



Bureau of Meteorology Privacy Policy

<i>File Reference:</i>	55/2958
<i>Document Name:</i>	Bureau of Meteorology Privacy Policy
<i>Document Version:</i>	1.0
<i>Document Date:</i>	07 March 2014
<i>Document Status:</i>	Approved
<i>Security Classification</i>	UNCLASSIFIED
<i>Approval</i>	Dr Rob Vertessy, Director of Meteorology and CEO
<i>Document owner:</i>	FOI & Privacy Coordinator
<i>Contact:</i>	For any questions, queries or comments about this policy, please contact the FOI & Privacy Coordinator at: privacy@bom.gov.au

Contents

Overview	4
How do we collect and hold personal information?	4
Purposes of collection.....	4
Types of personal information we may collect and hold	5
How we collect personal information	5
Privacy collection notices.....	6
Website visit data and cookies	6
How do we use and disclose personal information?.....	7
Primary and secondary purposes	7
Disclosure of personal information to third parties.....	7
Will we disclose your personal information overseas?	8
Storage and security of personal information.....	8
How we store and secure personal information.....	8
Retention and disposal of personal information.....	9
Your privacy rights.....	9
Can you deal with us anonymously or pseudonymously?	9
How can you access and / or correct your personal information?	9
Requests by current and former staff members for personnel records.....	10
How do you make a complaint about our privacy practices?.....	10
Internal roles and responsibilities	11
Everyone working for the Bureau	11
Senior Management	11
FOI & Privacy Coordinator	11
Agency Security Personnel.....	11
Branch /Section / Regional Managers	12

Further information	12
Review and revision.....	12
Endorsement	12
Key definitions	13
Personal Information.....	13
Sensitive Information	13
Consent	13
Use	14
Disclosure	14
Permitted General Situation.....	14

Bureau of Meteorology Privacy Policy

Overview

The Bureau of Meteorology (the Bureau) recognises the importance of protecting the privacy of individuals. We respect your rights to privacy under the [Privacy Act 1988](#) and the [Australian Privacy Principles \(APPs\)](#), and will comply with the requirements of this legislation.

This privacy policy describes how the Bureau manages and protects [personal information](#), including [sensitive information](#). This policy is a key component of the Bureau's Data and Information Management Framework.

Detailed information on privacy and the APPs is available on the website of the Office of the Australian Information Commissioner (OAIC) at: www.oaic.gov.au.

This privacy policy was last updated on 07 March 2014.

How do we collect and hold personal information?

Purposes of collection

The Bureau's mission is to provide Australians with the information needed to live safely and sustainably within our natural environment. This encompasses information about the atmosphere, oceans, water and land.

Our core functions and activities as set out in the *Meteorology Act 1955* and *Water Act 2007* include:

- taking and recording of meteorological, water and other environmental observations and information;
- providing weather forecasts and warnings and long-term outlooks to the general public, emergency services, and key industry sectors including agriculture, marine, civil aviation and defence;
- maintaining and publishing Australia's National Water Accounts; and
- researching, reporting and advising Government on meteorological, climate and water matters.

We also perform a range of administrative functions common to all Australian Government agencies, including financial management, personnel management, property management, and Work, Health and Safety (WH&S).

In performing and administering these functions and activities, we may need to collect some personal information about identifiable individuals, including (in limited circumstances), sensitive information.

All collection of personal information will be reasonably necessary for, or directly related to one or more of our functions and activities.

Types of personal information we may collect and hold

The Bureau's main holdings of personal and sensitive information relate to the recruitment, training and management of our employees, and other individuals who undertake work or services by agreement, including contractors, cooperative observers, visitors and volunteers. We also collect and hold personal information about individuals external to the Bureau who interact with us. The specific types of personal information we may collect and hold will depend on the functions and activities being undertaken, and can include:

- name;
- contact details (e.g. telephone numbers, email address, mailing address etc);
- age, date of birth, and other demographic information;
- profession, occupation or job title;
- financial information (e.g. records of payments made by or to you);
- employment, curriculum vitae and education information;
- photographic identification for staff, contractors, visitors and volunteers with physical access to Bureau sites;
- property information;
- travel information;
- conference registration information (e.g. dietary requirements);
- information about the products and services you have obtained from us, together with any other information necessary to deliver those products and services, and to respond to your enquiries;
- your personal views and opinions about our products and services; and
- any other information you provide to us.

Examples of sensitive information we collect and hold include:

- health information including medical and compensation related information about our employees;
- records relating to character checks and security clearances about our employees; and
- records relating to trade union or professional association membership provided for payroll purposes.

How we collect personal information

Generally, we will collect personal information about you directly when you deal with us by telephone, letter, email, face-to-face contact or through our website (www.bom.gov.au), such as when you:

- write to us, or provide feedback on our services (e.g. via telephone, email, letter, fax or through our website);
- apply for a job at the Bureau;

- enter into agreements with the Bureau (e.g. to be a cooperative observer, or lease property or equipment to us);
- request information from us (e.g. through Climate Data Services or under the *Freedom of Information Act 1982*);
- purchase products online or via commercial services agreements;
- subscribe to updates, bulletins, newsletters and publications; and
- visit our website and social media sites (e.g. Facebook).

We may also collect personal information about you from third parties when:

- you have provided express or implied consent; or
- we are required or authorised to do so by or under an Australian law or a court order; or
- it is unreasonable or impractical to collect the personal information from you.

We may collect sensitive personal information with your express or implied consent when it is necessary for, or directly related to, the performance of our functions or activities. The *Privacy Act 1988* also allows the collection of sensitive information in certain other exceptional circumstances, including where a [permitted general situation](#) exists.

Privacy collection notices

At or before the time we collect your personal information (or as soon as practical afterwards), we will take such steps as are reasonable in the circumstances to provide you with a privacy notice containing the following information:

- the facts and circumstances of the collection;
- the purpose for which we have collected the information;
- details of any law or court order that requires or authorises the collection of your personal information;
- the consequences (if any) if the personal information is not collected;
- the details of any other person or entity to whom personal information of the kind collected is usually disclosed;
- any likely cross-border disclosures; and
- a link to this Privacy Policy, including contact details you can use to request access to or correction of personal information we hold, or to make a complaint.

Website visit data and cookies

We log certain information about your visits to our website for statistical purposes, and to help improve our website, products and services. This includes information about the date and time of your visit, the type of browser you are using, the referring site and your server's IP address.

Some parts of the Bureau's website may use cookies to maintain site information and your setting preferences as you navigate different pages on our web site or when you return to the web site at a later time. Third party cookies are also used for web analytics, and to track how many people have seen a particular advertisement on the website.

You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this, you may not be able to use the full functionality of this web site.

No attempt will be made to identify users or their browsing activities, unless disclosure is required by law or due to a mandatory requirement of a Court, Government Agency or Regulatory Authority in the course of a legally enforced investigation.

For more information about how we collect and manage information collected about your online visits, please see our [website's privacy notice](#).

How do we use and disclose personal information?

Primary and secondary purposes

We will use and disclose your personal information for the particular purpose for which it was collected (the 'primary purpose'). For example, if you register and pay to obtain certain meteorological data from us, we will use your financial information to process your payment and use your nominated email address to issue your login details.

We may also use or disclose your personal information for a secondary purpose related to, or directly related to, the purpose of collection where you would reasonably expect that your information would be used for this other purpose. These secondary purposes may include activities such as market research, promotion of our products and services, public education and quality assurance.

We may also use or disclose your personal information for another purpose permitted by the *Privacy Act* and the APPs, including where:

- you provide express or implied consent; or
- we are required to, or authorised by an Australian law or a court or tribunal order; or
- a [permitted general situation](#) exists as defined in the *Privacy Act*; or
- a permitted health situation exists as defined in the *Privacy Act*; or
- we reasonably believe that the use or disclosure is necessary for enforcement related activities conducted by, or on behalf of, an enforcement body.

Disclosure of personal information to third parties

Examples of third parties we may disclose your personal information to in accordance with the above include:

- contractors and service providers;

- suppliers and other third parties with whom we have commercial relationships for business, marketing and related purposes;
- other relevant government agencies (e.g. ComSuper, Comcover, Australian Public Service Commission, the Department of Finance etc);
- our Minister, Parliamentary Secretary, Portfolio Department, and committees of Parliament;
- law enforcement bodies, agencies and authorities; or
- any organisation for any authorised purpose with your express or implied consent.

Will we disclose your personal information overseas?

In limited circumstances, it may be necessary to disclose your personal information to overseas recipients. For example, where you nominate an overseas referee in support of a job application, or where you are being seconded from, or to, an overseas meteorological agency for employment or training purposes.

Before disclosing personal information overseas, we will either:

- take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (APPs);
- form a reasonable belief that the recipient is bound by an overseas law or binding scheme to treat your personal information substantially the same way as provided for by the APPs; or
- seek your consent after expressly informing you of the potential consequences of providing your consent to the overseas disclosure.

We may also be required to disclose your personal information to an overseas entity by or under an Australian law or court order or if another exception exists under the Privacy Act.

Storage and security of personal information

How we store and secure personal information

Your privacy is important to us. Access to personal information will be on a strictly 'need to know' basis, and we will take reasonable steps to ensure your information is protected from misuse and loss, and from unauthorised access, modification or disclosure.

Personal information which is in hardcopy formats is stored using our physical filing system, while electronic data is stored on agency servers, hard disks and tapes. In some instances, we may store your personal information with contracted third party storage providers.

Physical security measures may include:

- physical access restrictions on Bureau premises;
- application of appropriate protective security markings; and
- storage of sensitive information in secure containers and / or areas.

Electronic media is accessed only by nominated system administrators for the purpose of maintenance and remediation activities. System administrators may be a combination of Bureau personnel or contracted third party providers. Third party providers are contracted to complete tasks as detailed in their agreement with the Bureau.

The Bureau complies with mandatory Government security controls, e.g. Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM) for ICT systems.

Specific electronic security measures may include:

- access controls and passwords on key systems;
- only authorised Bureau staff are permitted remote and physical access to data centres and their devices used by our agency;
- third party providers obtain physical access to agency datacentres and devices only as per contract arrangements;
- security software is installed on all critical agency ICT devices including the corporate desktop provided to general users;
- ICT systems monitor real-time events via a variety of methods including logging processes, running scripts and with intelligent 'self-learning' mechanisms to detect erroneous or malicious activity;
- physical ICT devices installed on our network offer varying degrees of security, e.g. firewalls;
- use of secure online payment systems; and
- encryption of electronic files where government regulations require certain personal data to be provided to other agencies (e.g. Department of Finance).

Retention and disposal of personal information

Records containing personal information will be managed and disposed of in accordance with National Archives of Australia (NAA) requirements.

Your privacy rights

Can you deal with us anonymously or pseudonymously?

Where it is practicable, you may choose to remain anonymous or adopt a pseudonym when dealing with us.

However, in certain situations it is necessary for us to collect your name and other identifying information – e.g. when you apply for a job with us, or request access to your personal information under either the *Privacy Act* or *Freedom of Information Act*.

How can you access and / or correct your personal information?

You have a right to request access to personal information we hold about you, and to request its correction.

If you wish to obtain access to, or seek correction of, your personal information you are encouraged to contact the FOI & Privacy Coordinator in the first instance to informally discuss your needs, and the options that may be available:

- Telephone: (03) 9616 8428
- Email: privacy@bom.gov.au
- Mail: FOI & Privacy Coordinator
Bureau of Meteorology
People Management Branch
GPO Box 1289
MELBOURNE VIC 3001

If you choose to make a formal request under the *Privacy Act*, you should specify the type/s of information you are seeking to access or correct, and provide your contact details including an email address or mailing address.

You will not be charged for lodging a request to access or correct your personal information.

Before providing access to or correcting your personal information, we may require you to verify your identity.

We will respond to requests for access and correction under the *Privacy Act* within 30 days. If access or correction is refused, we will provide you with a written notice setting out the reasons for the refusal, and provide information about how you can make a complaint, if you wish to do so.

If your correction application is refused, we will take reasonable steps to associate a statement with your personal information which provides that you believe that your personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

You may also request access to and seek correction of personal information under the *Freedom of Information Act 1982* (FOI). For further information, see: <http://www.bom.gov.au/foi/>

Requests by current and former staff members for personnel records

Current and former staff seeking access to their personnel records should contact People Services in the first instance, as it may be possible to make the information available to you under administrative arrangements outside of the *Privacy Act*.

People Services can be contacted via email: personnel_help@bom.gov.au

If you are not satisfied with the response from People Services, you may still request access to the information under either the *Privacy Act* or *FOI Act*.

How do you make a complaint about our privacy practices?

If you wish to make a complaint about our privacy practices, you should submit a written complaint to the FOI & Privacy Coordinator using the contact details set out in this policy. We will respond to your complaint within 30 days.

If you are not satisfied with our response, you may make a written complaint to the Privacy Commissioner setting out the details of the practices which you think interfere with your privacy. The Privacy Commissioner will generally expect you to complain to the Bureau first, and will likely refer your complaint to the Bureau if you have not done so already.

For more information about the Privacy Commissioner, you can visit the Office of the Australian Information Commissioner's website (www.oaic.gov.au) or telephone 1300 363 992 (local call charge).

Internal roles and responsibilities

Everyone doing work for the Bureau

Everyone doing work for the Bureau has a responsibility to ensure that they comply with the requirements of the *Privacy Act*, the APPs, this privacy policy and relevant local procedures and guidelines when collecting, storing, using or disclosing personal information.

This includes the Bureau's employees, contractors, consultants, visitors and volunteers.

To support this responsibility, the Bureau will continue to issue enterprise-wide advice, guidance and training on key privacy related issues.

Senior Management

The Assistant Director, People Management (ADM) is the Senior Executive Service officer within Corporate Services Division responsible for the Bureau's enterprise privacy framework, including this policy. ADM is also the Bureau's Chief Information Security Officer (CISO).

Recommendations and reporting to the Bureau's Executive on key privacy related matters and initiatives will be through the Deputy Director Corporate (DDC) and the Deputy Director Information Systems and Services (DDI), who is also the Bureau's Chief Information Officer (CIO).

FOI & Privacy Coordinator

Ongoing management and further development of the enterprise privacy framework will be managed by the FOI & Privacy Coordinator, who is also responsible for providing guidance, advice and training on specific privacy matters; and handling personal information requests and complaints under the *Privacy Act*.

Agency Security Personnel

The Bureau's Agency Security Advisor (ASA) and Information Technology Security Advisor (ITSA) will provide protective security advice associated with privacy matters, including recommendations about appropriate physical and electronic storage and systems controls.

Branch /Section / Regional Managers

Branch, section and regional managers are responsible for ensuring that reasonable steps have been taken to comply with the Privacy Act and APPs in relation to personal information which their business units collect, store, use or disclose. This includes incorporating privacy considerations (as appropriate) into their local policies, procedures and systems, and local implementation of enterprise-wide advice and guidance issued by the FOI & Privacy Coordinator, Agency Security Personnel and other relevant staff.

Branch, section and regional compliance may be subject to periodic or ad-hoc compliance monitoring.

Further information

To find out more about how we manage personal information you can contact:

FOI & Privacy Coordinator
Bureau of Meteorology

People Management Branch
GPO Box 1289
MELBOURNE VIC 3001
AUSTRALIA

Tel: (03) 9616 8428

Email: privacy@bom.gov.au

Review and revision

From time to time, we will review and revise this Privacy Policy. We reserve the right to amend this policy at any time and any amendments will be notified by posting an updated version on our website at: www.bom.gov.au

Endorsement

This policy has been endorsed by the Director of Meteorology.

Dr Rob Vertessy

Director of Meteorology and CEO

07 March 2014

Key definitions

Personal Information

Personal information is defined by Section 6(1) of the *Privacy Act 1988* as any information or opinion about an identified individual, or an individual who is reasonably identifiable:

- Whether the information or opinion is true or not, and
- Whether the information or opinion is recorded in a material form or not.

In general terms, personal information is any information that identifies you, or could be used to reasonably ascertain your identity.

Sensitive Information

Sensitive information is specifically identified by the *Privacy Act 1988* as a subset of personal information, including information about your:

- racial and ethnic origins;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices;
- criminal record; and
- health information.

Under the Australian Privacy Principles (APPs), sensitive information is generally afforded a higher level of privacy protection than other personal information.

Consent

Consent can be expressed by the individual, or implied. The four key elements of consent are:

- The individual is adequately informed before giving consent
- The individual gives consent voluntarily
- The consent is current and specific; and
- The individual has the capacity to understand and communicate their consent.

Use

Generally, the Bureau uses personal information when we handle and manage that information within the Bureau, or otherwise retain effective control over it (e.g. when personal information is stored on a third party server with appropriate contractual privacy protections in place).

Disclosure

The Bureau discloses personal information when it is made accessible to others outside the Bureau, and the information is released from the Bureau's effective control.

Permitted General Situation

The information handling requirements imposed by some APPs do not apply if a 'permitted general situation' exists.

The *Privacy Act* s16A specifies a number of permitted general situations, including when collection, use or disclosure is necessary or reasonably necessary for:

- lessening or preventing a serious threat to life, health or safety;
- taking appropriate action in relation to suspected unlawful activity or serious misconduct (e.g. investigating a suspected serious breach of the Australian Public Service Code of Conduct);
- locating a person reported as missing;
- establishing, exercising or defending a legal or equitable claim; or
- a confidential alternative dispute resolution process.