

# Use of Portable Storage Devices



## **A guide to policy development**

Edition 1 – August 2009



Office of the  
Victorian Privacy  
Commissioner

# Contents

1. Introduction .....	1
2. Scope .....	2
3. Technical controls .....	5
4. Policy framework for use of PSDs .....	7
5. Governance .....	11
APPENDIX 1: PSD policy development checklist .....	12
APPENDIX 2: Recommendations from <i>Use of Portable Storage Devices – Privacy Survey</i> .....	14

Copyright © Office of the Victorian Privacy Commissioner, 2009

The material included in this publication is designed to give general guidance only. It should not be relied on as legal advice. The Office of the Victorian Privacy Commissioner (Privacy Victoria) accepts no liability for loss or damage that may be suffered by any person or entity that relies on information in this publication. No liability is accepted for any information or service which may appear in any other format. Copyright is owned or controlled by Privacy Victoria unless otherwise indicated. Copyright in materials from third parties may be owned by others. Permission to reproduce their work should be separately sought.

Privacy Victoria wants people to have easy access to information about privacy. The contents of this publication may be copied and used for non-commercial use. The material should be used fairly and accurately and this publication acknowledged as the source. The authors of material, where known, should be credited, consistent with the moral rights provisions of copyright law.

COVER PHOTO: [www.istockphoto.com](http://www.istockphoto.com)

# 1. Introduction

Portable Storage Devices (PSDs) can be extremely useful in the workplace. Their functionality and relatively low cost means that their use is proliferating. But the very nature of PSDs presents significant problems for organisations, especially in relation to data security. They can store whole databases but they are small – so they can easily be lost. Worse, they may be unrecognisable as a PSD that can be brought into the workplace and used to store corporate data. Recently, an advertisement for a well-known brand of sunglasses announced the imminent arrival of glasses that would feature a detachable arm containing a 4GB USB key. This illustrates the difficulty of controlling the use of PSDs.

The use of PSDs must be addressed because failure to do so can – and almost certainly will – result in a breach of one or more of the 10 Information Privacy Principles (IPPs) which the Victorian public sector must comply with under the *Information Privacy Act 2000* (Vic). Although IPP 4 (Data Security) is an obvious principle relevant to the use of PSDs, others need to be considered such as IPP2 (Use and Disclosure), IPP 3 (Data Quality) and IPP9 (Transborder Data Flows).

In January 2009 Privacy Victoria published a report on the findings of its survey into the Victorian Public Sector's use of PSDs.<sup>1</sup> Significantly, but not surprisingly, the survey showed that the public sector generally handled PSDs poorly and that their use of them potentially posed a serious data security risk.

The report made 17 Recommendations to assist organisations to comply with the IPPs in their use of PSDs. These recommendations appear at Appendix 2. The first Recommendation was that at a minimum organisations need to have a formal policy on PSD use. This guide is intended to assist organisations to develop such policies and related procedures. A short checklist drawn from the guide appears at Appendix 1 but I recommend that the whole document is read before the checklist is used.

Finally – a caution. Some of the IPPs refer to organisations taking 'reasonable steps' rather than being absolute. It is a widespread belief that if policies and procedures are in place that alone will constitute 'reasonable steps' – for example to protect personal information from misuse, loss, unauthorised access, modification or misuse (IPP4). This is not so. In a number of instances when a breach has been reported to this office, an organisation had policies and procedures in place, but were of no use because they were ignored. The mere existence of a policy does not in my view constitute 'reasonable steps' without some demonstrable effort to make users aware of the content of them, and that they are adhered to. And in some instances, depending on the nature of the personal information stored on the PSD, merely having a policy may not be sufficient.

My thanks to Jon Armstrong for his work in preparing this guide.

Helen Versey  
Victorian Privacy Commissioner

---

<sup>1</sup> *Use of Portable Storage Devices – Privacy Survey*, January 2009 available at [www.privacy.vic.gov.au](http://www.privacy.vic.gov.au)

## 2. Scope

Policies and procedures relating to PSD use should be based on the risk management profile of the organisation. A thorough risk assessment will have considered a broad range of risk factors, as illustrated below. Where PSDs have not previously been given specific attention, the risk profile should be revisited to ensure they are given due regard, as they pose a significant data security risk.

Risk assessments should explore the prospect of implementing technical controls to counter inappropriate PSD use. When conducting the associated cost-benefit analysis of introducing technical controls, the potential costs of dealing with PSD related security breaches should be considered.

### Existing suite of policies and procedures

What do you already have in place? Organisations should have various policies and procedures to cover data and equipment protection. These could be all encompassing documents or a series of subject specific materials. An audit of existing policies and procedures should be conducted to determine where gaps exist before deciding how to cater for PSDs.

A useful means of auditing existing documentation is to view data from a life-cycle perspective, and ask where the 'path of least resistance' to data misuse may lie. To illustrate, if the rules surrounding PSD use were to become too restrictive or obtuse, then users may look for alternative pathways through say, a light-touch email policy. Accordingly, restrictions introduced to combat PSD misuse should have consequential amendments to other data use policies.

It is recommended that PSD policies be stand alone. However, some organisations may prefer to integrate new contents into existing, broader application policies. If subsumed in broader documents (e.g. IT security policy) then references to PSDs should be clear and detailed. The key point is that users be able to find the rules with a minimum of effort.

### Legislative and regulatory obligations

The *Information Privacy Act* is concerned with the protection of personal information – large volumes of which can be stored on a single PSD. However, there are several other legislative instruments that should be addressed through policies and procedures, including the *Public Records Act* and the *Freedom of Information Act*. Organisation specific Acts and regulations which may contain relevant provisions should also be addressed through policy.

Besides personal information, confidential corporate information (e.g. contracts, intellectual property) can also be stored on PSDs – even on the same device. Hence it would be illogical for a PSD policy to focus on one category of data only; data is most unlikely to be segmented in a convenient manner.

Information classification schemes, if well conceived and implemented, can assist organisations to use PSDs in a suitable manner, as the classification by definition must take account of the legislative and regulatory environment. It is recommended that the use of PSDs be included in the planning phase, to ensure that their use is tied to the classification policies and procedures (e.g. classified data requiring mandatory encryption).

## Definition of PSDs

What do you include and what do you exclude? The potential list is long and growing all the time. OVPC's survey excluded CDs/DVDs as they are media not devices, and excluded laptops as they have more in common with networked PCs. But the definition of PSDs is a local concern, based on local operational realities. Whatever the conclusion, all devices that can connect to an organisation's network, and related media, should be covered through policies and procedures.

Yet the definition exercise can prove frustrating. One way to deal with this is to use inclusive language ("PSDs include the following devices...."), and the list can then be expanded as new products come to market.

If laptops are included in the PSD definition they may not be afforded the same protections as say, networked PCs. Problems could arise if the only rules surrounding the use of laptops were to be found in a stand-alone PSD policy, as they may be overlooked.

Organisations should also consider whether 'music players' such as iPods and MP3 players are suitable devices for use in work areas, given their data storage capacities and the risk they pose for IT environments.

## User types

What are the different categories of user accessing your network? Should some parts of the organisation have more stringent controls than others?

Ideally, network access should only be granted once the role and employment status of individuals has been determined in advance. This would make decisions about PSD use relatively easy. However, this is not standard practice, partly because it would require greater integration between line managers, Human Resources, Finance and IT systems administrators before users can start.

One important scoping consideration is whether some business areas should have more robust controls such as port disabling (e.g. USB ports). Examples include:

- Service counters or data processing areas, where there is no business-related need for port access.
- Areas which handle highly sensitive information which require higher security measures than elsewhere in the organisation. What might be considered 'reasonable steps' to protect personal information from loss, misuse or unauthorised access will not necessarily be the same for all business areas.<sup>2</sup>
- Although port disabling can be a low cost solution, it can introduce significant inconvenience to other business areas. For example, corporate communications staff may require port access in order to undertake in-house publishing work.

---

<sup>2</sup> See Office of the Victorian Privacy Commissioner *Guidelines to the Information Privacy Principles* September 2006 IPP4 pp 96 – 103, available at [www.privacy.vic.gov.au](http://www.privacy.vic.gov.au)

## Audience

Who will write the policies and procedures? And who are they being written for?

IT systems administrators may not be the right people to write policies with the broad range of users in mind. Besides, PSD use is not merely an IT concern, despite some organisations seeing all technical matters as an 'IT responsibility'. There are behavioural factors to consider, particularly if policy is to be the sole means of control. Policy authors should be able to reflect on the following:

- How do people go about their work in the organisation? and
- The legal environment for the organisation, including privacy considerations.

## Service Providers

The data life-cycle may involve other entities that are either outside your network or run your network under contract. How to ensure consistent rules in service providers is an important scoping consideration, and may become particularly relevant in the case of a privacy breach involving misuse of PSDs. Three scenarios are presented.

### OUTSOURCING OF FUNCTIONS TO THE PRIVATE SECTOR

Traditional outsourcing arrangements are common for technology services and sometimes for human resource functions. Typically, organisations will have included a Section 17 (*Information Privacy Act*) clause into the relevant State contract which binds the service provider to the IPPs. Service provider policies surrounding PSD use should be consistent with those of the outsourcing organisation.

### CENITEX

The Centre for IT Excellence (CenITex) may appear to be a contracted service provider, but is actually a Victorian Government agency managing a number of departmental IT environments. So, it is subject to the *Information Privacy Act* in its own right, and as a 'service provider'. But the same principle applies: departmental policies surrounding PSD use should be in harmony with CenITex policies.

### FUNDED AGENCIES

Organisations such as the Department of Human Services have a number of private and community sector organisations that deliver services. They should also have consistent PSD use policies.

## 3. Technical controls

What does the policy say about technical controls? If technical controls have been implemented – whether software, hardware or a combination – then users need to know what the implications are for them. Policies and procedures should include relevant information.

### Principles behind the selection of technical controls

#### STANDARDS

Victorian Government agencies and departments are required to comply or align with ISO 27001 and ISO 27002. This supports consideration of technical controls, particularly where *compliance* is decided upon.

#### SOFTWARE CONTROLS

Endpoint Security tools<sup>3</sup> offer a wealth of features that can provide significant PSD control. Even Windows Vista includes features that can be utilised. The ongoing management requirements need to be factored in though, as it could be a major undertaking to determine which individual devices are permitted to use say, USB ports, as the means of enforcing restrictions on the use of iPods and MP3 players.

#### MIXED IT ENVIRONMENTS

These present more issues for device management. Whether a mix of PCs and Apple Macs, or XP and Vista, technical controls will need to cater for the different combinations.

#### ENCRYPTION

Encryption options should be explored for all PSDs which are likely to be used to store personal information, including USB keys, mobile phones, PDAs and even so-called ‘music players’. The likely administrative overheads surrounding encryption must also be factored in.

### Policy implications of PSD technical controls for users

#### HOME AND REMOTE USE

PSD technical controls are manageable where only corporate equipment can be used for remote and home access (e.g. laptops). However, controls are more difficult to impose when organisations permit VPN (Virtual Private Network) clients to be installed on privately owned equipment (e.g. home PCs). In some scenarios, users can flout network controls altogether. As discussed under Scope, organisations need to align all their technology policies to ensure data protection is adequately covered, and if technical controls cannot be implemented, then behavioural controls must be specific. However, there is always going to be a major risk where home PCs are used for VPN access and ‘appropriate behaviour’ (i.e. consistent with corporate policy) is all you have to protect against home users downloading corporate data to personal PSDs.

---

<sup>3</sup> See *Use of Portable Storage Devices – Privacy Survey*, January 2009 available at [www.privacy.vic.gov.au](http://www.privacy.vic.gov.au)

## DISABLING PORTS

Where across-the-board USB port disabling is implemented, organisations need to cater for exceptional circumstances to allow devices to be used by specific users for set periods to achieve relevant business objectives. Users need to know what to do when they have a genuine work-related need to utilise the ports.

## ENCRYPTION

If personal information is permitted to be stored on PSDs, encryption should be used. However, the encryption method must be simple and able to work in other environments. Note that 'native encryption' can be difficult to use and easily ignored.

## ERASING PERSONAL INFORMATION

Simple deletion is not sufficient, as personal information still resides on the PSD and can be retrieved by a technologically competent person. If organisations determine that data on PSDs should be subject to true erasure, then they should make a strong 'digital wipe utility' available. Users should then be informed about the use of this tool.

## 4. Policy framework for use of PSDs

Good policies target the right audience, giving them clear instructions, in language they can understand. Good policies must be supported by relevant procedures; otherwise they are merely statements of intent. What follows is a comprehensive list of topics that should be considered when framing your PSD policies.

### Purpose

Organisations generally understand that all computers connected to an organisation's network need to be protected against security risks. The same cannot be said for PSDs, which are sometimes regarded as gadgets, or worse, toys. Therefore, it is recommended that policies include a statement of purpose to address such misconceptions.

Where policies are supported by technical controls it is self-evident that the organisation is concerned about the potential for PSD misuse. But where the policy is the sole means of protection, it is critical that users are educated about the data loss/theft risks that surround inappropriate PSD use. Compliance with legislation such as the *Information Privacy Act* should also be integrated into the objectives.

### Language and Audience

Regardless of whether the PSD policy is stand alone or a section of a broader technology use policy, it should be written in language easily understood by non-technical users. An exception to this principle would apply for related procedures written for technical specialists (e.g. systems administrators), but in general, all users need to know where they stand in clear, unambiguous language.

#### AUDIENCE

The same rules may not apply to different user groups, and should have been considered at the scoping phase. The following list highlights the need to determine whether different rules are to apply to different user types.

- **EMPLOYEES:** could encompass a variety of roles and permissions. Those with broader access privileges may need specific information in a policy.
- **CONTRACTORS:** they may be employees of a contracted company or an individual hired through an agency. They are often confused with staff as they work alongside them with similar network rights. However, they may be effectively unknown to Human Resource business units, and acquire network access through manager requests. They are likely users of personal PSDs, and prone to believing that such policies do not apply to them.
- **CONTRACTED SERVICE PROVIDERS:** where information technology functions are outsourced, the relevant companies will be major users of PSDs. Those companies will have their own policies and procedures, but should ensure they are consistent with the rules of their client organisation/s. The same principle applies to CenITex and funded agency scenarios.
- **CONSULTANTS:** although there are similarities with contractors, the terms are not synonymous. Consulting tasks may require less network access than contracting, yet this may not be a consideration at the time. Highly likely to be users of personal PSDs, and also prone to believing that such policies do not apply to them.

- **SYSTEM ADMINISTRATORS:** whether employees or contractors, by definition they have greater access privileges than standard users. They will require more complex and technical procedures. They are capable of turning off technical controls, and therefore can present a serious threat to compliance with PSD policies.
- **STUDENTS:** students are major users of PSDs and often have a high level of technical competence. If they have access to the corporate network, policies must include them.
- **VOLUNTEERS:** a number of organisations have volunteers accessing their network, perhaps solely via PSDs. This represents a further policy challenge, as punitive measures for non-compliance with policies may be more difficult to enforce. Again, this is another important scoping consideration.

## Technical controls

Where policies are used in combination with hardware and/or software controls, the procedures surrounding those other controls should be made clear in the policy. Users need to understand the nature of the implemented restrictions, not only from a risk education perspective, but also, to avoid confusion. To illustrate: where USB ports have been restricted to specific corporate PSDs, or disabled altogether, users need to know why and what to do if a genuine business need arises.

## Corporate PSDs

Regardless of whether PSD technical controls are used in your organisation's network, corporate PSDs will at least be subject to the existing protections of your IT environment (e.g. anti-virus regime). Corporate PSDs can also be identifiable, as opposed to personal devices. A well written policy will consider all the following factors for inclusion.

### PROCUREMENT AND TRACKING

Organisations need sound PSD management measures, including user obligations. These measures include:

- Prospective users providing an acceptable business case before a PSD will be purchased and supplied.
- An organisation standard on what types and brands of PSD will be purchased.
- Maintaining a central register of all corporate PSDs.
- PSDs should be defined as 'attractive items' and tracked accordingly.
- Active enforcement measures, such as IT Help Desk staff explaining PSD use to users prior to handing over devices.

### UPDATING NETWORK DATA

Failure to update corporate data following amendment on a PSD raises critical data integrity and records management issues which must be addressed. If data on a PSD is amended then corporate systems must be updated promptly to maintain data integrity. Policies need to include rules to address this. Technical controls will not assist where users fail to observe this requirement. This principle also applies where personal PSD use is permitted.

## PERMISSIBLE DATA AND USAGE

Organisations should define which categories of data are permissible for use, and in what circumstances. These include:

- When corporate PSDs may be used for personal use.
- Which data cannot be stored on unencrypted PSDs, and if not, whether encrypted PSDs may be used.
- Whether users may share the use of corporate PSDs. Note that this runs the additional risk of private and personal information being seen by others.
- PSDs should not be sent through the mail because of the risk of loss.
- PSD policies and related procedures should clearly explain to users how and when to delete, or digitally wipe data from devices in their possession.

## REALLOCATION AND DISPOSAL

Organisations should ensure that PSDs are only passed on to other users once corporate data has been deleted, or preferably, digitally wiped. But when PSDs are deemed obsolete, a suitable disposal regime should be developed which, in some circumstances, may include outright destruction.

## LOSS OR THEFT

Users should be made aware that PSD loss or theft needs to be reported. They should also be aware of the reporting procedure, with responsible officers clearly identified.

## DATA BACKUP

PSDs (e.g. USB keys) should not be used in lieu of a formal data backup regime. Users should be informed that informal data backup practices are not appropriate without management approval.

## ENCRYPTION

Thorough analysis of the potential user experience – both within and external to the organisation's network – should be explored prior to implementing a PSD encryption regime. Comprehensive procedures will be required for 'native' software encryption, as the onus is placed on the individual to protect the data. More robust solutions require users to do less, but enforced password protection typically generates a greater management workload for IT business units.

## Personal PSDs

The key decision for organisations is whether to permit the use of personal PSDs, and if so, which types, by which users, and under what circumstances. Where supported by technical controls, that key decision can be put into effect with some confidence. However, where policy is the sole means of restricting or managing the use of personal PSDs, an organisation needs to be prepared for constant vigilance. Note that many of the points raised under the previous header (Corporate PSDs) will also apply.

An obvious means of controlling the use of personal PSDs is to ensure that a suitable range of corporate PSDs are available for use.

It is recommended that any request for use of personal PSDs should be subject to prior management approval, and a register established to assist compliance. Personal devices should be subjected to analysis prior to and post use in a corporate network.

## Remote use (including home use)

Working remotely raises issues, not least of which is the likelihood that users will be outside existing network protections. Existing remote use, fleet security and even email policies should be cross-referenced to ensure they are not compromised by remote PSD use. Even if technical controls have been introduced, it is simplistic to believe that PSD use in remote locations, including the home, will always be consistent with the organisation's expectations. Unauthorised users, such as family members, become important factors to consider.

## Communication and Enforcement

Policies should be actively and effectively communicated, rather than left to passive methods. Induction only happens once and generic emails are not always read. Where technical controls are implemented, users will soon realise that there are systemic restrictions on their PSD use. But where the controls are solely policy-based, and only passively reinforced, they may not observe the rules at all. The following suggestions should be considered:

### LINE MANAGER RESPONSIBILITIES

Do responsible managers know what they are meant to be monitoring? They need to be aware of the storage capabilities of iPods and MP3 players, and whether their use is permissible. They need to know more about iPhone capabilities, and what a corporate USB looks like, among other things. Unless they know, they cannot control.

### AUDIT

Tracking PSD use is possible where endpoint security software is implemented. It is recommended that policies explain the nature of these audit logs, as a pre-condition to PSD use. Without such software tools, auditing the use of, say USB ports, is almost impossible.

### DISCIPLINARY ACTIONS

Users need to know the consequences for non-compliance with the policy. It needs to be remembered that the loss of a PSD is not a matter of the cost of the device itself (e.g. \$70 for a 16Gb USB key) but rather, the loss of potentially thousands of sensitive case files.

### OWNERSHIP AND ADVICE

Users need to know where to go for advice about PSD use. While this will likely be the IT Help Desk, emphasis should also be given to Records Management, Human Resources, and the Privacy Officer.

## 5. Governance

Under Scope, it was recommended that a PSD policy should be seen as part of the suite of data protection policies, to ensure that the data life-cycle is given end-to-end treatment. This has major implications for governance. Accordingly, organisations should consider the following.

### Approval

Who approves the policy? This is a significant decision, for the higher up the management chain you go, the more likely it is that the risks surrounding PSD misuse will be appreciated. The CEO is ideal, but at the very least a member of the Executive/senior management team should be responsible. In either case, it is recommended that the policy be subject to Executive team consideration prior to approval.

### Consistent policies in associated organisations

There should be a formal process whereby entities such as contracted service providers are required to have consistent policies on matters such as PSD use. Where an organisation that has a MoU (Memorandum of Understanding) with other organisations involving data use, these need to address PSD use. MoUs should always be current, but technological developments mean that the governance framework of all parties to an MOU needs to be actively managed.

It is probable that PSD use has not found expression in MoUs to date, something that should be addressed as a matter of priority.

### Review Cycles

It is recommended that organisations review policies more than every 12 months. PSD technologies are constantly changing, and policies and procedures may quickly become out of date.

# APPENDIX 1:

## PSD policy development checklist

1.	Who will write your policies and procedures?	
2.	Who approves the policies? Ensure it is someone sufficiently senior.	
3.	Clearly state the purpose of your policy, including the risks associated with the use of PSDs.	
4.	Write your policy in a language easily understood by non-technical users.	
5.	Consider your audience. The same rules may not apply to different users. For example, consultants are likely to be users of personal PSDs. If an external company is a contracted service provider it may have its own policies and procedures and these should be consistent with yours.	
6.	What policies do you already have in place? Audit your existing documents for those that impact on PSDs.	
7.	Are you going to integrate PSD policies into existing ones? If so ensure users can find the rules with minimum effort.	
8.	What other legislative and regulatory obligations do you have that impact on your use of PSDs?	
9.	Do you have an information classification scheme or are you planning one? If so, PSD use needs to be tied to your classification policies and procedures.	
10.	Define which PSDs you include in your policy. Consider using language that allows for additions as new products come onto the market.	
11.	What are the different categories of users accessing your network? Should some parts of your organisation have more stringent controls on the use of PSDs than others?	
12.	Do you have PSD technical controls in place? If so your policies and procedures should include information about them relevant to users.	
13.	Do you allow the use of home computers? Are users permitted to access your network remotely? If so, how will your PSD technical controls apply?	

14.	Do your procurement policies include PSDs?	
15.	Do you maintain a central register of corporate PSDs?	
16.	Will you allow the use of personal PSDs? Consider how their use can be managed if not supported by any technical controls.	
17.	Does your policy define which categories of data are permissible for use on PSDs and in what circumstances?	
18.	Does the policy have rules for updating corporate data on the network if changes are made to information held on a PSD?	
19.	If encryption is provided, is it easy to use and explained in your policy and procedures?	
20.	Does the policy include what needs to be done in the event of loss or theft of both corporate and personal PSDs?	
21.	Does the policy include rules around re-allocation of PSDs? Ensure data is deleted before re-allocation of PSDs.	
22.	Is the secure disposal of PSDs addressed in your policy?	
23.	If technical controls are implemented, do your policies explain whether auditing of their use is possible? Audit controls are not effective unless users are aware of them.	
24.	How are you going to actively and effectively communicate policies and ensure users and responsible managers are fully aware of their responsibilities?	
25.	Do users know where to go for advice about PSD use?	
26.	Do you have a review cycle? Remember PSD technology is constantly changing and your policies and procedures may quickly become out of date. A review cycle should be at least 12 months but preferably more frequent.	
27.	Do you have MoUs with other organisations involving the use of personal information? If so, MoUs need to address PSD use.	

## APPENDIX 2:

# Recommendations from *Use of Portable Storage Devices – Privacy Survey*

---

**RECOMMENDATION 1:** Organisations should have a formal policy on PSD use.

---

**RECOMMENDATION 2:** Risk assessments of PSD use should take account of the assumed strengths and weaknesses of software and hardware protections.

---

**RECOMMENDATION 3A:** PSDs should be defined as ‘attractive items’ and tracked accordingly.

---

**RECOMMENDATION 3B:** Users should be made aware that PSD loss or theft needs to be reported. They should also be aware of the reporting procedure, with responsible officers clearly identified.

---

**RECOMMENDATION 4A:** Organisations should take steps to exercise greater control over non-staff by introducing procedures that distinguish their roles prior to network access being granted. To ensure that employment status is clear greater integration between responsible managers, Human Resources, Finance and systems administrators may be required.

---

**RECOMMENDATION 4B:** Hardware and/or software controls should be introduced to assist organisations distinguish between PSD use for staff, contractors and consultants.

---

**RECOMMENDATION 5A:** Organisations should consider whether iPods and MP3 players are suitable devices for use in the work environment, taking into account their data storage capacities and the risk they pose for their IT environments.

---

**RECOMMENDATION 5B:** Where restrictions are placed on the use of iPods and MP3 players, consideration should be given to the means by which controls are to be enforced (e.g. software and/or hardware controls?)

---

**RECOMMENDATION 5C:** Where policy alone is to be relied on, responsible managers need to be aware of the storage capabilities of iPods and MP3 players.

---

**RECOMMENDATION 6:** PSDs (e.g. USB keys) should not be used in lieu of a formal data backup regime unless a thorough risk assessment has demonstrated that corporate memory is suitably retained and protected. Users should be informed that informal data backup practices are not appropriate without management approval.

---

**RECOMMENDATION 7A:** Where hardware controls (e.g. disabling USB ports) are the agreed solution to the risks posed by PSDs, organisations need to cater for exceptional circumstances to allow devices to be used by specific users for set periods to achieve relevant business objectives.

---

**RECOMMENDATION 7B:** Risks posed by all active ports and interfaces must be considered.

---

**RECOMMENDATION 7C:** Organisations should consider which business areas may be appropriate for port disabling (e.g. service counters or data processing).

---

**RECOMMENDATION 8A:** Risk assessments should include cost-benefit analysis of introducing controls, compared with the cost of security breaches.

---

**RECOMMENDATION 8B:** Although hardware controls can be low cost, the trade-off with perceived or actual loss of convenience should be addressed.

---

**RECOMMENDATION 8C:** Organisations should keep abreast of changes in their licensed software suites, as PSD protections may be included at no extra cost.

---

**RECOMMENDATION 9:** Organisations should explore the device management capabilities of their existing software suites, as they may already incorporate PSD software controls awaiting set up. Ongoing management requirements should also be factored in.

---

**RECOMMENDATION 10A:** A robust PSD use policy should be devoted solely to such devices. If this is not practical, substantial attention to PSDs should be included as part of a broader policy. Policies should be written in language accessible to non-technical users.

---

**RECOMMENDATION 10B:** Policies should be actively and effectively communicated, rather than left to passive channels.

---

**RECOMMENDATION 10C:** Active enforcement measures should be adopted. Examples include Help Desk staff explaining PSD use to users prior to handing over devices, upon receipt of a signed Acceptable Use form.

---

**RECOMMENDATION 10D:** Where policies are used in combination with hardware and/or software controls, the procedures surrounding those other controls should also be made clear.

---

**RECOMMENDATION 10E:** PSD policies and related procedures should clearly explain to users how and when to delete data from devices in their possession.

---

---

**RECOMMENDATION 11A:** Encryption options should be explored for all PSDs which are likely to be used to store personal information. This includes USB keys, mobile phones, PDAs and even so called ‘music players’. Where encryption options are either not available or too convoluted for users, organisations should take steps to ensure those devices are not used to store personal information.

---

**RECOMMENDATION 11B:** Thorough analysis of the potential user experience – both within and external to the organisation’s network – should be explored prior to implementing a PSD encryption regime.

---

**RECOMMENDATION 11C:** Thorough analysis of the potential administrative overheads surrounding PSD encryption should be undertaken.

---

**RECOMMENDATION 12A:** Organisations should ensure that PSDs are only passed on to other users once corporate data has been deleted.

---

**RECOMMENDATION 12B:** Organisations should develop disposal regimes for PSDs which, in some circumstances may include outright destruction.

---

**RECOMMENDATION 13:** To help mitigate the broader security risks, strict limits on the use of personal devices should be enforced, in combination with providing a suitable range of corporately owned PSDs.

---

**RECOMMENDATION 14:** Organisations should implement an information classification scheme. The use of PSDs must be included in the planning phase, to ensure that their use is tied to the classification policies and procedures (e.g. classified data requiring mandatory encryption).

---

**RECOMMENDATION 15:** When evaluating the risk factors for technology resources in organisations, ensure that PSDs are assessed under all the same categories that are applied to laptops.

---

**RECOMMENDATION 16:** The Education sector in general, and tertiary education in particular, must ensure that they protect personal information from PSD misuse.

---

**RECOMMENDATION 17:** Controls implemented by organisations in light of this and other reports need to be flexible enough to cater for developments in PSD technologies.

---

# Victoria's Information Privacy Principles (IPPs) Summary

## 1. Collection

Collect only personal information that is necessary for performance of functions. Advise individuals that they can gain access to their personal information.

## 2. Use and Disclosure

Use and disclose personal information only for the primary purpose for which it was collected or a secondary purpose the person would reasonably expect. Uses for secondary purposes should have the consent of the person.

## 3. Data Quality

Make sure personal information is accurate, complete and up to date.

## 4. Data Security

Take reasonable steps to protect personal information from misuse, unauthorised access, modification or disclosure.

## 5. Openness

Document clearly expressed policies on management of personal information and provide the policies to anyone who asks.

## 6. Access and Correction

Individuals have a right to seek access to their personal information and seek corrections. Access and correction will be handled mostly under the Victorian *Freedom of Information Act*.

## 7. Unique Identifiers

A unique identifier is usually a number assigned to an individual in order to identify the person for the purposes of an organisation's operations. Tax File Numbers and Driver's Licence Numbers are examples. Unique identifiers can facilitate data matching. Data matching can diminish privacy. IPP 7 limits the adoption and sharing of unique identifiers.

## 8. Anonymity

Give individuals the option of not identifying themselves when entering transactions with organisations, if this would be lawful and feasible.

## 9. Transborder Data Flows

Basically, if your personal information travels, privacy protection should travel with it. Transfer of personal information outside Victoria is restricted. Personal information may be transferred only if the recipient protects privacy under standards similar to Victoria's IPPs.

## 10. Sensitive Information

The law restricts collection of sensitive information like an individuals racial or ethnic origin, political views, religious beliefs, sexual preferences, membership of groups or criminal record.

The Information Privacy Principles  
are simply...

the right information,  
to the right people,  
for the right reason,  
in the right way,  
at the right time.



Office of the  
Victorian Privacy  
Commissioner

GPO Box 5057  
Melbourne Victoria 3001  
Australia  
DX 210643 Melbourne

Level 11  
10-16 Queen Street  
Melbourne Victoria 3000  
Australia

Local Call 1300 666 444  
Local Fax 1300 666 445

[www.privacy.vic.gov.au](http://www.privacy.vic.gov.au)  
[enquiries@privacy.vic.gov.au](mailto:enquiries@privacy.vic.gov.au)