

**Guide to completing T031— Application for access to unlisted mobile phone numbers for permitted research**

**Application to use and disclose unlisted mobile phone information in the Integrated Public Number Database for permitted research under the *Telecommunications Regulations 2001***

The form relates to division 5.2 of the *Telecommunications Regulations 2001.*

TABLE OF CONTENTS

ABOUT FORM T031 3

TERMINOLOGY 3

COMPLETING THE FORM 5

LODGMENT INFORMATION 5

TIMEFRAMES AND CONSULTATION 5

ACMA PRIVACY STATEMENT 6

COMPLETING THE FORM 7

PART 1: Sole or primary entity and research details 7

**Questions 1–7—proposed permitted research** 7

**Question 8—receipt of mobile information** 8

PART 2: Research entity details 9

**Question 1—previous authorisation/s** 9

**Question 2–6—legislative compliance including the Privacy Act** 9

**Questions 7–8—use and disclosure of mobile information** 10

**Question 9—your obligations when calling people** 11

**Questions 10–11—contacted person’s consent** 11

**Question 12—internal dispute resolution procedures** 12

**Question 13—disclosure and de-identification of authorised research** 12

**Question 14—your research employees** 12

**Questions 15–17—technical systems for accessing mobile information from IPND Manager** 13

**Question 18—contravention of authorised conditions** 13

**Questions 19–20—no use or disclosure of mobile information when authorisation ends** 13

**Question 21—no use or disclosure of research information when authorisation
ends/voluntary removal** 14

**Question 25—no use or disclosure of research information if you are removed from
an authorisation** 14

PART 3: Privacy Impact Assessment 15

**THIS GUIDE NOTE IS NOT A SUBSTITUTE FOR LEGAL ADVICE**

# ABOUT FORM T031

These notes assist applicants to complete *T031— Application for access to unlisted mobile phone numbers for permitted research* and the Privacy Impact Assessment(application form). They are a guide only and should not be relied upon as legal advice or ACMA endorsement of an application.

|  |  |
| --- | --- |
|  | *You are encouraged to seek independent advice.* |

The application form is for individuals or entities seeking authorisation to use unlisted mobile phone numbers and/or related postcodes from the Integrated Public Number Database (IPND) under the [*Telecommunications Regulations 2001*](https://www.legislation.gov.au/Details/F2019C00671) (the Regulations)*,* for **permitted research** (Reg 1.7A). This means research which isn’t primarily commercial and is one of the following:

* is relevant to public health, including epidemiological research
* relates to an **electoral matter** and is conducted by or for:
* a registered political party
* a political representative
* a candidate in an election for an Australian Parliament or a local government authority
* will contribute to the development of public policy and is conducted by or for the Commonwealth or a **Commonwealth entity**.

The application form can be downloaded from the ACMA website:

[acma.gov.au/accessing-ipnd](https://www.acma.gov.au/accessing-ipnd)

For more information about the IPND, see the ACMA’s website [acma.gov.au](http://www.acma.gov.au).

# TERMINOLOGY

In these notes and in the application form, all bolded terms are defined in the Regulations.

You should review the definitions in the Regulations and note the difference between **mobile information** and **research information**:

* **Mobile information** is the shortened term used in this guide and the application form for **authorised** **unlisted mobile number information**. In summary, it means an unlisted mobile number in the IPND that appears to be for residential use and/or the associated postcode, and the ACMA has authorised its use for **permitted research**.
* **Research information** means the information you get from a person you contact using the **mobile information** for the purposes of **the research**.

|  |  |
| --- | --- |
|  | *The definitions of* ***mobile information*** *and* ***research information*** *link them strictly to* ***permitted research*** *under authorisation. This means you can’t use* ***mobile information*** *and* ***research information*** *for other research/purposes.* |

Questions in the application deal with either or both **mobile information** and **research information** and you should address your responses accordingly.

Unless the context indicates otherwise, **evidence** means evidence of your practices, procedures, processes and systems that are or will be in place to comply with conditions of authorisation.

# COMPLETING THE FORM

The form has three parts and a declaration.

Sole Applicants

If you are the sole applicant, you must complete Parts 1, 2 and 3 and sign the declaration at the end of the application form.

Multiple Applicants

If you are applying for authorisation with other researchers under the same application:

* the primary/lead **research entity** must complete Parts 1 and 2
* every applicant must individually complete Part 2
* the primary/lead **research entity** must lodge Part 3, the Privacy Impact Assessment. Only one assessment is required but it must cover all applicants. Refer to the Office of the Australian Information Commissioner website [oaic.gov.au](http://www.oaic.gov.au) for assistance
* every applicant must sign the declaration at the end of the form.

|  |  |
| --- | --- |
|  | *There are serious penalties for knowingly providing false or misleading information to a Commonwealth entity such as the ACMA.*  |

# LODGMENT INFORMATION

**How to submit the application**

By email to: ipnd@acma.gov.au

Or by post to: IPND

Australian Communications and Media Authority

PO Box 13112 Law Courts

Melbourne VIC 8010

**Help with lodging an application**

For assistance completing or submitting the application, email ipnd@acma.gov.au or call the ACMA Customer Service Centre during business hours on 1300 850 115.

## TIMEFRAMES AND CONSULTATION

Once the ACMA receives a valid application, it has up to 90 calendar days to decide to grant or refuse an authorisation. This timeframe can be extended if the ACMA requests further information from an applicant. If the information is not provided:

* where there are multiple applicants under one application, the ACMA can disregard the entity which does not respond to the information request
* where there is a single applicant, disregard the application.

|  |  |
| --- | --- |
|  | *You should carefully read Part 1 and Division 5.2 of the Regulations before completing the application form and contact the ACMA if you have questions. A comprehensive application addressing all requirements of the Regulations with reasonable detail and specificity will assist the ACMA’s timely assessment.* |

The ACMA may consult any person or body it considers appropriate when assessing an application. The ACMA may inform you that it is doing so, but is not required to tell you that it is consulting.

# ACMA PRIVACY STATEMENT

The *Privacy Act 1988* (the Privacy Act) imposes obligations on the ACMA in relation to the collection, security, quality, access, use and disclosure of personal information. These obligations are detailed in the Australian Privacy Principles.

The ACMA may only collect personal information if it is reasonably necessary for, or directly related to, one or more of the ACMA’s functions or activities.

The ACMA will not use the information in an application for any other purpose, nor will we disclose it, unless we have your consent, or we are otherwise permitted to do so under the Privacy Act.

Further information on the Privacy Act and the ACMA’s Privacy Policy is available at [acma.gov.au/privacy-policy](https://www.acma.gov.au/privacy-policy). If you have any questions, please contact the ACMA’s privacy contact officer by email at privacy@acma.gov.au.

# COMPLETING THE FORM

|  |  |
| --- | --- |
|   | *Please be* ***specific*** *in your responses and avoid general statements. Responses such as ‘We confirm we will comply with this requirement’ or ‘We comply with the [Privacy Act/industry code]’* *mean the ACMA will write to you to request further information. Better responses will do one or more of the following:* * *provide documents showing, or describe in reasonable detail, relevant* ***practices, procedures, processes and systems*** *you have in place now, or will develop, to comply with conditions of a research authorisation. If you provide a supporting document, please point to the relevant parts of the document.*
* *refer to specific provisions of other legislation or regulations with which you comply, and explain or provide examples of* ***how*** *you comply with those provisions and* ***how*** *that equates to compliance with conditions of a research authorisation.*
 |

## PART 1: Sole or primary entity and research details

Part 1 must be completed by a sole applicant, or by the primary/lead applicant for an application that covers multiple applicants.

**Questions 1–7—proposed permitted research**

You:

* can request access to unlisted mobile phone numbers or associated postcodes or both
* must indicate how many mobile numbers and/or postcodes you want, and the basis on which they are requested. For example, an applicant conducting research for a state based public health project might request all mobiles with postcodes in that state
* can only access **mobile information** to conduct **permitted research** (see below) that isn’t primarily commercial
* need to describe the proposed research in enough detail for the ACMA to be satisfied the research is **permitted research**
* can only request access to the **mobile information** for up to 12 months.

**Public health research**

Public health research includes epidemiological (that is, relating to the incidence, distribution, and control of diseases).

**Electoral matter research**

**Electoral matter** is defined in the Regulations as a matter which is intended or likely to affect voting in:

* an election to an **Australian Parliament** or to a **local government authority**
* a referendum under a law of the Commonwealth or a law of a State or Territory.

Applicants are required to provide the details of the candidate, **political representative** or **registered political party** and the relevant jurisdiction.

**Public policy research for the Commonwealth or a Commonwealth entity**

Research conducted by or for the Commonwealth or a **Commonwealth entity** must contribute to the development of public policy.

A **Commonwealth entity** as defined in the *Public Governance, Performance and Accountability Act 2013* is:

* a Department of State
* a Parliamentary Department
* a listed entity
* a body corporate established by a law of the Commonwealth.

Research conducted for a primarily commercial purpose is not **permitted research**. The aim is to ensure that researchers can’t access IPND information primarily for a commercial purpose. However, if you are conducting research for another entity, you can receive a financial benefit (such as payment) for providing the research services. You should provide sufficient information about the primary and secondary purpose/s (if applicable) of the proposed research.

|  |  |
| --- | --- |
|  | *If the* ***research*** *is to be conducted for another entity (for example a public health organisation, a* ***registered political party*** *or a* ***Commonwealth entity****), you need to provide evidence of your authority to conduct the research for that entity (for example, a signed contract or letter of authority).* |

**Question 8—receipt of mobile information**

If there is more than one applicant, one entity (usually the primary or lead **research entity**) can nominate to receive the **mobile information** from the IPND Manager on behalf of all applicants. The entity that receives the **mobile information** must confirm that it will, within 10 business days of receiving the information, inform:

* the ACMA
* any other research entity under the same authorisation.

|  |  |
| --- | --- |
|  | *The IPND Manager charges for the provision of the* ***mobile information****. Applicants are encouraged to review the IPND Manager’s website* *telstra.com.au/consumer-advice/ipnd* *and/or mail* *ipnd.manager@team.telstra.com* *for information on costs and other matters, such as the format in which the* ***mobile information*** *is provided.* |

## PART 2: Research entity details

Part 2 of the application form must be completed individually by all applicants. This covers matters the ACMA must consider when deciding whether to grant an authorisation, including details and evidence about how you will comply with the conditions of an authorisation, if granted.

**Question 1—previous authorisation/s**

If you’ve been authorised under the Regulations or the *Telecommunications Integrated Public Number Database Scheme 2017* before, the ACMA takes your compliance with that previous authorisation into account.

If applicable, you need to provide evidence of:

* the previous authorisation, such as correspondence from the ACMA granting authorisation
* the extent of your compliance with a previous authorisation, such as a summary of the previous research project, how it was conducted, any issues and how they were resolved, etc.

**Question 2–6—legislative compliance including the Privacy Act**

You must be covered by the *Privacy Act 1988* (the Privacy Act) for the period of a research authorisation. This is a condition of authorisation and the only exception applies to **registered political parties**. If you are conducting research for a **registered political party** (but you are not a **registered political party** yourself), you must still be covered by the Privacy Act.

‘Covered by the Privacy Act’ means one of the following:

* an organisation within the meaning of the Privacy Act
* a ‘small business operator’ (within the meaning of the Privacy Act) that has chosen to be treated as an organisation under section 6EA of the Act.

If you are going to collect, use or disclose personal information in connection with the **authorised research**, you must:

* not breach the Australian Privacy Principles (APP) or a [**registered APP Code**](https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/)
* ensure your collection, use and disclosure of personal information complies or is consistent with the Privacy Act.

These conditions apply even if you are a **registered political party** or some of your political acts or practices are exempt under section 7C of the Privacy Act 1988.

For more information about APPs, applicants should visit the Office of the Australian Information Commissioner’s website [oaic.gov.au](http://www.oaic.gov.au)

You need to provide evidence about compliance with the APPs and **registered APP codes**. This may include written policy and procedure documents such as privacy policies and/or data handling protocols and staff training materials.

You must comply with all applicable unsolicited contact laws, namely the Privacy Act, the *Spam Act 2003* and the *Do Not Call Register Act 2006*.

More information can be found at:

* *Privacy Act 1988*—[oaic.gov.au](https://www.oaic.gov.au/)
* *Spam Act 2003*—[acma.gov.au](https://www.acma.gov.au/)
* *Do Not Call Register Act 2006*—[donotcall.gov.au](https://www.donotcall.gov.au/).

You must also comply with applicable rules under the *Telecommunications Act 1997* and any legislative instrument made under that Act. This includes the [Telecommunications (Telemarketing and Research Calls) Industry Standard 2017](https://www.legislation.gov.au/Series/F2017L00323)(the Industry Standard).

This includes:

* section 139 of the Telecommunications Act about agreements, contracts or arrangements for telemarketing and research activities
* the [Industry Standard](https://www.legislation.gov.au/Details/F2017L00323) which applies to voice calls made to Australian numbers for certain purposes including to conduct opinion polling or standard questionnaire-based research.

More information about the Industry Standard can be found at [donotcall.gov.au](https://www.donotcall.gov.au/).

|  |  |
| --- | --- |
|  | *Compliance with requirements under the Industry Standard is in addition to the requirements to provide certain information to contacted persons under the Regulations – see question 9 below.* |

|  |  |
| --- | --- |
|   | *Evidence may include procedure documents, call scripts, description of technical processes to meet requirements (such as technological measures to restrict calling times) and* ***research employee*** *training materials.*  |

**Questions 7–8—use and disclosure of mobile information**

You must not record or use **mobile information** unless it is for the **research** for which the ACMA granted authorisation. You need to demonstrate that you will comply with this requirement and that the **mobile information** won’t be used for other purposes.

You can only disclose **mobile information** to:

* your **research employees**—note: this meansan individual employed or engaged by you to conduct the authorised research
* other **research entities** covered by the same authorisation
* the ACMA (if requested).

This means, for example, if:

* you employ people to work on other research projects, you must not disclose the **mobile information** to them
* ifyour **research employees** work on the **permitted research** and *other* research projects at the same time, **research employees** can only use the **mobile information** for the **permitted research** (not any other research).

Evidence might include documented:

* protocols for physically or electronically restricting access to the **mobile information**
* protocols for ensuring the **mobile information** can only be accessed by specified **research employees** conducting the **permitted research**
* education/training materials for **research employees.**

**Question 9—your obligations when calling people**

You can only contact a person using **mobile information** by calling the person (the **contacted person**). The Regulations specifically say that you can’t use it to send texts.

During the call, your conversation with the **contacted person** must include:

* your (the **research entity’s)** name
* the purpose of the research—note: this must align with the purpose for which authorisation is granted
* how you obtained the mobile number used to call the **contacted person**
* how youpropose to use the **contacted person’s research information**
* that you have been authorised to use **mobile information** from the IPND by the ACMA for the purposes of the research
* if asked by the **contacted person**—how the **contacted person** can access any personal information you hold about them;
* asking the **contacted person** if they consent to the use and disclosure of their **research information**
* telling the **contacted person** that that they may withdraw any consent so given at any time during the call
* providing the **contacted person** any other information that is required by law (for example, under the Privacy Act).

|  |  |
| --- | --- |
|  | *Compliance with these requirements is in addition to other requirements including under the Industry Standard—see question 6 above.* |

|  |  |
| --- | --- |
|   | *Applicants must provide evidence that they will provide the required information to* ***contacted persons****. Evidence may include a detailed call script and training materials for* ***research employees****.* |

**Questions 10–11—contacted person’s consent**

If a **contacted person** says, during a call, that they refuse or withdraw consent to the use or disclosure of their **research information**, certain rules apply to you.

You must:

* not record, use or disclose the **research information**
* not use the person’s mobile number and/or postcode
* as soon as reasonably practicable but within 10 business days at the latest, take all reasonable steps to destroy the **contacted person’s** **research information**
* notify other **authorised** **research entities** covered by the same authorisation about the consent withdrawal.

You must also have practices, procedures, processes and systems in place to:

* action notifications you receive from another **research entity** under the same authorisation that a **contacted person** has refused/withdrawn consent
* ensure **research information** about a contacted person who refuses/withdraws consent is not used or disclosed.

|  |  |
| --- | --- |
|   | *Evidence may include procedure documents, call scripts, description of technical processes to meet requirements (such as automatic deletion of incomplete polls/surveys and inclusion of mobile numbers on an internal ‘do not call’ list) and* ***research employee*** *training materials.*  |

**Question 12—internal dispute resolution procedures**

**You** must have internal dispute resolution procedures to handle inquiries or complaints from a **contacted person** about your use or disclosure of their **research information**.

The procedures must show:

* how you will deal with inquiries and complaints
* that you will provide the ACMA’s contact details to a person who wishes to escalate a complaint
* how you will provide reasonable assistance in relation to a complaint if so requested by the ACMA.

|  |  |
| --- | --- |
|   | *Evidence should include a written internal dispute resolution procedure and may include call scripts and other standard information to be provided to complainants, and* ***research employee*** *training materials.* |

**Question 13—disclosure and de-identification of authorised research**

You can only disclose **research information** in the following ways:

* to **research employees**
* if it is de-identified (meaning it does not identify the **contacted person**, and the **contacted person** is not reasonably identifiable from the information) and it does not include the person’s public number
* as authorised or required under an applicable law.

You must provide evidence of practices, procedures, processes and systems to meet this requirement.

|  |  |
| --- | --- |
|   | *Evidence may include policy documents, technical security measures, and* ***research employee*** *training materials.* |

The Office of the Australian Information Commissioner provides guidance on when a person is reasonably identifiable from information—[oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information](https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information).

You must carefully consider whether methods to **de-identify** **research information** are sufficient and should seek further advice if required.

|  |  |
| --- | --- |
|  | *This rule is subject to the requirements that apply if a* ***contacted person*** *refuses or withdraws consent. In this case, an* ***authorised research entity*** *must not record, use or disclose the* ***research information****, and must take all reasonable steps to destroy it within 10 business days (see questions 10–11 above).* |

**Question 14—your research employees**

You must take all reasonable steps to ensure your **research employees** are aware of and comply with conditions of authorisation and that they notify you of anything that might result in a breach of conditions of authorisation.

|  |  |
| --- | --- |
|   | *Evidence might take the form of* ***research employee*** *training materials, training and education systems, and process/procedure documents to be followed in the event of a contravention or possible contravention of a condition.* |

**Questions 15–17—technical systems for accessing mobile information from IPND Manager**

Youmust have technical systems capable of receiving the **mobile information** from the IPND Manager. You are also asked:

* whether **mobile information** and **research information** will be accessible to or handled by overseas entities
* if so, to provide evidence of the privacy and security measures which will protect the information when accessed/handled by the overseas entity.

|  |  |
| --- | --- |
|   | *Evidence might include documentation and/or detailed descriptions of security measures such as:* * *premises and storage security including restricted authorised access*
* *encryption, password protection, firewalls, audit trails*
* *limiting access to mobile information and research information to required research employees only.*
 |

|  |  |
| --- | --- |
|  | *If authorisation is granted by the ACMA, the* ***mobile information*** *is provided to the sole or primary applicant (unless another applicant is nominated) by Telstra, the IPND Manager, and there are associated charges. Applicants are encouraged to review the IPND Manager’s website* *telstra.com.au/consumer-advice/ipnd* *and/or email* *ipnd.manager@team.telstra to* *confirm information on costs and other matters, such as the format in which the* ***mobile information*** *is provided.* |

**Question 18—contravention of authorised conditions**

If a condition of an authorisation is contravened, you must give written notice to the ACMA and take reasonable steps to minimise the effects of the contravention.

|  |  |
| --- | --- |
|   | *Evidence might take the form of* ***research employee*** *training materials, training and education systems, and process/procedure documents to be followed in the event of an actual or potential contravention of a condition and for notifying the ACMA.* |

**Questions 19–20—no use or disclosure of mobile information when authorisation ends**

When one of the following occurs, you become a **former authorised research entity:**

* an authorisation ends
* you remove yourself voluntarily from an authorisation with ACMA approval
* you are removed from an authorisation by the ACMA for breaching a condition of authorisation.

There are restrictions on the use and disclosure of **mobile information** by **former authorised research entities**.

You must provide evidence demonstrating that you will:

* not record or use **mobile information**
* not disclose **mobile information** unless authorised or required to do so by the ACMA
* take reasonable steps to destroy the **mobile information** within 10 business days after the authorisation ends or you are removed from the authorisation.

|  |  |
| --- | --- |
|   | *Evidence may include documents outlining or detailed description of technical processes to meet requirements (such as bulk deletion of* ***mobile information****), senior sign-off of destruction of* ***mobile information*** *and* ***research employee*** *training materials.* |

**Question 21—no use or disclosure of research information when authorisation ends/voluntary removal**

There are also restrictions on the use and disclosure of **research information** by **former authorised research entities** when an authorisation ends, or you voluntarily remove yourself from an authorisation.

You must provide evidence demonstrating that you will not:

* record or use **research information**
* disclose **research information** unless the information is de-identified (that is the information does not identify the **contacted person** and the **contacted person** is not reasonably identifiable from the information) and does not include the **contacted person's** public number.

|  |  |
| --- | --- |
|   | *Evidence may include documents outlining or detailed description of technical processes to meet requirements (such as bulk deletion of* ***research information****), senior sign-off of destruction of* ***research information*** *data and* ***research employee*** *training materials.* |

**Question 22—no use or disclosure of research information if you are removed from an authorisation**

The rules are different if the ACMA removes you from a **research authorisation** following a breach of your authorisation. In this case, you must:

* not record, or use, the **research information**
* not disclose the **research information**, unless authorised, or required to do so by or under an applicable law
* take all reasonable steps to destroy the **research information** within 10 business days after you are removed from the authorisation.

|  |  |
| --- | --- |
|   | *Evidence may include documents outlining or detailed description of technical processes to meet requirements (such as bulk deletion research information), senior sign-off of destruction of research information data and* ***research employee*** *training materials.* |

## PART 3: Privacy Impact Assessment

Each applicant is required to submit a Privacy Impact Assessment (PIA) as part of an application for authorisation.

A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

The Office of the Australian Information Commissioner sets out 10 steps for undertaking a PIA:

1. Threshold assessment
2. Plan the PIA
3. Describe the project
4. Identify and consult with stakeholders
5. Map information flows
6. Privacy impact analysis and compliance check
7. Privacy management—addressing risks
8. Recommendations
9. Report
10. Respond and review.

Applicants are required to conduct a PIA and provide a report to the ACMA in the form set out at Part 3 of the application.

Applicants are strongly encouraged to read the Office of the Australian Information Commissioner’s [*Guide to privacy impact assessments*](https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments)for guidance on preparing the PIA.