

INFORMATION SHARING AGREEMENT

Between

Chief Executive of Firearms Safety and Education New
Zealand

and

Commissioner of the New Zealand Police | Ngā Pirihimana o
Aotearoa

(The 'Parties')

Made under section 355(3) of the Arms Act 2026

Version 1.0

Interpretation

The following terms used in this Agreement are defined as follows:

Term	Definition
Arms Act	Arms Act 2026.
Policing Act	Policing Act 2008.
Arms items	Have the meanings given in the Arms Act.
FSE/Arms Regulator	The Arms Regulator established under section 303 of the Arms Act and known as Firearms Safety and Education New Zealand.
Police	New Zealand Police, continued as instrument of the Crown under section 7 of the Policing Act.
Chief Executive	The chief executive of the Arms Regulator appointed under section 305 of the Arms Act.
Commissioner	The Commissioner of the New Zealand Police appointed under section 12 of the Policing Act.
Parties	The parties to this Agreement, being the Commissioner and the Chief Executive.
Police employee	Has the meaning in section 4 of the Policing Act and means a person employed under section 18 of the Policing Act and, except in Part 4 (of the Policing Act), includes a person seconded to Police.
Regulator staff	Police employees who are not constables and who report to (or up to) the Chief Executive as part of FSE, while remaining Police employees for employment purposes under the Policing Act. Regulator staff include both: staff who have a written delegation from the Chief Executive under section 311 of the Arms Act to perform specified Arms Act functions, duties, or powers; and other FSE staff who do not require a section 311 delegation because they perform corporate, administrative, advisory, communications, official information, legal, or other support functions. For Regulator staff with section 311 delegations, section 309 of the Arms Act deems the Chief Executive to hold specified Commissioner employment powers under the Policing Act and removes the Commissioner's ability to exercise those powers for that group. For other Regulator staff, equivalent employment-management authority is provided through Commissioner employment delegations. For the avoidance of doubt, Regulator staff does not include any other "person" who may be delegated functions under section 309 of the Arms Act, and no such other "person" is covered by this information sharing agreement.
Police staff	Police employees, excluding Regulator staff.
FSE information	Information held by FSE.
Police information	Information held by Police.

Information	Means data, facts, knowledge, records, or communications in any form that can be recorded, stored, processed, transmitted, or understood by a person or system, including: • personal Information • official Information • classified Information • confidential Information.
Personal Information	As defined at section 7 of the Privacy Act 2020.
Official Information	As defined at section 2 of the Official Information Act 1982.
Classified Information	Official Information that requires specific security measures to protect its confidentiality, integrity, and availability. It is applied to information that would cause harm to individuals, organisations, or national interests if compromised, and access is strictly limited to individuals with an appropriate national security clearance. Refer: https://www.protectivesecurity.govt.nz/classification
Confidential Information	Means information that is not in the public domain, is known only to a limited group of people, and is communicated or held in circumstances creating an obligation of confidence. Based on information in the Office of the Ombudsman, <i>Confidentiality – A guide to section 9(2)(ba) of the OIA and section 7(2)(c) of the LGOIMA</i> .
Direct data access	Means approved electronic access by a user to information held in another party's system, without a separate case-by-case requirement and subject to access controls, assurance reviews, use limits and/or other safeguards agreed by the Parties.

Legal framework, status, and scope of agreement

1. This Agreement provides for the information that may be shared between the Chief Executive and the Commissioner under section 355(3) of the Arms Act. In accordance with the requirements of section 356, this Agreement sets out:
 - a. the information or classes of information that each party may have access to
 - b. the method and form of access
 - c. safeguards to protect the information
 - d. purposes for access.
2. Section 355(1) and (2) of the Arms Act provide for certain information types that the Commissioner and the Chief Executive must provide each other with access to. Information that may be accessed or disclosed in the performance of this Agreement does not deal with information which one Party is required to provide the other Party with access to under section 355(1) and (2) or 358 of the Arms Act.
3. Pursuant to section 355(4) and (5) of the Arms Act:
 - a. information sharing provided for under section 355 of the Arms Act applies despite anything to the contrary in any contract, deed, or document; and

- b. to the extent this information sharing agreement provides for the disclosure of personal information, that disclosure is additional to the grounds of permitted disclosure under information privacy principle 11 or 12 set out in section 22 of the Privacy Act 2020, but does not otherwise limit or affect those information privacy principles.
- 4. This Agreement does not limit or prevent other lawful means for information sharing.

Context

- 5. From 23 September 2026, the Arms Act 1983 will be repealed and replaced by the Arms Act.
- 6. The purposes of the Arms Act are to:
 - a. promote the safe possession and use of arms; and
 - b. impose controls to prevent the possession and use of arms for criminal activity.
- 7. In accordance with section 4 of the Arms Act, the arms regulatory regime reflects the following principles:
 - a. the possession and use of arms is a privilege; and
 - b. anyone doing anything involving arms must act in the interests of personal and public safety.
- 8. The Arms Act establishes an Arms Regulator, known as Firearms Safety and Education New Zealand (FSE), to oversee all aspects of firearms regulation. FSE will be an autonomous agency of New Zealand Police (Police).
- 9. This means FSE functions will be conducted separate from ordinary policing. FSE will make its own regulatory decisions. Police, however, remains responsible for policing, operational command, detecting and deterring offending, criminal investigation, and public safety responses in relation to firearms. Both FSE and Police have functions that support a safe and effective firearms system.

Parties

- 10. The Chief Executive is appointed as the independent chief executive of FSE under section 305 of the Arms Act. The Chief Executive's responsibilities include performing or exercising the functions, duties and powers of the FSE under the Arms Act. The Chief Executive must act independently of the Commissioner.
- 11. The functions of FSE are set out in section 304 of the Arms Act and include:
 - a. administering the licensing, endorsement, permit, approval, and registry requirements under the Arms Act
 - b. assessing whether people are fit and proper to possess or use arms items, including by considering relevant safety, risk, and compliance information
 - c. promoting the safe possession, secure storage, and responsible use of arms through education, guidance, and engagement with the firearms community

- d. monitoring, auditing, and supporting compliance with regulatory requirements by licence holders, business licence holders, clubs, ranges, and other regulated participants
 - e. using graduated and proportionate regulatory tools to respond to non-compliance, including conditions, suspensions, revocations, inspections, infringement responses, and other statutory interventions where appropriate
 - f. collecting risk and incident information from specified agencies and other authorised sources, where that information is relevant to firearms-related safety, risk assessment, compliance, or regulatory decision-making
 - g. collecting, holding, analysing, and sharing information necessary to support regulatory decision-making, public safety, and the effective operation of the firearms system.
12. The Commissioner is the Commissioner of Police. The functions of the Police include:
- a. keeping the peace
 - b. maintaining public safety
 - c. law enforcement
 - d. crime prevention
 - e. community support and reassurance
 - f. national security
 - g. participation in policing activities outside New Zealand
 - h. emergency management.
13. Areas of common interest between FSE and Police include:
- a. **System Integrity** – maintaining accurate licensing, registry, compliance, and risk information across the firearms system so agencies are acting on the best information available and can maintain oversight of the whole Arms regime.
 - b. **Regulatory Safety** – assessing suitability, managing risk, supporting compliance, and responding to firearms-related incidents
 - c. **Community Safety and Law Enforcement** – preventing, detecting, investigating and resolving serious and organised criminal offending involving firearms, and ensuring that firearms are not misused
 - d. **Boundary Risks and Incidents** – cooperating on risks and incidents involving firearms where Police and FSE functions intersect
 - e. **National Security** – preventing and responding to extremist threats and other national security risks.

The need for information sharing arrangements

14. Purposeful information access and disclosure is a vital enabler to ensure the Parties fully co-operate and coordinate effectively in their areas of common interest. The Parties both need timely access to information to support firearms safety, regulatory

decisions, public safety, and law enforcement. Access status does not affect FSE's independence. When Regulator staff use Police information for Arms Act purposes, they act within the FSE regulatory framework and remain accountable for using the information only for the authorised purpose.

15. To meet the purposes and principles of the Arms Act, regulatory and law enforcement functions must operate in an integrated way. In most situations this will require direct access to information to keep both the public and staff safe. Public safety risks may arise if information is not being routinely accessed or disclosed. This agreement sets out the framework for confident information access and sharing to support an effective regulatory and law enforcement regimes that need to work together.

Guiding principles

16. The guiding principle are:
 - a. the Parties agree that any information accessed or disclosed under this Agreement will be purposeful and connected to the Parties' lawful functions and activities
 - b. it is the responsibility of the accessing Party to establish a lawful purpose prior to accessing information held by the other Party
 - c. it is the responsibility of the disclosing Party to establish a lawful purpose prior to disclosing information to the receiving Party
 - d. it is the responsibility of the receiving or accessing Party to establish a lawful basis prior to using disclosed or accessed information
 - e. except as provided for under this Agreement, each Party is responsible for establishing a lawful basis before on-sharing information obtained under this Agreement with any agency that is not a Party to this Agreement
 - f. the Parties intend to continue to provide feedback and discuss matters of mutual concern that arise in the performance of this Agreement.

Purposes for which information is to be shared

17. The purposes for accessing or disclosing each class of information under this Agreement are described in the Tables at **Appendix A**, Part One and Two.
18. The purposes for FSE accessing or receiving Police information are:
 - a. to support the assessment of third parties connected to an applicant, licence holder, or other regulated person, where Police-held information about those third parties or relationships may be relevant to a fit and proper assessment under the Arms Act, or to the reliability of information provided by them, and/or to whether a person who is not fit and proper may be reasonably likely to have access to firearms (e.g. information about referees, proposed referees, household members and cohabitants)
 - b. to support FSE's regulatory analysis, system oversight, risk identification and strategic regulatory planning functions under section 304, where Police-held

information is relevant to firearms-related harm, emerging risks, system vulnerabilities, compliance priorities, or the effective operation of the firearms regulatory system, and is not limited to a specific applicant, licence holder, or regulated entity.

19. The purposes for Police accessing or receiving FSE information are:
- a. to assist Police to establish whether an activity is legal (e.g. details about manufacturing approvals)
 - b. to assist with the assessment of risk and to support public and Police safety, maintain national security, prevent crime, and provide community support and reassurance (e.g. information from a health practitioner or about lost and stolen firearms reported to FSE)
 - c. to assist with detecting, deterring, and investigating possible offending and prosecuting any offending identified in line with the Solicitor General's Prosecution Guidelines (e.g. non-compliance related information about firearms licence holders, or diversion offending).

Classes of information

20. The classes of FSE information to be shared with or accessed by Police under section 355(3), is limited to the following classes of information set out in Part 1 of **Appendix A**:
- a. information that establishes approval of lawful activity under the Arms Act
 - b. information to assist with the assessment of risk and to support public and Police safety, maintain national security, prevent crime, and provide community support and reassurance (e.g. information from a health practitioner or about lost and stolen firearms reported to FSE)
 - c. information that assists with detecting, deterring, and investigating possible offending and prosecuting any offending identified in line with the Solicitor General's Prosecution Guidelines (e.g. non-compliance related information about firearms licence holders).
21. The classes of Police information to be shared with or accessed by FSE under section 355(3), is limited to the following classes of information set out in Part 2 of **Appendix A**:
- a. information about third parties connected to an applicant, licence holder, or other regulated person that may be relevant to assessing whether the fit and proper person or disqualification criteria for a relevant decision under the Arms Act (see for example sections 70 and 71). This includes Police-held information relevant to mandatory prohibitions, fit and proper person criteria, suitability, firearms safety, public safety, offending, compliance, family violence, organised crime, extremist, national security, or other risk indicators that may inform a decision under the Arms Act.
 - b. strategic, situational, threat-based, operational or analytical Police-held information and information relevant to firearms risk, harm, diversion, trafficking, unlawful possession or use of arms items, organised crime, violent

extremism, national security, family violence, compliance trends, emerging offending patterns, or other system-level risks relevant to FSE's regulatory functions.

Method and form of access

22. Direct data access to the classes of information covered by this agreement is the expected method of access by the Parties. Access by Regulator staff and Police staff respectively is permitted where the purpose is within the scope of their duties and where the information is available for access through existing ICT systems.
23. Case-by-case enquiries, Requests for Information (RFI), may be made in an agreed format, through authorised Party Operational Contacts will be used where:
 - a. the class of information is not available through direct data access; or
 - b. the class of information is classified at the level of SENSITIVE or above; or
 - c. the classes of information, are source-restricted, caveated, particularly sensitive or require assessment. These instances may require source handling, redaction, deconfliction, originator approval, or contextual explanation before it can be provided.
24. Information covered by this Agreement may also be disclosed proactively on the disclosing Party's own initiative.
25. The Parties agree that any information it receives that is relevant to safety risks will warrant urgent proactive sharing and both Parties will work together to ensure that this can occur.
26. The following methods may be used by the Parties when requesting and disclosing information other than by direct data access:
 - a. secure email
 - b. verbal communication (e.g. phone, videoconference, face-to-face communication).

Requests for Information

27. The Parties will designate and maintain Operational Contacts within their organisation through which all RFIs will be processed. The Relationship Management and Operational Contact roles are set out at **Appendix B** to this Agreement. Relationship Managers will ensure Parties have the relevant contact details for Operational Contacts, which may be updated at any time by a Relationship Manager in writing to the other Relationship Manager.
28. Each Party will designate specific Operational Contacts to manage RFIs from the other Party as part of their role description.
29. RFIs may be made by either Party to an Operational Contact using the relevant RFI Templates, unless there is a valid reason for requesting the information via a different channel.

30. RFIs should be documented in a manner that provides for auditing, compliance, and assurance purposes. For example, the use of RFI forms and an email response.
31. Where the Parties request and/or disclose information verbally, (e.g., by phone, videoconference, or face-to-face communication), both Parties will make a written record at the earliest opportunity (e.g. a follow-up email chain, outlining what information was requested and/or shared and the legislative basis for the sharing).
32. A Party that decides 'not to disclose' information when requested to do so will provide reasons for this decision to the other Party.
33. Any unresolved dispute, issue or difference about a decision 'not to disclose' information or provide feedback on the decision, will be referred to the appropriate Operational Contact listed at **Appendix B**.

Use and on-sharing of Information

34. The Party receiving or accessing information will only use it for the purposes of this agreement (refer paragraphs 17 - 19), unless the receiving or accessing Party has a lawful basis for using the information for another purpose.
35. Information will only be disclosed to staff who need to see or otherwise use the information to achieve the purpose/s for which it has been supplied or accessed.
36. For the on-sharing of information, usual considerations will apply, including information Privacy Principle 11 (or other lawful basis) when personal information is involved, or seeking permission from the other Party where other sensitivities arise. Any conditions that apply to the Party that holds the information will also apply to the party that accesses or receives that information.

Compliance safeguards and information management

37. Each Party will take all reasonable steps to ensure Regulator staff and Police staff who are involved with the access or disclosure of information are appropriately vetted, trained and cleared to the appropriate level of the Protective Security Requirements (PSR) classification system. This includes staff who are responsible for submitting, receiving, assessing, and responding to RFIs.
38. All information will be managed in accordance with the New Zealand Government Information Classification System including the requirements set out in the Government's PSR, and the New Zealand Information Security Manual (NZISM).
39. Each Party will assign appropriate classifications and endorsements to each item of information disclosed to the other Party.
40. A Party that receives information will apply the mandatory safeguards and controls to ensure that information is sufficiently protected against any loss or unauthorised access, use, modification or disclosure, or any other misuse.
41. For Police information that FSE receives or has access to, and which section 127 of the Arms Act applies to because disclosure would be likely to:
 - a. endanger the safety of any person; or

- b. prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or
- c. prejudice the entrusting of information to the Police, the New Zealand Security Intelligence Service, or the Government Communications Security Bureau on a basis of confidence by:
 - i. the Government of any other country, or an agency of the Government of any other country; or
 - ii. any international organisation;

the Chief Executive will ensure that such information is withheld in accordance with section 127 of the Act, and where unsure, first consult with Police. Additionally, where a case involving such information is to be considered by the Firearms Licensing Review Committee under the Part 7, subpart 2 of the Arms Act, the Chief Executive will draw this to the attention of the Firearms Licensing Review Committee members and remind them that the information is not to be released (sections 330 and 331 of the Arms Act refer).

- 42. A Party that receives information in the performance of this Agreement will not retain the information once it is no longer required for the purpose it was disclosed, accessed, or used, and in line with each Parties' obligations under the Public Records Act 2006, the Privacy Act 2020 and the Health Information Privacy Code 2020.
- 43. The Parties commit to adopting best practice personal information management practices to ensure that information accessed and shared under this agreement is lawful, proportionate, purpose-limited, role-based, secure, and auditable, including:
 - role based access controls to ensure staff only have access to required systems
 - mandatory staff security and privacy training
 - event logging, alerting and auditing
 - software patching and updating
 - systems certification and accreditation.
- 44. The Information created and held by FSE will continue to be retained and sentenced for disposal in accordance with the Police disposal authority, in accordance with the Public Records Act 2005.

Training and onboarding

- 45. The Parties will encourage opportunities to provide or participate in joint training that will enhance the Parties' capability to meet the objectives of this Agreement.
- 46. All FSE staff who directly access information in the performance of this Agreement will have undertaken normal Police processes including pre-employment checks, be subject to the Police Code of Conduct, have undertaken all Police employee onboarding processes and training, have been inducted by their manager, and be familiar with relevant Police information and security policies. FSE staff will also have

training on any Police databases to which they will have access (e.g. the National Intelligence Application).

47. The Parties will ensure that their respective staff that have direct data access to the other Party's information are those who need it for their duties (role-based approval), and that new staff are instructed about the permissions of their role for data access and sharing.
48. All staff must participate in any further training as required by the Party that owns the database for which further training is required. Staff who do not maintain training currency may have their access revoked, suspended or restricted.

Privacy and security breaches

49. The Parties must notify the other Party of any actual or suspected unauthorised access to, or use, or disclosure, of any information covered by this Agreement as soon as practicable, but no later than 24 hours after the actual or suspected breach is identified.
50. The Parties must investigate any actual or suspected unauthorised access, use or disclosure of any information supplied under this Agreement.
51. Where the breach, or suspected breach, has caused or has the potential to cause serious harm to the affected individuals, the Parties will agree on who is responsible for ensuring that affected people receive appropriate help and that the notifiable breach provisions of the Privacy Act are complied with, including notifying the Privacy Commissioner.
52. If either Party has reasonable cause to believe that a breach of any other security provision in the Agreement has occurred or may occur, that Party may undertake any investigations that it considers are necessary.
53. Where a Party commences an investigation, the other Party will provide the investigating Party with reasonable assistance, and the investigating Party will keep the other Party informed on the progress and outcome of that investigation.
54. If there has been or may have been a breach, either Party may suspend the exchange of information under this Agreement by notice in writing to give the relevant Party time to remedy the breach.
55. All Police employees, whether Regulator staff or Police staff, are subject to Police's Code of Conduct. Any inappropriate access, dissemination or use of information obtained in the performance of this Agreement may be subject to disciplinary proceedings, in accordance with Police's Code of Conduct and relevant Police Instructions. An applicable integrity and conduct standard may apply to Regulator staff under section 19 of the Public Service Act 2020.
56. Police may commence criminal proceedings with respect to any inappropriate access, dissemination, or use of information, depending on the nature and intent of the alleged or suspected conduct.
57. The Independent Police Conduct Authority also has oversight of both Regulator staff and Police staff and may be notified of any breaches of privacy.

Assurance review

58. The Parties will review the operation of this agreement within the first three years of its signing, and thereafter at five-yearly intervals.
59. The purpose of the joint review is to confirm that the safeguards in this Agreement have been implemented and are operating as intended. In doing so, the Parties will consider whether:
 - those safeguards remain proportionate while having regard to the functions of both Parties;
 - the context in which information is being accessed or disclosed;
 - whether information is not being accessed or disclosed when it should be;
 - any barriers to essential information sharing; and
 - the Parties' common interests in public and personal safety are being supported.
60. The joint review also provides an opportunity to identify and resolve any practical issues that have arisen in relation to the direct data access arrangements.
61. The Parties will agree on the review methodology detailing the review procedures, documentation and evidential requirements prior to commencing the first review. This procedure will be managed by the Party Representatives listed at paragraph 78 below.
62. Additional reviews may be undertaken if Police or FSE agree that it is necessary or desirable, including because of unauthorised access, use or disclosure of any information covered by this Agreement that has, or may result in, serious harm to an affected individual or individuals.

Accuracy of Information

63. Reasonable steps will be taken to ensure that any information accessed or disclosed in accordance with this Agreement is timely, accurate, up-to-date, and complete at the date of disclosure.
64. It is the duty of the receiving or accessing Party to verify the Information should it be intended to take further action.

Transfer of Requests for Information

65. If either Party receives an information request from a third party the Official Information Act 1982 or the Privacy Act 2020 (including a correction under Information Privacy Principle 7), the Party that receives the request may transfer the request to the other Party where:
 - a. the Party that receives the third-party request does not hold the information requested and believes the other Party does; or
 - b. the Party that receives the request believes the request is more closely connected with the other Party's functions or areas of responsibility.

Māori data considerations

66. The Parties recognise that Māori data may be held, accessed, used, or shared through several information pathways between Police and FSE in the firearms system. The parties will be guided by the Māori Data Governance Model designed for use across the public service.

Issue or dispute resolution

67. The Parties will attempt in the first instance to resolve all issues, disputes or differences concerning the interpretation or performance of this Agreement locally (by local representatives or managers and the relevant Operational Contact) and at the earliest opportunity.
68. If agreement cannot be reached within 28 calendar days, then the matter should be referred to the appropriate Relationship Managers, detailed at **Appendix B**, for resolution.
69. If agreement cannot be reached within a further period of 28 calendar days, then the matter will be referred, in writing, to the Commissioner and the Chief Executive for their resolution.

Commencement, review, and termination

70. This Agreement shall come into effect on the date of signature by the Commissioner and the Chief Executive. It remains in effect unless otherwise notified and agreed to by both Parties.
71. The Parties shall review this Agreement at intervals of no more than five years.
72. Each Party has the right to review at any time on providing 30 calendar days' notice in writing to the other Party.
73. All notices of review shall be in writing and sent to the Party Representatives listed at paragraph 78 below.
74. Any variation will take effect once agreed in writing between the Parties, having first been consulted with the Privacy Commissioner in accordance with section 356(3) of the Arms Act.
75. This Agreement may only be terminated by the Commissioner or the Chief Executive (or their authorised delegates) providing formal notice in writing to the other Party. The termination will take effect three months after the notice of termination is received, unless the Parties mutually determine otherwise.
76. If there are changes to Government policy or agency practice or changes proposed to Party's ICT systems which may affect the purpose or operation of this Agreement, each Party agrees to:
 - promptly inform the other of those changes

- review and vary any aspects of this Agreement in accordance with section 356(2), and after consulting with the Privacy Commissioner, as per section 356(3) of the Arms Act.

77. Any Schedules attached to this Agreement form part of the Agreement.

Party representatives

78. The Parties assign the following position-holders as their Party representatives for this Agreement:

- **Police** – Commissioner of New Zealand Police: Richard Chambers
- **FSE** – Chief Executive of Firearms Safety and Education New Zealand: Dr Kelvin Watson

Costs

79. Unless otherwise agreed, the cost of meeting the commitments of this Agreement should be met by the Party incurring the cost.

Commencement

80. This agreement will take effect on 23 September 2026.

Signatures



Commissioner of New Zealand Police
Richard Chambers

Date 22 September 2026



Chief Executive of Firearms Safety and
Education New Zealand

Date

Appendix A: Classes of Information

Part 1 – Classes of FSE information to be accessed New Zealand Police

This Part captures information covered by the section 355(3) information sharing agreement. This information is in addition to information Police can directly access under section 355(1) and 358.

	Purpose for Police accessing or receiving information	Class of information held by FSE relevant for this purpose	Examples of Information required (not exhaustive list)
1	To assist Police in establishing whether activity is legal for a policing purpose in section 9 of the Policing Act 2008.	Information that establishes lawful activity.	Details of gun shows consented to (refer s. 88). Information about approvals for theatrical use, including on-site theatrical armourers, dates and approved locations (refer ss. 87 and 89). Information about approved ammunition sellers (refer ss. 175-184). Information about approved pistol shooting clubs and certified pistol shooting ranges; and enrolled non-pistol shooting clubs, enrolled non-pistol shooting ranges, and temporary non-pistol shooting ranges, and any cancellations or suspensions (refer ss. 218-221, 226-228, 232-238, 240, 243-245, 248-249). Information about the activities business licence holders are permitted to undertake and classes of arms items they are permitted to hold and sell (s. 85). Information about pest controller records, i.e. who is permitted to be in possession of restricted firearms under multi-user agreement at any given time (refer s. 277).

			Details of all permits issued and used (includes permits to possess including where manufactured under s. 66), permits to import (including permits to import by visitor licence holders and when the firearms are removed from the country under s.138) and information about exports under s. 202.
			Details of persons who have been authorised or permitted to possess restricted ammunition (refer s. 38).
			Firearms licence photos.
			Details about manufacturing approvals issued (refer ss. 66-68).
			Details about museum licences (refer s. 102 and 111).
			Details about museum worker licences and relevant museum and classes of arms items (refer ss. 113, 118-121).
			Details about firearms licences status, including suspension, and decisions following suspension, but also expired licences and decisions on expired licences where the licence holder has applied for new firearms licence.
			Details about a licence holder who has surrendered their licence.
2	To support public and Police safety, prevent crime,	Information to assist with assessment of risk to keep the	Details of persons approved to receive arms items and ammunition following revocation, surrender or expiry of firearms licence (ss. 164 – 166).
			Red flag/risk information, e.g. including third party information reported by a health practitioner or member of the public.

	protect national security, and provide community support and reassurance (e.g. when interacting with firearms licence holders, or when assessing whether a person poses a national security risk).	public and Police safe, maintain national security, prevent crime and provide community support and reassurance [This also includes all information for purpose 1 listed in column 3]. For example, this information is provided to the Tactical Intelligence Analysts to inform staff safety persons of interest (SSPOI) assessments.	Information on lost and stolen arms items reported to the FSE (refer s. 136).
3	To detect, deter, and investigate possible offending and prosecuting any offending identified in accordance with the Solicitor-General's prosecution guidelines (e.g. non-compliance related information about firearms licence holders, diversion of firearms).	Information that assists with detecting, deterring and investigating possible offending and prosecuting any offending identified [This also includes all the information in purposes 1 and 2 listed in column 3].	Case file information, e.g. information from a firearms licence such as referee details. Non-compliance related information about licence holders (e.g. infringement notices, improvement notices). Information about illegally held arms items or suspicious activity detected by the FSE (i.e. information that when analysed may uncover potential offending or further lines of enquiry). Information about what action the FSE is taking when a licence ends or is suspended to recover arms items, ammunition and the licence card. Information about Chief Executive-received notification of non-delivered arms items (refer s. 137).

Part 2 – Classes of Police information to be accessed by FSE

This Part captures information covered by the s 355(3) information sharing agreement. This information is in addition to information FSE can directly access under section 355(2).

	Purpose for FSE accessing or receiving Police information	Class of information held by Police relevant for this purpose	Examples of Information required (not exhaustive list)
1	To support the assessment of third parties connected to an applicant, licence holder, or other regulated person, where Police-held information about those third parties or relationships may be relevant to a fit and proper assessment under the Arms Act, or to the reliability of information provided by them, and/or to whether a person who is not fit and proper may be reasonably likely to have access to firearms. Examples include information about referees, proposed referees, household members and cohabitants.	Police information about third parties connected to an applicant, licence holder, or other regulated person that may be relevant to assessing whether the fit and proper person or disqualification criteria for a relevant decision under the Arms Act (see, for example, sections 70 and 71). This includes Police-held information relevant to mandatory prohibitions, fit and proper person criteria, suitability, firearms safety, public safety, offending, compliance, family violence, organised crime, extremist, national security, or other risk indicators that may inform a decision under the Arms Act.	Information about referees, proposed referees, household members, cohabitants, associates or other connected persons that may be relevant to the matters the chief executive must consider including under ss 70-72, 146-147, and 153 to 158. For example: information indicating whether a third party may affect the reliability, accuracy or completeness of referee information or other information provided in support of an application, licence, endorsement, permit, certification or enrolment decision. Information that Police have received from other law enforcement agencies, intelligence or security agencies, overseas agencies, health practitioners, members of the public or other authorised sources.

2	To support FSE's regulatory analysis, system oversight, risk identification and strategic regulatory planning functions under section 304, where Police information is relevant to firearms-related harm, emerging risks, system vulnerabilities, compliance priorities, or the effective operation of the firearms regulatory system, and is not limited to a specific applicant, licence holder, or regulated entity.	Strategic, situational, threat-based, operational or analytical Police information and information relevant to firearms risk, harm, diversion, trafficking, unlawful possession or use of arms items, organised crime, violent extremism, national security, family violence, compliance trends, emerging offending patterns, or other system-level risks relevant to FSE's regulatory functions.	Information that assists FSE to identify emerging risk indicators, compliance priorities, regulatory interventions, education needs, audit priorities, or opportunities to strengthen system integrity. For example: strategic, tactical, operational or analytical products relevant to firearms-related harm, offending, diversion, trafficking, unlawful possession or use of arms items, or emerging risks across the firearms system. Information about patterns, trends, locations, groups, associations, entities, behaviours, typologies or vulnerabilities that may affect FSE's regulatory priorities, compliance activity, education activity, licensing settings, or risk-based decision-making.
---	---	---	--

Appendix B - Relationship managers and operational contacts

FSE	New Zealand Police
Relationship Manager	Relationship Manager
Director Communities and Corporate	Strategic Advisor District Support
Operational Contact	Operational Contact
Director Regulatory Compliance and Investigations	Firearms Relationship Manager
Operational Contact	
Director Service Delivery	