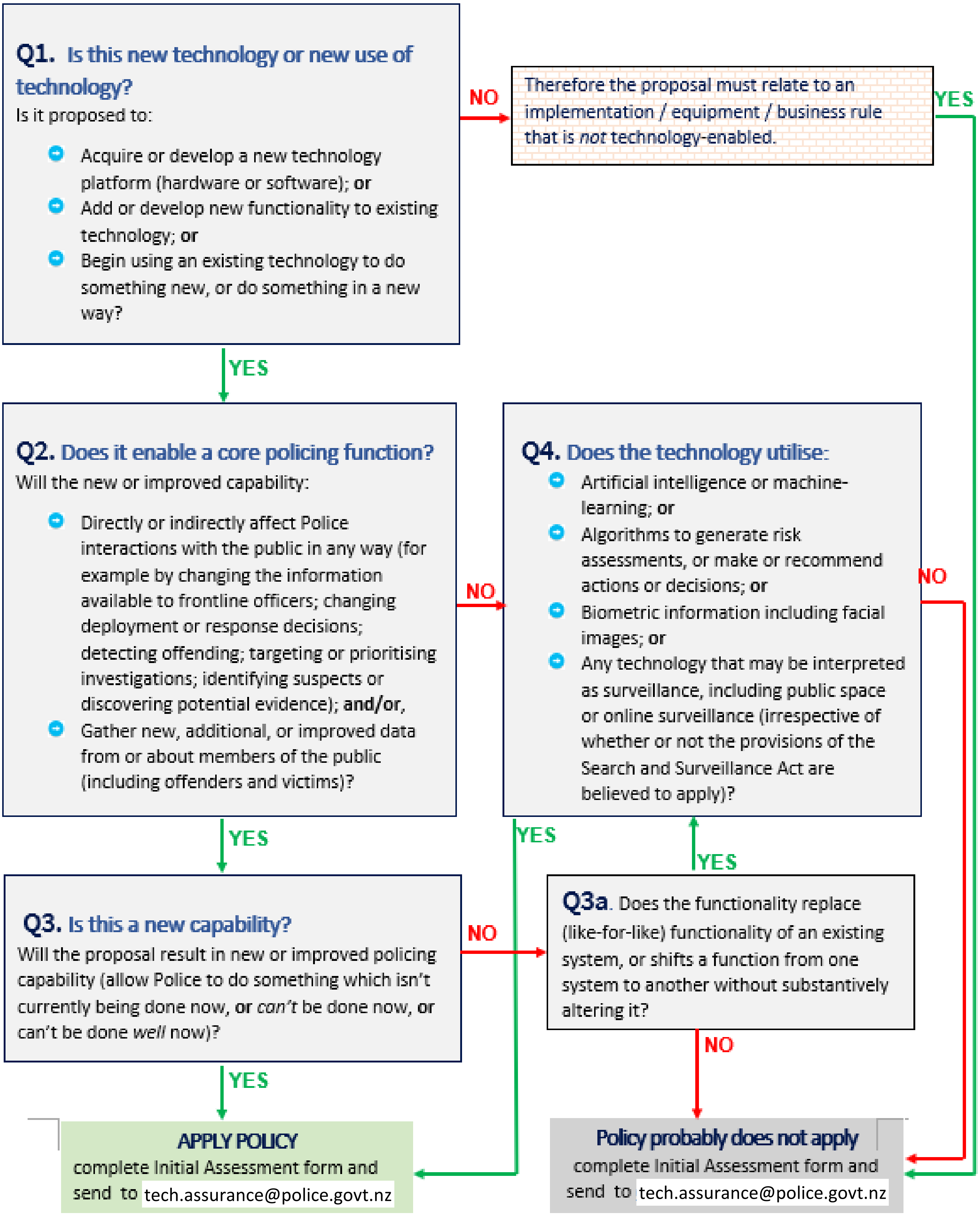
The lawfulness of a proposed new capability or new use is not a factor which determines whether or not this policy applies.

As transparency and accountability are key objectives of this policy, where there is any room for doubt, the policy should be assumed to apply. Where the policy does not apply, business owners may choose to work with the Technology Assurance team to identify potential risks and develop appropriate mitigation and controls.

*Scope of approvals*

Any governance approval 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.

## Initial Policy Assessment Decision Tree Diagram



**Q1. Is this new technology or new use of technology?**
Is it proposed to:

- Acquire or develop a new technology platform (hardware or software); **or**
- Add or develop new functionality to existing technology; **or**
- Begin using an existing technology to do something new, or do something in a new way?

Therefore the proposal must relate to an implementation / equipment / business rule that is *not* technology-enabled.

**Q2. Does it enable a core policing function?**
Will the new or improved capability:

- Directly or indirectly affect Police interactions with the public in any way (for example by changing the information available to frontline officers; changing deployment or response decisions; detecting offending; targeting or prioritising investigations; identifying suspects or discovering potential evidence); **and/or,**
- Gather new, additional, or improved data from or about members of the public (including offenders and victims)?

**Q3. Is this a new capability?**
Will the proposal result in new or improved policing capability (allow Police to do something which isn't currently being done now, **or** *can't* be done now, **or** can't be done *well* now)?

**Q3a.** Does the functionality replace (like-for-like) functionality of an existing system, or shifts a function from one system to another without substantively altering it?

**Q4. Does the technology utilise:**

- Artificial intelligence or machine-learning; **or**
- Algorithms to generate risk assessments, or make or recommend actions or decisions; **or**
- Biometric information including facial images; **or**
- Any technology that may be interpreted as surveillance, including public space or online surveillance (irrespective of whether or not the provisions of the Search and Surveillance Act are believed to apply)?

**APPLY POLICY**
complete Initial Assessment form and send to tech.assurance@police.govt.nz

**Policy probably does not apply**
complete Initial Assessment form and send to tech.assurance@police.govt.nz

## 3. *Principles*

### Introduction to the Principles

Ten Principles underpin the decision-making framework. These are intended to be technology agnostic and not linked to any specific technology. That is, they should be able to be usefully applied (as relevant) both to novel or advanced technologies such as algorithms and AI, and simpler technologies such as CCTV or body-worn cameras.

Similarly, they should be applicable to new technology capabilities or use-cases, whether they utilise new or existing technology platforms; and to technology proposals either to trial or adopt the technology.

The Principles are illustrated by a series of statements, which are intended to aid understanding of what the Principles mean and help to structure assessment of whether a proposal aligns with the Principles or not. All technology proposals should align with each of the statements, to the extent they apply in the particular use-case.

Alignment should be demonstrated before a technology proposal is approved via the two-step governance approval process for trial or adoption. Alignment with one or more principles may be provisionally assessed at the point of a proposal to trial if it is intended that the trial and evaluation will further investigate the issue.

### Focus on the application of the technology

Principles-based assessment requires a central focus on the proposed use-case – not just on the technology itself. That is because a technology itself is seldom likely to be either inherently harmful or beneficial: what matters most, in terms of both ethical decision making and public acceptability, is how it is used, the impacts, and whether the benefits of that particular use outweigh or are proportionate to the harms.

### Focus on the people affected by the technology

Identify the stakeholders (people, communities, and groups) who have an interest in the use of this technology, especially if the use of the technology is likely to affect them. Considering how they may be affected in direct and indirect ways can help identify potential harms that need to be balanced against the benefits.

### Consider interactions with other tools and processes

Technologies increasingly work alongside or with other systems, which can produce outcomes not originally envisaged if considered alone. For example, a proposal to use Facial Recognition Technology may need to evaluate what might happen if that capability is deployed via a drone, which could carry different implications to a system deployed on the ground. Identifying potential for scope creep can help with establishing the boundaries for appropriate use of the technology.

**Principle 1: Necessity**

- There is a demonstrable, legitimate need for Police to acquire the capability the technology is intended to deliver and a clear problem statement
- Use of the technology supports and achieves the strategic direction of Police, including Our Business and the Executive Strategic Performance Template (SPT)
- The technology will deliver an identifiable public or policing benefit that would not otherwise accrue, assist Police to meet relevant legislation, or lessen a significant risk that would otherwise be present. The benefits of these technologies may be quantitative in nature, such as increased crime prevention and efficiency of police operations, or qualitative, such as an increase in public trust and an improved perception of Police

**Principle 2: Effectiveness**

- The technology design is well understood and explainable to users and impacted people
- The policing objectives of the technology's proposed use are well defined and explainable
- There is an evidence base or other good reason to believe the technology will be effective in delivering these objectives
- Output of the proposed technology will be fit-for-purpose and of the quality necessary to support the intended use (such as intelligence, investigative, evidential, or forensic use)
- The proposed technology has been used or tested in a New Zealand context, to ensure compatibility with New Zealand Police outcomes

**Principle 3: Lawfulness**

- The technology's proposed use is reasonable and lawful
- The technology is applied only within the agreed scope of the proposal
- Potential legislative changes are considered for short-term impact on the proposal

**Principle 4: Partnership**

- Te Tiriti o Waitangi has been considered in the design and proposed use of the technology
- A te ao Māori perspective has been considered in assessing the possible or percieved impacts of the technology or its use on Māori
- If the technology includes any form of data collection and use, relevant mechanisms are in place to ensure data is treated as taonga and Māori sovereignty is maintained
- Māori, Pacific and/or other communities have been involved in co-design or consulted and any concerns responded to
- Business owners have liaised with MPES to evaluate the potential effects and risk mitigation strategies for Māori, Pacific and/or other communities

**Principle 5: Fairness**

- Any possible biases or perceived unfairness arising from the technology design or its proposed use are clearly identified and able to be mitigated[1]
- The proposed use of the technology is appropriate

**Principle 6: Privacy**

- The technology incorporates privacy by design in data sourcing, use, retention and storage
- Privacy impacts in an operational environment have been assessed and identified privacy risks will be mitigated

**Principle 7: Security**

- Appropriate data governance will ensure data is handled and stored securely, and data quality and integrity are assured
- Information security and operational security risks have been assessed, including data intrusion risks, and identified risks will be mitigated

**Principle 8: Proportionality**

- Impacts on the human rights and interests of individuals, particular groups or communities, and the collective public interest of the community as a whole have been considered
- A te ao Māori perspective has been considered
- The following impacts have been considered:
    - privacy, safety, security and other impacts on affected **individuals** (e.g. suspects, offenders, victims, staff, members of the public)
    - the collective human rights and interests of **particular groups or communities** affected (e.g. communities of ethnicity, age, gender or diversity, or particular geographical communities)
    - human rights and the collective public interest of the **community as a whole**
- Any negative impacts are proportionate to the necessity and benefits of the proposal
- No other identified alternative solution or strategy, that is viable having regard to cost and other feasibility considerations, would meet the need and deliver the benefits with less negative impact

**Principle 9: Oversight and accountability**

- The proposed technology has been assessed and/or peer reviewed for technical adequacy
- Risks including privacy, security, te ao Māori, human rights and ethical risks identified have been mitigated and residual risk is within acceptable margins

[1] If the technology is at an early (early procurement, pre-trial) stage, it may not always be possible to identify all possible biases, if a previously unidentified bias arises, further consultation with the Technology Assurance Team may be required.

- Policy, process, audit and reporting controls have been developed to assure that the technology is used only as intended
- Review processes have been developed for trial evaluation and/or to monitor operational performance, to measure whether the technology is delivering the intended outcomes and benefits
- The system in which the technology is deployed, and any substantive decisions made by or based on the technology's output (such as resource deployment, identification of possible suspects, or enforcement decisions) are subject to active human oversight
- Potential for scope creep is identified and defined to avoid unintended use
- Plans or procedures for incidental or unintended findings are considered

**Principle 10: Transparency**

- The technology, the way it is to be used, and the rationale for any decisions made by the technology itself, or by people on the basis of its output, are understood by those assessing and operating it, and are clearly explainable to others
- Mechanisms (whether general or specific to the technology use) exist for individuals or groups adversely affected by the technology to challenge or seek review of decisions
- Information about the technology, its proposed/authorised use(s), justification for these uses, and oversight and accountability mechanisms will be published or otherwise made freely available to the public, to the greatest extent possible (having regard to operational security, commercial and other considerations)
- Assessments, evaluations, reviews, audits and other reports will be published or otherwise made freely available to the public, to the greatest extent possible (having regard to operational security, commercial and other considerations)

## 4. Assessment process

A five-step assessment process to reach a principled decision on a new technology use proposal is described in the shaded box below.

The process presupposes that the business group has already done desktop research/evaluation to develop a proposal that is sufficiently advanced to allow for meaningful assessment against the Principles, and assessment of privacy, security, legal and ethical implications.

The process mandates three documents to be created in every case that falls within scope of the policy:

- A **Technology Proposal** produced by the business group owner
- A **Policy Risk Assessment (PRA)** produced by the Technology Assurance Team
- Governance cover papers, produced by the Technology Assurance Team, which will also include specific advice on te ao Māori, and algorithm-related considerations (where relevant)

Further documents may also be required on a case by case basis, including:

- A Privacy Impact Assessment
- An Information Security Risk Assessment
- Information on algorithms to demonstrate compliance with the **Guidelines for algorithm life-cycle management**
- Other supporting documents or expert reports as required

### Technology Proposal assessment: process overview

| 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. Contact the Technology Assurance team who can evaluate the assessment form and indicate if the policy applies or not, or if the proposed use of technology is sufficiently low-risk. The Technology Assurance team will log the use of the technology to ensure complete records. |
| **2.** Develop Proposal | Business owner (proposer) | Complete the **Technology Proposal** document. The document template contains guidance to assist in completing this step. The Proposal document is sent to the Technology Assurance Team via tech.assurance@police.govt.nz |
| **3.** Work with the Technology Assurance Team | Business Owner | 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 **Guidelines for algorithm development and life-cycle management** is required to be adhered to, and/or if |

| | | |
|---|---|---|
| | | other expert input (such as a te ao Māori perspective) are required. |
| **4.** Consider the proposal and develop a Policy Risk Assessment | 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.<br>The Technology Assurance Team produce a **Policy Risk Assessment (PRA)** evaluated against the Principles.<br>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 paper makes clear recommendations on the proposal and may also recommend that the proposal be referred to the Expert Panel on Emergent Technology for independent advice to inform further consideration by the Security Privacy Reference Group (with approval deferred), or as supplementary advice to inform Executive consideration of endorsement.<br>The 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.<br>The papers submitted to the Governance Groups should include as attachments:<br>• The **Policy Risk Assessment**<br>• Privacy Impact Assessment / Information Security Risk Assessment (if conducted)<br>• Any specialist or Expert Panel advice received on the proposal or other relevant supporting information as required<br>• The **Algorithm Questionnaire** (as required) |
| 4a. Contact other experts as required, and produce assessments if required | Chief Privacy Officer (CPO) / Chief Information Security Officer (CISO) / other subject-matter expert (as appropriate) | Technology Assurance will help the business owner connect with other internal experts. Produce Privacy Impact Assessment / Information Security Risk Assessment / Legal Opinion / other expert assessment (as appropriate) in consultation with the 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 | SPRG | Receive advice and recommendations from the Technology Assurance Team and make a |

|  |  |  |
|---|---|---|
| Governance approval:<br>Step 1 - approval recommendation by Security and Privacy Reference Group (SPRG) |  | recommendation on whether or not to approve the proposal. This recommendation will be based on the proposal meeting security and privacy requirements. SPRG may refer the proposal to the Expert Panel on Emergent Technology or any other key stakeholders for independent advice. |
| 5a. Two step Governance approval:<br>Step 2 - endorsement decision by Executive Member(s) | Executive Leadership Team | For proposals with high organisational risk (as identified by the Chief Advisor: Technology Assurance and affirmed by SPRG), the Executive Leadership Team should review and decide whether or not to endorse the SPRG decision, preferably through an Assurance-themed ELT meeting.<br>Should a request be required more urgently than the ELT schedule will allow, it can be raised to an appropriate Tier 2 Executive member (who is not part of SPRG) for endorsement via the Chief Advisor: Technology Assurance.<br>The Executive Lead member(s) 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).<br>If endorsed by the Executive, 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. |

## *5. New Technology Working Group – Purpose and Membership*

The New Technology Working Group is a semi-formal group, convened by the Chief Advisor: Technology Assurance to support new technology assessment and governance approvals processes. Its advice will be provided to business owners on a consensus/shared accountability basis. Membership may vary but should include representation of/from:

- Chief Privacy Officer
- Chief Information Security Officer
- Māori, Pacific and Ethnic Services
- Legal
- ICTSC
- Evidence-Based Policing
- Assurance Group
- Other policing expertise relevant to particular proposals but arms-length from business owners, such as Operational Capability, Iwi and Communities, High-tech Crime Group, or District representative (as appropriate)

The New Technology Working Group's main purpose is to give initial consideration of a Technology Proposal and provide semi-formal feedback to the business owner. New Technology Working Group is engaged early in the process so that the Group can provide internal Police expert perspectives, who can advise the business owner:

- Whether, in their consensus view, the proposal falls within scope of the policy or not. This provides a second opportunity to triage very low risk proposals out of the process
- Whether the proposal is sufficiently well-developed to proceed, or whether the business owner should flesh out details in particular areas
- Provide advice to inform the policy risk assessment from a security, privacy, legal and ethical perspective and guiding principles
- Whether supporting documents such as a Privacy Impact Assessment, Information Security Risk Assessment, te ao Māori or other expert assessment should be produced
    - The relevant expertise will be present in the Working Group and the necessary work can therefore be initiated immediately
- Whether or not the technology appears substantively to involve the use of an algorithm, and whether the guidelines for algorithm development and life-cycle management for algorithm developers should also be followed
- Any other relevant advice – for example, if a similar proposal has recently been considered and the outcome of that consideration

Advice of the Group should be formally recorded for purposes which could include policy evaluation, research, audit, and accountability. These may be required to be produced later.

## *6. Expert Panel on Emergent Technology (EPET)*

The Panel is an advisory body convened to give independent advice on proposals referred to it by Police, in the form of recommendations and guidance for the consideration of the Commissioner of Police. The Technology Assurance Team, SPRG and the Executive can refer proposals to the Panel at any point of the proposal process, where the panels advice will be helpful to inform decision making.

The panel provides expert scrutiny, review, and advice on new technology which is a key part of providing assurance within Police, and reassurance to the wider public, that privacy, ethical, and human rights implications have been considered before decisions are made to trial or adopt new technology capabilities.

The Panel is also responsible for advising Police of algorithms proposed (to ensure privacy, human rights and ethics interests are appropriately safeguarded, and any unintended consequences are identified), are in line with the **Algorithm Charter for Aotearoa New Zealand**.

The Panel's review work and advice to the Commissioner of Police is expected to consider consistency with Te Tiriti, proactive partnerships with Māori, and implications for Māori, Pacific and Ethnic communities.

The Panel comprises of an independent Chair and up to five other independent members. Panel members will collectively have expertise in privacy, ethics and human rights matters; data and technology; Te Ao Māori and an understanding of Māori data sovereignty issues; and public policy.

## *7. Technology Proposal, Policy Risk Assessment, and Algorithm Guidelines*

### Technology Proposal

The **Technology Proposal** is a summary of the proposed new technology use. A specification for this document is contained in the shaded box below.

As described in the process overview, the Technology Proposal will be used as a basis for assessing whether a Privacy Impact Assessment and/or Information Security Risk Assessment is required to inform the decision-making process. It is also the basis on which a Policy Risk Assessment will be conducted.

**Technology Proposal Document**

A Technology Proposal should include at least the following headings and information.

*Use case*

- What is the technology proposed to be used for? This should be a description of the specific purpose, or kinds of situations in which the technology is intended to be used (such as types of crime being investigated, or operational situations where the technology would be employed). This should include an outline of the proposed ‘end state’ deployment of the technology, as envisaged if a trial is successful.

*Technology description*

- What is the technology and how does it work? This should include an overview of the technical functionality, including a description of data sources where relevant. If the technology mainly relies on an algorithm to analyse data (e.g. to assess risk, make decisions, or produce recommendations for staff action) this should be specifically noted.

*Necessity [ref Principle 1]*

- What do Police need to be able to do (or do significantly better), that they can’t do now? Outline how the proposal supports and achieves the strategic direction of the organisation. Make specific linkage to Our Business and the Executive SPT. What existing policing capability gap is the technology intended to bridge? This should be a brief statement that describes an existing policing challenge or shortfall: for example, in meeting a public interest in, or expectation of, service delivery or harm prevention in a specific area.

*Engagement [ref Principle 4]*

- How have Te Tiriti o Waitangi and a te ao Māori perspective been considered in the design and proposed use of the technology? How have Pacific and other communities been considered?

*Controls [ref Principles 3, 9]*

- How it is proposed to ensure that the technology is not used beyond its intended use case. This could include, for example, policy guidance, legislative or regulatory guidance, approvals processes, reporting and audits.

*Proportionality [ref Principle 8]*

- Consider the policing requirement versus implications on an individual or community. Can the proposed solution be justified against the impact on people's privacy or other rights/expectations of fairness (e.g. use of their data, surveillance of lawful activity, perceived 'targeting'); and in terms of the likely initial and ongoing financial/resourcing costs to Police (to the extent the approximate scale of such costs may be known)? Briefly describe any such impacts and costs and how they are justified, having regard to the above (necessity, use case, controls). Reference to the Principles may help identify possible impacts.

*Trial and evaluation proposal [ref Principles 2, 9]*

- What the parameters are for the proposed trial (for example, how many users/devices, in what locations, and for how long) and how the trial is proposed to be evaluated. This should include a description of how the trial will be determined to be a success.

*Risks [ref Principles 5, 6, 7]*

- What are the key technology or business risks that need to be considered? Is there any existing mitigation in place? Types of risks to consider include Fairness/Bias, Privacy, Security, and others.

*Transparency [ref Principle 10]*

- Are there any restrictions that need to be put in place on how this proposal is shared, or justifications for "less than default" transparency through the lifecycle of the project?

*How will the technology be funded?*

Will this be funded within the Business Owner's allocated funding; or will this require an Investment Proposal through to Business Case? Advise options for the testing/trialling stage, and, should the technology be implemented, consider ongoing costs to maintain the technology. The implications of any proposal on investments, finances, staffing, training, procurement and IT should be transparent. Give as much relevant information as possible.

While financial approvals are not generally part of the Technology Assurance process, Business Owners are asked to consider if there is sufficient resourcing to uphold and maintain assurance controls, provide reporting as required, and to handle irregular demand such as OIA or media requests.

## Policy Risk Assessment

A **Policy Risk Assessment (PRA)** is the structured assessment of the Technology Proposal against the Principles. The PRA should state whether (and, if so, how) the proposal aligns with each of the statements contained in the Principles, including whether the proposal is proportionate and ethical. This analysis will be informed by the Technology Proposal and any further relevant information including any Privacy Impact Assessment / Information Security Risk Assessment produced, and any supplementary specialist advice received (for example, advice from a te ao Māori perspective).

The PRA will form a key part of the advice to the Governance Group and should therefore be presented in full to support any recommendations made.

The PRA template requires an assessment against each and every statement in the Principles (even if the assessment is simply “Not applicable”). It is important to demonstrate for the record that the full spectrum of possible issues has been actively considered.

The PRA template contains guidance in the righthand column. This is not intended to be prescriptive and the assessor should apply their own judgement as to what is relevant or not in order to demonstrate how compliance is achieved, and under what conditions (if any).

In time, as PRA assessors, consumers of the advice, and the wider organisation become more adept at applying the framework, lower risk or less significant proposals might be satisfactorily assessed against a briefer PRA which allows for aggregated commentary against each of the 10 Principles, to highlight only the most salient issues bearing on decision-making.

### General guidance for completing a PRA

- Each cell in the righthand column of the completed PRA should describe, in a few sentences (2-5), **how** the proposal complies with the corresponding statement. In some cases a slightly longer commentary may be necessary. If significantly more lengthy explanation is warranted, consider appendices.
- Commentary should include any conditions/qualifications to the assessed compliance, including any further work that is recommended to align with the principle.
- Commentary should reference source documents (such as the Technology Proposal or Privacy Impact Assessment) wherever possible, to demonstrate the basis on which compliance has been assessed.
- The PRA is an accountability document, and is a key foundation for governance decision-making. As such, if the evidence does not clearly support an assessment of alignment with a given principle, invite the proposer to produce more evidence; and if doubt remains, ensure that doubt is clearly recorded in the PRA.

### Colour coding

*Shade each box to provide a rapid visual aid for checking compliance with the principles. Green means full compliance …*

*… while orange indicates conditional or qualified compliance, or compliance subject to completion of further work.*

*Red would indicate that, at the time of assessment, the proposal could not demonstrate compliance with the relevant principle.*

## Adherence with Guidelines for algorithm development and life-cycle management

While, technically, algorithms are utilised to greater or lesser degree in every computerised technology, they are usually incidental to the policing capability delivered by the technology.

Some technologies, however, rely substantively on algorithms that may even have been programmed specifically to deliver or enable a policing function or capability. For example:

- Algorithms which analyse data to generate risk assessments, prioritise interventions, make decisions, or recommend actions
- Algorithms which search data to identify possible evidence or persons of interest, or scrape/extract/aggregate data of potential interest

In cases where an algorithm is central to the capability of a technology, appropriate design, use and performance of the algorithm are key to assessing the proportionality of the policing capability it enables. As well as assurances within the design and performance of an algorithm, it is important to maintain human oversight to mitigate any risk of inaccuracy within algorithm-informed decision-making.

The business owner is required to make an initial judgment of whether a technology is algorithm-dependent as part of the Technology Proposal, and as part of adherence to the **Guidelines for algorithm development and life-cycle management** and compliance with the **Algorithm Charter of Aotearoa New Zealand**. The Guidelines cover the design, use, and management of the algorithmic technology, such as how data is gathered, tested, inaccuracies, bias, how the data will be used throughout the technology's lifecycle, and how it will be monitored. The Business Owner must complete NZP's **Algorithm Questionnaire** for algorithm lifecycle management to demonstrate compliance with these guidelines and best practice. There are two checklists available:

- A **questionnaire** for use and approvals of **internally** developed algorithms, to be completed by the proposer/business owner
- A **questionnaire** for use and approvals of **third party** algorithms, to be completed by the proposer/business owner **and** the supplier.

This questionnaire will be further considered by the Technology Assurance Team, with advice provided to the Governance Groups accordingly. Based on that advice, governance approvals for technologies that depend on algorithms will be conditional on adherence to the Guidelines. Both the safety of the algorithm **and** alignment with the Principles must be considered.

## *8. Process following approval of technology*

### Proposals to deploy technology after successful trial

Trial and evaluation of a technology proposal are likely to provide additional evidence about possible privacy and other risks, and the effectiveness of control and mitigation strategies. Trial experience might also result in refinements to proposed limitations on the uses of a particular technology.

Therefore, a proposal to adopt for operational use or more widely deploy a technology, following a successful trial, should also be subject to the process described by 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.  In most cases, the mandated documentation will have been created to support the earlier trial proposal. This documentation will simply need to be updated to reflect any changed parameters and evidence gathered through trial and evaluation.

If evaluation has been positive, progression through the new technology governance approvals process a second time should not in most cases delay progress in parallel through other processes associated with full-scale adoption (such as development of a business case and/or investment proposal).

### Post-approval monitoring and oversight

Securing the SPRG approval and Executive endorsement via the five-step process completes the principled decision-making process established by the Framework. However, maintaining public trust and confidence requires that Police can continue to demonstrate trustworthiness in the use of technologies once approved for trial or adoption. The approvals process reflects this through its focus on ensuring appropriate trial evaluation and use controls form part of the Technology Proposal. EPET may also ask for updates on proposals they have previously reviewed.

At an implementation level, ongoing assurance of good stewardship of policing technologies (including assuring compliance with the approved parameters of trial or use) requires maintenance of centralised records. Police has previously committed to establishing and maintaining a centralised ‘stocktake’.

The centralised record should capture all proposals (including those that are assessed as not requiring governance approvals); record the governance decisions on them (whether approval was granted or not); and serve as a platform to enable monitoring of trial progress and evaluation, and support lifecycle management of technologies (including algorithms) once adopted and deployed. Monitoring and lifecycle management are likely to include assuring that trial or use takes place within approved parameters and subject to any conditions imposed, and scheduling of regular reviews of a technology’s performance against its intended purpose. It may also include scheduling of any associated reporting or other assurance loops that formed part of the approved proposal.

In the case of proposals to trial a new technology, the Chief Advisor: Technology Assurance should therefore be kept informed of trial progress, conclusion of the trial, and evaluated outcomes.

If a proposal to adopt (or operationally deploy) a technology is approved under this policy, the Chief Advisor: Technology Assurance should 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, is likely to have a material impact on the Policy Risk Assessment (including, for example, assessment of Proportionality) and will require further governance approvals based on updated documentation.

For proposals where there is medium or high risk (as identified by Chief Advisor: Technology Assurance and agreed to by SPRG), ongoing monitoring of the use of the technology may be set as a condition for approval. This may include regular reporting on usage (e.g. statistics), testing for bias, auditing usage logs for potential misuse, ongoing evaluations of effectiveness and performance, and checking for compliance with controls. A reporting and review schedule will be agreed to with the business owner at the time of approval.

If ongoing compliance with assurance controls cannot be demonstrated, then the approval to use the technology may be revoked. If there is immediate and ongoing harm, or any harm is unclear because we do not have appropriate monitoring in place, the approval can be revoked by the Chief Advisor: Technology Assurance at any time, subject to subsequent review and endorsement of that decision by the SPRG and/or the Executive. Otherwise, the Technology Assurance team will present a paper to SPRG presenting the context and recommending revocation of prior approval.