

Information for External Researchers Applying for Access to Resources, Data or Privileged Information

Applying for access to data or resources

External researchers are required to apply for access to Police data or to access resources of Police, including staff time or involving staff as participants in research. External researchers include Police staff who may be studying towards a higher degree or collaborating with any external agency on a research project.

It is the principal researcher's responsibility to ensure that the process described below is followed.

1. Read *the Police Policy for External Researchers' Access to Resources, Data or Privileged Information*, available on the Police website. This outlines the Police's Policy for providing access to its data, resources or privileged information, including relevant legislation and protocols, the principles governing this access, and the requirement for external researchers to enter into a Police Research Agreement. The Policy applies to all external researchers who request access to Police data, resources or privileged information.

Police may additionally require, before granting research approval and entering into a Research Agreement, that members of the research team undergo Vetting checks. Individual researchers failing the Vetting standard may only be granted access at the discretion of the Director Research and Evaluation in consultation with a member of the Police Executive.

An application to access data assumes researchers agree to comply with the Policy and the specific terms and conditions set out in the Research Agreement.

2. Check the availability and content of the dataset(s) of interest. This involves:

- a. consulting Police Research and Evaluation staff to determine whether a dataset is available;
- b. checking any information provided about the dataset (e.g. the questionnaire and/or any methodology reporting) to ensure that the data are available to support the proposed research.

3. Check the fit between the proposed research and the purposes for which the data were collected to ensure that these are not inconsistent (see Policy Principle 2 – Purpose).

4. Check that criteria for researcher access to the dataset are met (see Policy Principle 3 – Researchers).

5. Contact Police Research and Evaluation staff with any queries.

6. There is no application form to fill out but the application should consist of:

- a. Research proposal describing the research design, methodology, confirmation of relevant ethics committee approval and specific details of Police resource needed

including estimates of the amount of Police staff time involved. A template research proposal can be provided upon request.

- b. CV for the principal researcher.
- c. Declaration signed by an authorised delegate of the organisation, who is not one of the researchers, indicating support for the research and confirming that the researchers will abide by the terms and conditions of access
- d. Any other relevant background material.

7. Send the application documents to Police research@police.govt.nz.

Application consideration and approval

Upon receiving the application documents from an external researcher, Police will undertake the following steps.

1. Acknowledge receipt of the application and advise the applicant approximately how long the decision process is likely to take.

2. Consider whether the application is consistent with the principles in the Policy. Also considered will be:

- a. a decision on suitability of the applicant to carry out the research
- b. dataset availability
- c. compliance with purpose and researcher criteria
- d. likely quality (of outputs)
- e. security or confidentiality concerns.

3. Police must balance public interest in the activities of Police with the obligation to provide data to those who request it. With this in mind, Police has first priority for using the data. Priority for data access will also be given to researchers from organisations who have worked in partnership with Police in the management or collection of the relevant data.

Priority will then be given to researchers who have overseen or contributed to the relevant data via a Research Coordinating Group, Expert Reference Group or other such group as recognised by Police. While these priorities need to be considered, our obligation is to provide access to the data, where appropriate.

4. Advise the principal researcher of the outcome. The Police may additionally require, before granting research approval and entering into a Research Agreement, that members of the research team undergo Police Vetting or other Security Clearance check.

5. If the application is successful, provide the Research Agreement to be signed by the principal researcher, all researchers and a representative of the principal researcher's organisation.

If the application is unsuccessful, the principal researcher may resubmit an amended application.

Anyone who wishes to comment or provide feedback on their experiences with the application and the Policy may do so by way of email to: research@police.govt.nz.

Dealing with inappropriate disclosure

In the event of a breach in privacy, confidentiality or security, the following steps must be taken.

1. It must be immediately reported to the Police Director, Research and Evaluation, as per the Research Agreement.
2. The disclosure must be reported in the Police Security and Privacy Incident Register Database (SPIRD).
3. Police staff unrelated to the incident should investigate the details and assess the impact of the incident and its seriousness.
4. Police staff must forward recommendations about appropriate actions to the Police Director, Research and Evaluation.
5. The Police Director, Research and Evaluation is to approve proposed action to remedy the breach and impose any appropriate penalties. Penalties will be imposed in accordance with legal and ethical requirements and with consideration of the potential impact on public trust and confidence in Police.

The process will be transparent, except where publicising the incident could result in a further breach.