Australian Government
Bureau of Meteorology

Document type	Policy
Category	Privacy
Approved by	Executive Team
Date Approved	16 September 2019
Responsible officer	General Manager, Legal and Commercial
Sponsor	Group Executive, Corporate Services
Review date	16 September 2021

Privacy

Purpose

The Bureau has specific responsibilities under the Privacy Act 1988 (Cth) including adhering to the Data Breach Notification Scheme and the Australian Government Agencies Privacy Code, which include requirements for a clear and up to date privacy policy.

Scope

All Bureau staff, including ongoing and non-ongoing employees, students, volunteers, contractors and consultants engaged by the Bureau, must comply with this policy. We collect and hold *personal information* about individuals external to the Bureau who interact with us.

Policy

This policy informs Bureau staff how information obtained will be *used*, stored and *disclosed*.

Terms in *italics* in this policy have the meanings as set out in the Definitions section at the end of this policy.

1. About this policy

This policy will identify:

- The type of *personal information* that will be collected, stored, *used*, and *disclosed* by the Bureau
- When and how this *personal information* will be collected, *used*, stored, and *disclosed* by the Bureau
- Why *personal information* will be collected, *used*, stored and *disclosed*
- The process for how individuals can access their own *personal information*
- The process for how individuals can request the Bureau update and correct *personal information* that is held about them
- The process for making complaints to the Bureau relating to the collection, *use*, storage and *disclosure* of *personal* and *sensitive information*

2. Collection of *personal information*

2.1 Purposes of collection

The Bureau's mission is to provide trusted, reliable and responsive weather, water, climate and ocean services for Australia – all day, every day.
Our core functions and activities are set out in the Meteorology Act 1955 (Cth) and Water Act 2007 (Cth) and include:

- Collecting and recording meteorological, water and other environmental observations;
- Providing weather forecasts, warnings and long-term outlooks to the general public, emergency services, and key industry sectors;
- 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 workplace health and safety functions. We may need to collect *personal information* about identifiable individuals, including (in limited circumstances) *sensitive information*, in order to perform and administer our functions.

2.2 Type of *personal information* we may collect and hold

Most of the Bureau's collection of *personal information* involves individuals who undertake work for or on behalf of the Bureau. However, 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
- Our employees' records relating to character checks and security clearances;
- Records relating to trade union or professional association membership provided for payroll purposes.

2.3 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), social media platforms and the Bureau of Meteorology app or 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);
- Complete surveys relating to our products or services
- 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, twitter, Instagram and the Bureau of Meteorology app).

We may decrypt personal information in line with this policy.
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 information* from you with your express or implied *consent* and when it is reasonably 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.

2.4 Privacy collection notices

At or before the time we collect your *personal information*, we will take reasonable steps to provide you with a privacy collection notice containing the following information:

- The purpose for the collection of the information;
- Details of any law or court order that requires or authorises the collection of the *personal information*;
- The consequences (if any) if the *personal information* is not collected;
- The details of any third party that may receive the *personal information*
- Any likely cross-border *disclosures*; and
- Details on how to access this Privacy Policy

2.5 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, operating system of your device, pages accessed, the referring site and your device'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 the website.

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.

2.6 Social media

We use social media platforms including Facebook, Instagram, Twitter, YouTube, and LinkedIn. We use these sites to inform and engage the public about weather warnings, events and services conducted by us.

When you interact with us on these platforms, you are agreeing to the terms of service of these platforms. For more information about the privacy practices of these platforms you can read their privacy policies.

When you communicate with us using these social media platforms, we use an archiving and engagement services to manage content and comments across the social media platforms. This is to ensure that comments or complaints are attended to, and that comments are moderated under our community participation rules, so that our social media pages are a fair and accessible place for everyone. We may collect names or other personal information of individuals who have been banned from accessing our social media platforms to ensure they do not attempt to reengage with us in an antisocial matter on these platforms.

2.7 Publishing public photos on our platforms

We welcome contributions by the public on our social media platforms. Before you ask us to publish any photographic content on our social media platform, keep in mind that:

- We must obtain *consent* from the individual who took the photo;
- We must obtain *consent* from any individuals who are in the photo.

Before we agree to publish any photos, we will ask you for permission to republish on our social media accounts.

2.8 The Bureau of Meteorology App

If you install and use the Bureau of Meteorology's apps, some information about your device (e.g model, operating system) and how you are using Bureau's app will be collected via web analytics. If you choose to provide feedback to us from within the app, we may ask for details such as your email address and type of device.

3. How do we *use* and *disclose personal information*?

3.1 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 for meteorological data, we will use your financial information to process your payment and use your nominated email address to issue your login details. The Bureau reserves the right to decrypt data (including data that may be personally identifiable) for work purposes. This information may also be used for another purpose related to the purposes of information *disclosure*. 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 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

3.2 *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 – for example the service providers we use to manage content on our social media platforms;
- other relevant government agencies (e.g. ComSuper, Comcover, Australian Public Service Commission, the Department of Finance);
- 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.

3.3 Will we *disclose* your *personal information* overseas?

In limited circumstances, it may be necessary to *disclose* your *personal information* to overseas recipients. For example, if you nominate an overseas referee in support of a job application, or if we use a service provider that stores data overseas. Before *disclosing personal information* overseas, we will either:

- Take reasonable steps to ensure the overseas recipient does not breach the Australian Privacy

Principles (APPs);

- Form a belief that the recipient is bound by an overseas law to treat your personal information in a way that is substantially similar to the Privacy Act; or
- seek your *consent* after expressly informing you of the potential consequences of providing your *consent* to the overseas *disclosure*.

We may also *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.

3.4 *Disclosure* and the Notifiable Data Breach Scheme

Under the Notifiable Data Breach Scheme, the Bureau has an obligation to report to the OAIC any data breaches likely to cause serious harm to individuals whose *personal information* has been involved in the data breach. In the event of a such a data breach, the OAIC requests a report on the number of individuals affected by the breach. The OAIC does not ask for the personal details of the individuals affected and the Bureau will not *disclose* this information. If you are affected by data breach likely to cause serious harm to you, you will be notified of this in writing with any suggested mediations and steps that you would need to take as a result.

4. Storage and security of *personal information*

4.1 How we store and secure *personal information*

Access to *personal information* is on a strictly 'need to know' basis, and we take reasonable steps to ensure information is protected from misuse, loss, unauthorised access, modification or *disclosure*. *Personal information* which is in hardcopy formats is stored using our physical filing system and electronic data is stored on Bureau 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 authorised users for the purpose of maintenance and remediation activities. Authorised users 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 Commonwealth Government security controls, for example, the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM) for ICT systems.

4.2 Retention and disposal of *personal information*

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

5. Your privacy rights

5.1 Dealing with us anonymously or pseudonymously

Under the Privacy Act, you have the right to remain anonymous or use a pseudonym. The Bureau will aim to adhere to this right when possible however, in certain situations it may not be feasible for us to work with you without 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.

5.2 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 Privacy Officer in the first instance to informally discuss your needs, and the options that may be available, using the contact details set out in section 6.

If you choose to make a formal request under the Privacy Act, you should specify:

- The type/of information you are seeking to access or correct,
- 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*.

5.3 Verifying your identity

Before providing access to or correcting your *personal information*, we may require you to verify your identity. To verify your identity, we may either ask for a certified copy of photo identification, such as a driver's license or a passport.

5.4 Response timeframe

We will respond to requests for access and correction under the Privacy Act within 30 days.

5.5 What if the request is refused?

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. For further information, see: Freedom of Information

5.6 Making 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 Bureau's Privacy Officer using the contact details set out in section 6. 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).

5.7 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.

6. Bureau Internal roles and responsibilities

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.

To find out more about how we manage *personal information* you can contact:
Privacy Officer
Bureau of Meteorology
Corporate Services, Legal and Commercial Program
MELBOURNE VIC 3001
AUSTRALIA
Tel: (03) 9616 9000
Email: privacy@bom.gov.au

7. 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.

Endorsement

This policy has been endorsed by the Director of Meteorology.
Dr Andrew Johnson
Chief executive Officer and Director of Meteorology

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

Related requirements

Supersedes	Bureau of Meteorology Privacy Policy 55/2958
Legislation	Privacy Act 1988 Australian Government Agencies Privacy Code Archives Act 1983 Freedom of Information Act 1982
Government policies	Notifiable Data Breaches Scheme
Standards	
Bureau policies	
Bureau procedures	Privacy Data Breach Response Plan
Bureau processes	