



## PUBLIC SECTOR INFORMATION SHEET 3 – *Portable storage devices and personal information handling*

### Key Messages

This information sheet suggests a number of steps Australian and ACT Government agencies should consider taking to help safeguard personal information stored or handled on portable storage devices.

#### What is a portable storage device?

A portable storage device ('PSD') is defined in this information sheet as a small, lightweight, portable, easy to use device, which is capable of storing and transferring large volumes of data. Common PSDs include portable external hard drives, CDs/DVDs, USB keys, laptops/ notebooks, personal digital assistants (such as Pocket PC, Palm, BlackBerry), and devices with in-built accessible storage (such as MP3 players, iPods, and mobile phones).

#### What privacy risks are presented by PSDs?

According to a survey on PSD use conducted on behalf of the Office of the Privacy Commissioner in 2009, PSDs are widely used across Australian Government agencies.

The use of PSDs to handle personal information raises a number of privacy risks related to personal information storage and security. These include that personal information stored on a PSD may be compromised through the operation of malicious software or the PSD may be lost or stolen. Such risks arise from the technical capabilities of PSDs (high storage, fast speed of transfer and 'plug and play' functionality) along with their physical characteristics (small size, light weight, low cost, high portability).

The steps suggested in this information sheet may assist agencies to better manage personal information held by an agency that may be stored or handled on a PSD. These steps may also help agencies covered by the *Privacy Act 1988* to meet their obligations under Information Privacy Principle 4(a).

#### What can agencies do to enhance the security of personal information on PSDs?

Key steps which Australian and ACT Government agencies may consider taking include:

1. Undertake regular risk assessments of PSDs used in the work environment.
2. Ensure the agency has documented policies that apply to PSDs used in the work environment.
3. Promote active staff awareness, including through formal staff training, about these policies and other procedures applying to PSDs.
4. Install appropriate software controls.
5. Develop and implement an effective and timely response procedure for security breaches.

Agencies should also consider addressing in their policies and practices, the specific risks associated with any use of privately owned PSDs in the work environment and any use of PSDs when working remotely.

## Background

### Who is this information sheet for?

This information sheet has been developed for Australian and ACT Government agencies, where agency staff use portable storage devices ('PSDs') to store or handle personal information<sup>1</sup>.

### What is a PSD?

A PSD is defined in this information sheet as a small, lightweight, portable, easy to use device, which is capable of storing and transferring large volumes of data. Common PSDs include portable external hard drives, CDs/DVDs, USB keys<sup>2</sup>, laptops/ notebooks, personal digital assistants (such as Pocket PC, Palm, BlackBerry), and devices with in-built accessible storage (such as MP3 players, iPods, and mobile phones).

### What is this information sheet about?

A survey on PSD use in Australian Government agencies conducted on behalf of the Office of the Privacy Commissioner in 2009 shows that PSDs are widely used across Australian Government agencies<sup>3</sup>.

This information sheet aims to assist Australian and ACT government agencies to minimise the privacy risks associated with storing and handling personal information on PSDs. These include that personal information handled on a PSD may be compromised through the operation of malicious software or the PSD may be lost or stolen.

The information sheet outlines some steps agencies may consider taking in relation to PSDs issued for work purposes, as well as privately owned PSDs used at work.

These steps may help agencies covered by the *Privacy Act 1988* (the 'Privacy Act') to meet their obligations under Information Privacy Principle 4(a) ('IPP4(a)'). IPP4(a) provides that agencies need to ensure that a record in their possession or control containing personal information, is protected by reasonable security safeguards against loss, unauthorised access, use, modification, disclosure or other misuse.

To ensure ongoing compliance with IPP4(a), it will be important for agencies to take account of whether particular PSDs offer appropriate security safeguards when reviewing their IT procurement needs.

Agencies should also consult with their IT managers before deciding on particular software, hardware, access and other controls for PSDs used within their agencies.

### How does this information sheet interact with other legislative obligations and standards applying to PSDs?

Agencies also need to comply with any other applicable legislative obligations or standards applying to PSDs. These may include the *Australian Government Protective Security Manual* (the 'PSM') and the *Australian Government Information and Communications Technology Security Manual* ('ISM').

In general terms, the PSM provides minimum security standards that agencies need to meet for the protection of Australian Government resources, including information, personnel and assets<sup>4</sup>. The ISM provides minimum security requirements and guidance to assist in the protection of official government information that is processed, stored or communicated by Australian Government information systems<sup>5</sup>.

This information sheet is not intended to replace the standards in the PSM or the ISM. Instead, it has a different focus – on reasonable security safeguards for protecting personal information stored or handled on PSDs.

---

<sup>1</sup> 'Personal information' is defined in section 6(1) of the Privacy Act as 'information or an opinion, whether true or not, about an individual whose identity is apparent or can be reasonably ascertained from that information'.

<sup>2</sup> A 'USB key' is also known as a 'flash drive', 'USB stick', 'memory stick' or 'memory key'.

<sup>3</sup> See *Portable Storage Devices and Australian Government Agencies: Personal Information Survey 2009*, question 25 ([www.privacy.gov.au](http://www.privacy.gov.au)). The survey was designed by the Office based on a similar survey undertaken by the Office of the Victorian Privacy Commissioner in 2008.

---

<sup>4</sup> For further information on the Australian Government Protective Security Manual, see [www.ag.gov.au/](http://www.ag.gov.au/)

<sup>5</sup> For further information on Australian Government Information and Communications Technology Security Manual (designated ACSI 33), see [www.dsd.gov.au/library/infosec/ism.html](http://www.dsd.gov.au/library/infosec/ism.html).

## How can agencies enhance the security of personal information on PSDs?

The Office of the Privacy Commissioner (the 'Office') has identified five interrelated steps, which may help agencies to enhance the security of personal information stored or handled on PSDs:

1. Risk assessment
2. Documented policies
3. Active staff awareness
4. Appropriate software controls
5. Effective response to security breaches

### Step one – risk assessment

Agencies are encouraged to regularly assess the privacy risks associated with using PSDs to handle personal information in their workplace.

This risk assessment should have three main purposes. Firstly, it should identify the risks of using PSDs across an agency's different activities or operations. Secondly, it should allow an agency to evaluate the likelihood and the consequences of these risks occurring. Finally, it should help agencies to put in place safeguards, tailored to the agency's activities or operations, to manage the privacy risks associated with using PSDs.

The risks arising from using PSDs may differ within agencies, depending on the circumstances. Different parts of an agency may therefore need to put in place different safeguards to address the identified risks.

In assessing these risks, an agency may wish to consider the following factors, which are illustrated by examples. These factors are provided as a general guide, and are not exhaustive.

- **What kind of personal information is usually stored or handled on PSDs?**  
Some information is more likely to cause significant harm to an individual if it is compromised than other types of information, whether that harm is physical, financial or psychological.

For example, if a PSD storing individuals' names and bank account details is stolen, this may pose a greater risk of harm than if the PSD stored an individual's name and contact details (however, as discussed in the next example, the surrounding context may also be important).

- **Who is likely to be affected by a security breach, where personal information is compromised?**  
Depending on the context, certain people may be particularly at risk of harm should even their contact details be compromised.

For example, a breach of a child protection database containing name and contact details of a child's carer, may expose a child (and their carer) to a violent family member.

- **What types of PSDs are used to handle personal information in the agency?**  
Certain PSDs, due to their functionality, level of security protections and storage capacity, may be more likely to cause an individual harm if they are lost, stolen or otherwise accessed by an unauthorised person.

For example, if access to a laptop is protected by a strong password (a password which includes a combination of letters and numbers, and is changed regularly) it may be difficult for an unauthorised person to misuse personal information stored on it. However, if a USB key cannot be password protected, it may be easier for an unauthorised person to access and misuse any personal information stored on that PSD.

- **How often are PSDs used in the agency?**  
Where an agency regularly uses PSDs, this may increase the likelihood those PSDs will be lost, stolen or misused, and information on those PSDs will be compromised.

For example, staff working in a large agency, with offices spread out across Australia, may need to regularly use PSDs to handle personal information as part of their day-to-day activities. This may increase the likelihood that a PSD will be lost.

- **Does the agency prohibit staff from using privately owned PSDs at work?**

If an agency does not prohibit staff from using privately owned PSDs at work, this may increase the likelihood personal information from agency records will be uploaded on to privately owned PSDs and will be accessed by unauthorised users or misused.

Privately owned PSDs may also introduce viruses or other malware onto the agency's network, increasing the risk that the agency's IT network (and personal information stored on it) will be compromised.

- **What software and hardware controls does the agency apply to PSDs?**

'Software controls' involve installing specific control software, firewalls, system policies, or operating system controls. 'Hardware controls' may include physically disconnecting, removing or sealing off access ports, or using non-standard locking ports.

Having in place appropriate software and hardware controls may make it less likely for personal information on PSDs to be compromised.

- **How effective are current PSD controls?**

The effectiveness of current PSD controls may be assessed by maintaining and reviewing records of any security breaches.

- **Can the agency track PSD use?**

If an agency keeps a register of all PSDs permitted to be used at work (including privately owned PSDs), and undertakes regular stocktakes of that register, this could help it to quickly and accurately track how many PSDs are being used, what types of PSDs these are, who is using them and any missing PSDs.

This may also assist an agency's investigations in relation to a lost PSD. For example, once a staff member reports a PSD missing, the agency could check the register to identify the PSD and if IT facilities are available, disable access to that PSD.

## Step two – documented policies

All Australian Government agencies surveyed in the Office's survey on PSD use indicated that they provide access to or issue PSDs to staff<sup>6</sup>. However, not all of these agencies have specific policies in place that apply to PSDs and many of these policies do not cover all types of PSDs<sup>7</sup>.

A documented policy that sets out how staff may use PSDs at work can address some of the risks associated with PSDs that have been identified in the risk assessment.

Some of the key factors for agencies to consider when assessing whether their policy appropriately safeguards personal information stored or handled on a PSD are listed below. These factors are not in order of importance, nor are they exhaustive. Agencies should consider all the factors together before deciding what their policy needs to cover to address their own particular risks.

- **Application** – Applies to all staff members including, where applicable, contractors, consultants, interns, volunteers etc.
- **Flexibility** – Covers all the various PSDs used within the agency. It is also flexible enough to apply to new types of PSDs, with increased speed, capacity and functionality.
- **Minimal personal information** – Explains that staff should load or store the minimum amount of personal information possible on their PSD to complete any given task.
- **Privately owned PSDs** – Describes whether staff may use privately owned PSDs in the workplace to handle personal information, and if so, what types are acceptable and any limitations on their use.
- **Personal use** – Specifies if, and in what circumstances, agency issued PSDs may be used for personal use.

---

<sup>6</sup> See *Portable Storage Devices and Australian Government Agencies: Personal Information Survey 2009*, question 25 ([www.privacy.gov.au](http://www.privacy.gov.au)).

<sup>7</sup> See *Portable Storage Devices and Australian Government Agencies: Personal Information Survey 2009*, question 27 ([www.privacy.gov.au](http://www.privacy.gov.au)).

- **Transfer personal information** – Explains that staff need to transfer personal information from PSDs to the workplace network as soon as possible, and delete any trace of that information from the PSD.
- **Delete personal information** – Explains that staff need to delete personal information from the PSD using a strong digital wipe utility as soon as it is no longer needed.
- **Sharing PSDs** – Explains whether and in what circumstances staff may share PSDs storing personal information externally or with other staff members, and the security safeguards that should be in place such as software controls, before doing so.
- **Personal responsibility** – Provides that staff members are responsible for PSDs in their care. Such responsibility could involve locking PSDs in a briefcase, laptop case or other secure container when not in use and ensuring that any specified access controls are in place.
- **Obsolete or damaged PSDs** – Provides a secure process for disposing of outdated or damaged PSDs which ensures that any personal information remaining on the PSD is not accessible.
- **Lost or stolen PSDs** – Explains that staff need to report all lost or stolen PSDs that may store personal information, to a designated Management and IT position, as soon as practicable after a staff member notices the PSD is missing.
- **Breach** – Provides sanctions for breaching the policy.

For the policy to be effective, staff should be familiar with its terms. It is also important for agencies to actively audit compliance with the policy and to take appropriate disciplinary action in the event of a breach.

**Example: Ensuring a policy covers all types of PSDs used in the workplace.**

An agency has an IT security policy that applies to USB keys and CDs/ DVDs.

Many staff within the agency no longer store information on USB keys or CDs/ DVDs, but use personal digital assistants (such as Pocket PC, Palm, BlackBerry) to handle such information, due to the increased functionality of these PSDs. The agency's policy does not apply to personal digital assistants. As such, the policy does not address any risks specific to these PSDs which may include risks arising from synchronization capabilities and, in some cases, Bluetooth wireless connectivity.

The agency's policy has not kept pace with developments in IT use. The agency should have undertaken regular reviews of the types of PSDs being used in the workplace, and assessed whether its policy adequately addressed any additional risks associated with using these PSDs.

**Step three – active staff awareness**

Staff need to be aware of the terms of any applicable policies, practices or procedures applying to PSDs to be able to comply with them.

The Office's survey on PSD use indicated that most Australian Government agencies provide training for staff on the use of agency issued PSDs in the form of on-the-job training<sup>8</sup>.

This could be supplemented with formal training sessions to ensure a consistent message is conveyed to staff members about the policies, practices and procedures applying to PSDs.

Where possible, an initial training session should occur before issuing staff with a PSD (or where permitted before staff may use privately owned PSDs in the workplace) and at regular intervals afterwards.

<sup>8</sup> See *Portable Storage Devices and Australian Government Agencies: Personal Information Survey 2009*, questions 35 – 36 ([www.privacy.gov.au](http://www.privacy.gov.au)).

Some of the relevant issues to discuss with staff at PSD training sessions are outlined below.

- **Risks** – Outline the inherent privacy risks associated with using PSDs to handle personal information.
- **Policy** – Provide staff with a hard copy of the policy, and show them where to find it electronically. Also, highlight key parts of the policy applying to staff, including personal responsibility, acceptable use and what to do when a PSD is lost or stolen.
- **Software and hardware controls** – Describe any applicable software controls applying to the use of agency issued or privately owned PSDs, or hardware controls affecting privately owned PSDs.
- **Contacts** – Provide staff with a list of contacts in the IT or Personnel areas, who can assist staff with any issues associated with PSDs.

One way to confirm that staff understand the messages conveyed in the training session is to ask them to sign an 'Acceptable Use Agreement' at the end of the session. The Agreement should confirm that staff understand and consent to the responsibilities and obligations outlined in the training.

In addition, agencies should have ongoing activities to promote up-to-date staff awareness. This could include reminding staff during staff meetings, by email or in a staff bulletin of their obligations under the policy, referring to any limitations on PSD use in a computer logon banner, and reminding staff of where they can review the policy.

**Example: Facilitating staff awareness about applicable policies.**

Paul works in the Sydney office of a large agency, with many offices across Australia. The agency's information security policy expressly prohibits sending a USB key in the mail. The policy is available on the agency's intranet, but staff generally don't know what it says.

The agency keeps a record of individuals' names, addresses and tax file numbers on a database which can only be accessed from the Sydney office's network. One day, Lillianna, who works in the agency's Melbourne office, asks Paul to send her a copy of some of that information.

As Paul is not aware of the policy, he downloads the relevant information onto a USB key and sends it to Lillianna by post. Two weeks later Lillianna rings Paul to say the USB key has not arrived.

Paul realises that in this period, personal information on the USB key could have been accessed and mishandled by an unauthorised user. If Paul and other agency staff had been given training and regular reminders about the policy, this may have been averted.

**Step four – appropriate software controls**

'Software controls' involve installing specific control software, firewalls, system policies, or operating system controls. They can act as an important safeguard against loss, unauthorised access, use, modification, disclosure or other misuse of personal information.

Set out below are a number of software controls agencies may consider adopting to enhance the security of personal information stored or handled on PSDs. In determining whether these software controls are suitable for a particular agency consideration should be given to the operating requirements of the agency's IT platform, the functionality of the particular PSD and the agency's risk assessment.

- **Encryption** – Encryption is the process of systematically encoding data before transmission and during storage, so that an unauthorised party cannot easily decipher the data.

Where an agency identifies a significant risk that personal information stored or handled on a PSD may be compromised, it may address this risk by requiring that all personal information on a PSD should be encrypted.

In some cases software may not be available to encrypt information on a particular type of PSD, or may compromise the functionality of certain PSDs. The security limitations of particular PSDs should be taken into account when an agency is assessing its procurement needs.

- **Access Controls** – Agencies should consider ensuring that all PSDs have appropriate access controls.

Commonly used access controls which may limit unauthorised access to information stored or handled on a PSD include power on, screensaver and account passwords. Ideally, passwords should include a combination of letters and numbers, and should be changed regularly.

Where personal information is routinely handled on PSDs or the consequences of its compromise are significant, agencies may wish to adopt stronger access controls, including for example, denying access to the device after three failed login attempts.

- **Digital wipe software** – Another way to reduce the risk of personal information being accessed when a device is lost or stolen is to ensure such information is completely deleted from a PSD as soon as it is transferred to the agency's IT network and no longer needed on the PSD.

Generally, when files containing personal information are simply deleted from a PSD, data still resides elsewhere on the device. Digital wipe software can be used to delete personal information from a PSD more thoroughly. This software erases information stored on PSDs by overwriting it multiple times.

- **Malware Protection** – Malware (or malicious software) can wipe out large amounts of information including personal and sensitive information on a PSD, and destroy the PSD's functionality, without the user knowing. There are a number of types of malware, including viruses, worms, Trojans, keystroke loggers and spyware, which can compromise information handled on PSDs in different ways.

Where the device permits, agencies are encouraged to install anti-malware software on all PSDs used to handle personal information to minimise the risk that this information will be compromised. This software is designed to detect and protect a device from malicious software.

- **Tracking the use of PSDs** – Agencies may also wish to consider installing software that monitors how PSDs are used. This could help agencies to track data transfers onto PSDs, for example, where a significant quantity of data is unexpectedly transferred onto a PSD.

### Step five – effective response to security breaches

There are many different ways in which personal information stored on a PSD may be compromised. For example, malicious software may be installed on a staff member's laptop, a mobile phone may be mislaid at the airport, or a staff member's USB key may be stolen.

Agencies should therefore ensure they have policies and procedures applying to all PSDs used in the workplace that outline what to do in the event of a security breach.

Agencies may wish to review the Office's advisory *Guide to Handling Personal Information Security Breaches* (available on the Office's website). This provides general guidance on key steps and factors to consider when responding to a personal information security breach.

## What privacy considerations apply to using privately owned PSDs at work?

In this information sheet, a 'privately owned PSD' is any PSD used by a staff member which has not been issued (or to which access has not been provided) by their agency.

According to the Office's survey on PSD use, most Australian Government agencies do not prohibit staff from using any type of privately owned PSDs at work, or only prohibit the use of some privately owned PSDs (mainly privately owned laptops and notebooks)<sup>9</sup>. Further, almost half of Australian Government agencies surveyed do not have specific policies in place to govern the use of privately owned PSDs at work<sup>10</sup>.

A number of risks could arise from allowing staff to do this.

For example, a staff member could upload personal information stored on the agency's IT network, onto a privately owned PSD. Once uploaded, it would be difficult for the agency to track how this information is used and disclosed. The information could be shared with unauthorised users or if it is downloaded onto another computer, accessed by non-agency staff such as the individual's house mates.

Also, a privately owned PSD could introduce malware onto the agency's network, compromising its IT system.

### Example: Compromising the network.

Ping works at an agency which holds a large number of clients' banking details on its network. On her way to work, she is handed a brand new USB key at the train station as part of a promotion.

At work, Ping plugs the USB key into her laptop and accesses the agency's network. Unfortunately she does not know that the USB key has been programmed to communicate information from her agency's network to an external server outside the agency's network.

Once plugged in, the USB key facilitates the transfer of information, including the clients' banking details, to external servers.

Where the likelihood of these risks occurring is high or the consequences would be significant, an agency may need to adopt a strict approach to minimise the risks associated with privately owned PSDs. This may involve prohibiting the use of privately owned PSDs at work, or prohibiting their use to handle personal information.

Alternatively, an agency could consider using hardware controls to prevent PSDs accessing the agency's network, by physically disabling, removing or sealing access ports, or by using non-standard locking ports. In considering this option, agencies should be aware that such measures should only be used where there are significant risks associated with privately owned PSDs, as they may prevent staff from legitimately using agency issued PSDs.

If an agency allows staff to use privately owned PSDs at work, it should explain how it expects them to be used. This should be specifically covered in staff awareness activities (discussed at Step 3).

An agency's policies should also aim to address the privacy risks outlined above. For example, a policy could provide that:

<sup>9</sup> See *Portable Storage Devices and Australian Government Agencies: Personal Information Survey 2009*, questions 66 – 67 ([www.privacy.gov.au](http://www.privacy.gov.au)).

<sup>10</sup> See *Portable Storage Devices and Australian Government Agencies: Personal Information Survey 2009*, question 78 ([www.privacy.gov.au](http://www.privacy.gov.au)).

- **Management approval** – Staff may not use privately owned PSDs at work without prior approval from a designated manager. The PSD may then be added to a register of PSDs used within the agency.
- **Minimum security capabilities** – Privately owned PSDs may only be used at work where they have minimum security capabilities, such as password protection capabilities.
- **Software controls** – Before using a privately owned PSD at work, staff need to install specific software on the device. Where the device permits and where this is compatible with an agency's operating platform, this could include firewalls and anti-virus software.
- **Restrict uploads** – Staff may only upload personal information from the agency's network onto the privately owned PSD for work purposes with prior approval from a designated manager. This information may not be downloaded onto any other non-agency device unless specifically approved by a designated manager.
- **Compartmentalise work and private data** – Any personal information uploaded onto the PSD and stored on that device for work purposes must, where possible, be password protected. Such information should also be saved in a folder or drive separate to other data stored for private use on the PSD.
- **Limit sharing** – Staff should not share privately owned PSDs that are being used for work purposes with individuals who do not work at the agency.
- **Delete personal information** – Staff should delete personal information stored on the privately owned PSD for work purposes using a strong digital wipe utility, as soon as it is no longer needed.
- **Lost or stolen PSDs** – If a privately owned PSD that has been used for work purposes goes missing, this should be reported as soon as practicable after noticing it is missing.

## What privacy considerations apply to working remotely?

'Working remotely' covers a range of situations in which staff undertake their daily work activities away from the office. This may be because of work-related travel, home-based working arrangements (telecommuting), or working from a location other than the office.

In many cases, working remotely will involve using a PSD to handle information for work purposes, whether that PSD is a privately owned PSD or an agency issued PSD.

While it can be convenient for agencies and staff and, due to technological advancements is occurring more frequently, there are also a broad range of privacy risks associated with working remotely. These include:

- **Lost or stolen PSDs** – PSDs that are used to handle or store personal information may be lost or stolen from cars, public transport, airports or hotel rooms.
- **Shoulder surfing** – Personal information that is handled using a PSD may be overseen or overheard in public places.
- **Unauthorised access** – Personal information stored on a PSD may be accessed by family members or friends at home. For example, where a staff member downloads personal information from an agency issued personal digital assistant onto their home computer, and stores that information on the computer's local drive, this information could later be accessed by the staff member's house mate who shares that computer.
- **Unsafe networks** – Staff may access personal information stored on a PSD, by logging into a public or unsecured wireless network. These networks are open and inherently unsafe, as personal information may be accessed by another unauthorised device.
- **Anti-malware software** – Laptops and notebooks that are used to work remotely may have inadequate anti-malware software installed on them. As a result, personal information stored or handled on a PSD could be compromised.

**Example: Risks in storing personal information on a PSD when working remotely.**

Justin, who works for an agency, needs to review a report which refers to an individual's criminal record. He decides to finish this work at home so he uploads the report from the agency's network onto a laptop issued to him by the agency.

On the way home, Justin stops in at the grocery store and, forgetting that he has the laptop with him, leaves it in plain view on the back seat of his car. While he is gone, the laptop is stolen.

There are a number of things Justin could have done to handle this situation better. Firstly, he should have considered whether it was appropriate to store a report containing such sensitive information on his laptop and take it out of the office. Secondly, Justin should have ensured that the report was protected by strong access controls, such as password protection and encryption, when storing it on his laptop. Finally, Justin should have kept the laptop with him at all times, or at least ensured it was secured out of sight such as by locking it in the boot of his car.

The privacy risks related to working remotely can be minimised by developing an appropriate policy that specifically addresses these risks. Some of the key factors which an agency may consider including in a working remotely policy include:

- **Limited storage** – Where possible, personal information should not be stored on PSDs. If this is necessary, only personal information necessary to complete a task should be stored on the PSD. Any such information should be deleted using a strong digital wipe utility, as soon as it is no longer required for the task.
- **Public computers** – Work-related tasks involving personal information should not be conducted on public computers or networks.
- **Access controls** – Staff working remotely should use password protected screensavers, where the device permits.
- **Log off** – Staff need to log off or shut down a PSD when not in use.
- **Personal responsibility** – Staff should keep a PSD that is used to work remotely with them at all times, or, where this is not possible, the PSD should be stored in a locked container.

The agency should also explain to staff who work remotely the privacy risks of doing so, what is expected of staff when working remotely, the terms of any working remotely policy and the terms of any applicable PSD policy.

The privacy risks associated with working remotely may also be reduced by providing staff who work remotely with an agency issued PSD. In this way the agency can more easily standardise the software, access controls and other safeguards on the PSD.

## Further information

For further information, please see the following publications (available on the Office's website):

- *Public Sector Information Sheet- Information Privacy Principles*
- *Plain English Guidelines to Information Privacy Principles 4 – 7*
- *Guide to Handling Personal Information Security Breaches*

## Public Sector Information Sheets

Information sheets are advisory only and are not legally binding. The Information Privacy Principles ('IPPs') in section 14 of the Privacy Act legally bind agencies.

Information sheets are based on the Office of the Privacy Commissioner's understanding of how the Privacy Act works. They provide explanations of some of the terms used in the IPPs and good practice or compliance tips. They are intended to help agencies apply the IPPs in ordinary circumstances. Agencies may need to seek legal advice on the application of the Privacy Act to their particular situation. Nothing in an information sheet limits the Privacy Commissioner's ability to investigate complaints under the Privacy Act or to apply the IPPs in the way that seems most appropriate to the facts of the case being dealt with. Agencies may also wish to consult the Privacy Commissioner's guidelines and other information sheets.

## Office of the Privacy Commissioner

Privacy Enquiries Line **1300 363 992** - local call (calls from mobile and pay phones may incur higher charges)  
TTY 1800 620 241 – no voice calls; Fax + 61 2 9284 9666; GPO Box 5218, Sydney NSW 2001.

Public Sector Information Sheet 3  
Web HTML and PDF published May 2009  
ISBN 978-1-877079-67-2

© Commonwealth of Australia 2009

[www.privacy.gov.au](http://www.privacy.gov.au)