

|  |
| --- |
| Privacy and information security guideline for funded agency staff |
|  |

Contents

[Privacy and information security 1](#_Toc49509025)

[Requirements and best practice 1](#_Toc49509026)

[Types of information 2](#_Toc49509027)

[Victorian Protective Data Security Standards 3](#_Toc49509028)

[Summary of obligations 3](#_Toc49509029)

[Protective Markings 4](#_Toc49509030)

[Best practice information management 4](#_Toc49509031)

[Handling personal information 4](#_Toc49509032)

[Sharing personal information 4](#_Toc49509033)

[Passwords 5](#_Toc49509034)

[Unsolicited and suspicious emails 5](#_Toc49509035)

[Free web-based email accounts and file sharing software 5](#_Toc49509036)

[Clear desks and screens 6](#_Toc49509037)

[Information disposal 6](#_Toc49509038)

[Visitors 6](#_Toc49509039)

[Portable storage devices 6](#_Toc49509040)

[Privacy and information security incidents 7](#_Toc49509041)

[Incident reporting 7](#_Toc49509042)

[Where do I find further information? 7](#_Toc49509043)

# Privacy and information security

## Requirements and best practice

Failure to appropriately collect, store, use and disclose information where it is lawful to do so can leave the department and funded agencies without key information to support clients efficiently and effectively. It also exposes clients to significant risk. This guideline has been developed to assist funded agency staff to:

* Understand their obligations in relation to privacy and information security.
* Become familiar with the relevant legislative and compliance frameworks, including how agencies assure the department the steps they’re taking to protect privacy and keep public sector information secure through their auditing processes.
* Develop a privacy aware culture through best practice information management and cyber security awareness training.
  + Know where to get further information and resources. See the [Victorian Office of the Information Commissioner (OVIC) website](https://ovic.vic.gov.au/) < <https://ovic.vic.gov.au/>> for further information around privacy and information security. For information regarding the protection of health information, see the Health Complaints Commissioner (HCC) website: <https://hcc.vic.gov.au/>

In summary privacy is about protecting personal (including health information and sensitive information which from here on will be referred to as ‘personal information’) information, whether in hard copy or electronic form, from:

* Unauthorised access and disclosure (limit to those who have a need-to-know).
* Unauthorised modification (maintain the integrity of the information).
  + Inappropriate transmission, transportation, storage and disposal, and loss of information.

This guideline is to assist funded agencies understand their privacy obligations; it is not exhaustive. It is the responsibility of each agency to understand and comply with its privacy obligations.

## Types of information

| Type | Description |
| --- | --- |
| Health | Information or an opinion about:  the physical, mental or psychological health (at any time) of an individual; or  a disability (at any time) of an individual; or  an individual's expressed wishes about the future provision of health services to him or her; or  a health service provided, or to be provided, to an individual –  that is also personal information.  Health information also includes personal information: collected to provide, or in providing, a health service; about an individual in relation to tissue or body substance donation; that is genetic information which is or could be used to predict the health of an individual or their descendants. |
| Personal | Information or an opinion – whether true or not – about an individual whose identity is apparent or can reasonably be ascertained from the information but does not include health information.  For example, for a person with a disability (resident) living in a group home this includes personal profiles, plans, case notes and file notes. |
| Sensitive | Sensitive information is a subset of personal information. It means information or an opinion about an individual’s:  racial or ethnic origin  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. |

Personal information and its disclosure is protected under Victorian law, including but not limited to the:

* *Health Records Act 2001*
* *Adoption Act 1984*
* *Privacy and Data Protection Act 2014*
* *Children, Youth and Families Act 2005*
* *Public Records Act 1973* 
  + *Disability Act 2006.*

The Information Privacy Principles (IPPs) and Health Privacy Principles (HPPs) set out principles which guide the way in which personal and health information must be gathered, used and stored. In summary the principles cover the following things. OVIC gives details of the IPPs (and how they apply) on its website.

* **Collection:** An agency must not collect health or personal information unless it is necessary.
* **Use and Disclosure:** An agency must not use or disclose personal or health information for a purpose other than the primary purpose, unless an exception applies.
* **Data Quality:** An agency must take reasonable steps to ensure that the personal or health information it collects, uses or discloses is accurate, complete and up to date.
* **Data Security:** An agency must take reasonable steps to protect the information it holds from misuse, loss, unauthorised access, modification or disclosure.
* **Openness**: An agency must set out in a document clearly expressed policies on its management of personal or health information, which should be available to anyone who asks for it.
* **Access and Correction:** An agency that holds personal or health information must ordinarily provide individuals with access to their information. This may be via a Freedom of Information request.
* **Unique Identifiers:** Agencies should not apply unique identifiers to individuals unless it is reasonably necessary to enable the agency to perform its duties, and in accordance with IPP 7/HPP 7.
* **Anonymity:** Wherever lawful and practicable, individuals must have the option of not identifying themselves.
* **Transborder data flows:** An agency should not transfer personal or health information outside Victoria unless that information will continue to be protected in accordance with the IPPs and HPPs, and in accordance with IPP9/HPP 9.
* ***Personal Information only*** – **Sensitive Information:** Organisations must not collect sensitive information unless under certain circumstances (e.g. with consent, as required by law, to prevent harm), in accordance with IPP10.
* ***Health Records only*** – **Transfer or Closure of Practice of Health Service Provider:** Agencies have specific information management requirements in this circumstance, including under HPP 10.
  + ***Health Records only*** – **Making Information Available to Another Health Service Provider:** Health Service Providers must share health information with other Health Service Providers upon individual’s request, and in accordance with the Health Records Act including HPP 11.

More information about the IPPs and HPPs can be found [Information Sheet: Privacy Principles](https://ovic.vic.gov.au/privacy/guidelines-to-the-information-privacy-principles/).

## Victorian Protective Data Security Standards

The Victorian Protective Data Security Standards (VPDSS) comprise 12 standards covering governance, information security, personnel security, physical security and ICT security. The Victorian Information Commissioner requires the Department to attest against the Standards every 2 years in August. For funded agencies this means not acting or engaging in a practice that contravenes the VPDSS. Accordingly, it is expected that funded agencies will:

* Identify the information assets they have (relating to activity the Department funds as a minimum) and their key systems that are involved in managing this information.
* Have a current Information Security Policy, Privacy Policy and Information Asset Governance Policy endorsed by the senior management of the organisation.
* As an initial cybersecurity baseline, funded agencies should implement the Australian Government's [Australia Cyber Security Centre (ACSC) Essential Eight](https://www.asd.gov.au/publications/protect/essential-eight-explained.htm). This involves an assessment of compliance with the Essential Eight and planning to remediate any identified gaps as soon as practicable. Free resources include a free [maturity model assessment](https://www.asd.gov.au/publications/protect/essential-eight-maturity-model.htm) tool.
* Undertake a self-assessment of VPDSS, identify security risks and have a protective data security plan in place to remediate and improve their security maturity including mitigate risks. Funded Agencies should also subscribe to the [Stay Smart Online](https://www.staysmartonline.gov.au/) website service.

## Summary of obligations

Funded agencies must ensure that:

* Staff are trained about privacy, data security and data quality requirements and how the Information and Health Privacy Principles apply to their day-to-day work.
* Service users are informed about how their personal information will be used and disclosed, including how their personal information is protected from misuse, loss, unauthorised access, modification and disclosure.
  + They comply with the IPPs and HPPs.

As part of service agreement monitoring, agencies can expect to be asked:

* Are staff provided training or support resources about the obligations of organisations in managing privacy, data security and data quality requirements and how the IPPs and HPPs apply to their day-to-day work? The organisation needs to provide a verbal or written description of staff training about information privacy, data security and data quality.
* To undertake three activities related to providing assurance to the department in accordance to VPDSS and information security. The Information Security for Funded Organisations SharePoint site goes into detail regarding the three required activities and assurance. To obtain access please email vpdss.infosec@dhhs.vic.gov.au
* Are service users informed about how their personal information will be used and disclosed, including how their personal information is protected from misuse, loss, unauthorised access, modification and disclosure? The organisation needs to provide a copy of the Information Privacy Statement it provides to service users.
* What procedures and initiatives are in place to improve compliance with the IPPs and HPPs? The organisation needs to provide a verbal or written description of any information privacy, data security and data quality initiatives.
  + Agencies may be asked to provide their information governance policy; the policy should demonstrate that the organisation has considered their information management risks.
  + Agencies as part of the assurance process will be asked to provide their self-assessment, security risk profile assessment and protective data security plan when audited.

## Protective Markings

Information from the Department that we share with you may contain protective markings. Protective markings are information sensitivity labels applied to information handled by the department and shared with its agencies, partners and third-party providers. Protective markings are part of the mandatory VPDSS managed by the Office of the Victorian Information Commissioner (OVIC).

The funded agency portal will soon have more information on protective markings, that’s part of the mandatory VPDSS that funded agencies are obliged to comply. More information on the definitions of protective markings can be found at <https://www.dhhs.vic.gov.au/protective-markings>.

# Best practice information management

The following section provides guidance on best practice day-to-day management of information in order to assist funded agencies with practical actions in order to:

* Comply with legislative and compliance frameworks and standards.
  + Promote a privacy aware culture.

## Handling personal information

Personal information may only be accessed and used for a valid work purpose. When handling personal information:

* confirm recipient details before sending faxes or emails, and consider whether email or fax is sufficiently secure to protect the information from unauthorised access (e.g. should the information be password protected or encrypted?)
* always store any hard copies of confidential information that you are not using in a secure cabinet or room
* be aware of your surroundings and people nearby
* limit taking hard copy information away from secure sites
* secure information when travelling e.g. in briefcase, folder.
* dispose unneeded copies of information securely
  + ensure the information is available to people who need to access it.

## Sharing personal information

Personal information may be shared only:

* when a formal agreement exists in relation to information or data sharing between parties
  + in circumstances permitted under the Privacy and Data Protection Act.

To minimise the risk of unauthorised disclosure:

* check with your manager before sharing confidential information if you are unsure
  + do not use Internet-based file sharing software to share confidential information (e.g. BitTorrent, Dropbox).

When sharing information with authorised persons via email:

* ensure all confidential information is attached to the email in a password protected zip folder
* enable encryption where available
* do not include confidential information in the subject line or body of the email
* do not send information to or from free web-based email accounts such as Gmail, Hotmail or Yahoo! If this is the only means available (e.g. the recipient only has Gmail), encrypt the information so it can only be accessed by the intended recipient.
  + do not share or discuss confidential information on social networking applications or sites such as Facebook, LinkedIn and Twitter.

## Passwords

* User IDs and passwords for access to computer services are for the sole use of the person to whom they are allocated.
* Make passwords difficult to guess. Consider using a passphrase instead for example: !Liketog0totheBeach
* Keep all passwords secret—do not write them down or provide them to another person.
  + Change passwords regularly.
  + Utilise multi-factor authentication for added security.

### Downloading software and applications

Software and applications downloaded from the Internet can contain viruses that threaten the security of information stored on users’ computers.

Remember:

* Do not download unauthorised software from the Internet onto your computer
  + Lodge a formal request with your manager if you need software installed in order to complete your work activities.

## Unsolicited and suspicious emails

Unsolicited emails can contain viruses that threaten the security of information stored on users’ computers.

If you receive an email from an unknown sender and it looks suspicious:

* do not open the email or click on links contained in its subject line or body
  + report the email to your manager and delete the email immediately.

## Free web-based email accounts and file sharing software

Free web-based accounts and file sharing software are often owned by international companies in foreign jurisdictions. Information is stored on systems outside of Australia with differing legislation applied to the information. Examples of free web-based email accounts include:

* Gmail
* Hotmail
  + Yahoo!

Examples of file sharing programs include:

* BitTorrent
* Kazaa
  + Limewire

Once information has been sent to web-based email accounts or uploaded onto file sharing programs it can no longer be controlled. Personal information should not be sent:

* to or from a free web-based email account
  + via internet-based file sharing software.

## Clear desks and screens

Work environments should be clear of personal information when unattended. This means:

* not leaving documents containing confidential information unattended on photocopiers, fax machines or printers or desks
* locking your computer’s screen when leaving it unattended
* only printing documents when absolutely necessary
  + storing portable storage devices and hard copies of confidential information in a secure drawer or cabinet, not on your desk.

## Information disposal

Ensure record retention requirements have been met prior to the disposal of any business information.

When disposing of personal information:

* Place unneeded working documents or copies of information in secure bins or adequate shredders.
  + Ensure any electronic media including computers, hard drives, and USB keys are sanitised when no longer required.

## Visitors

To help minimise the risks to the security of personal information:

* ensure all visitors are registered, their identity verified, and accompanied at all times
* make sure staff are aware of the risk of tailgating when entering agency premises
* be aware of unaccompanied people who you do not recognise
  + notify your manager if you believe an unauthorised person is present on premises.

## Portable storage devices

Portable storage devices are usually small and capable of storing large amounts of information, and in some cases can be used to copy, transmit or share information.

Examples of portable storage devices include:

* removable media (e.g. CD-ROMs, DVDs, USB drives)
* digital MP3 players (e.g. iPods)
* laptops, tablet computers and slates (e.g. iPads)
* smartphones (e.g. iPhones)
  + mobile phones.

Using portable storage devices to access, store or transport personal information involves considerable risk because:

* they can be easily lost or stolen, and then accessed by unauthorised people
  + using portable storage devices in public or non-agency premises increases the chance of accidentally disclosing personal information to unauthorised people.

To minimise the information security risks associated with using portable storage devices:

* only use encrypted portable storage devices to store personal information
* unless there is no alternative, avoid storing personal information on portable storage devices
* secure portable storage devices when unattended e.g. lock in a drawer
* be careful of what you say and information you view in public
  + report lost or stolen portable storage devices immediately to your manager.

# Privacy and information security incidents

Privacy and information security incidents may result from unauthorised people accessing, changing or destroying personal information.

Examples of situations from which incidents may arise include:

* accidental download of a virus onto an agency computer
* clicking on phishing links[[1]](#footnote-2)
* discussing or sharing of personal information on a social networking website such as Facebook
* loss or theft of a portable storage device including mobile devices containing personal information
* non-secure disposal of hard copies of personal information (i.e. placing readable paper in recycle bin or hard waste bin)
* documents sent to the wrong fax number or email address
  + documents sent to a free web-based email account such as Yahoo!, Gmail or Hotmail.

Privacy and information security incidents can:

* occur due to accidental or deliberate actions
* result from human error or technical failures
  + apply to information in any form, whether electronic or hard copy.

## Incident reporting

In accordance with Service Agreement section 17.3 (i) it is vital all privacy and information security incidents are reported as soon as possible so that their impact may be minimised. Staff should be aware of:

* how to identify potential privacy and or security incidents
* the reason for reporting incidents is so their impact can be minimised - not to punish individuals
  + the need to report all incidents to their manager as soon as they become aware of them.

The Client Incident Management System (CIMS) focuses on incidents that have a direct impact on clients of the department or related funded organisations. Service providers are required to submit client incident reports and follow-up information electronically to the department for quality assurance and endorsement. This will help to improve the experience and safety of all clients.

Further information can be found on the [Client Incident Management](https://providers.dhhs.vic.gov.au/cims) page.

Privacy incidents are not in scope for CIMS. Funded agencies must use the web based [Privacy Incident Report eform](https://feedback.dhhs.vic.gov.au/layout.html#/privacy) to notify the department about privacy incidents. Where required, the department may report a privacy or security incident to OVIC.

# Where do I find further information?

[Office of the Victorian Information Commissioner: Privacy and Data Protection](https://www.cpdp.vic.gov.au/) for resources, including a Privacy Impact Assessment template, information asset register and data security resources. VPDSS related information is also available.

|  |
| --- |
| To receive this publication in an accessible format email <privacy@dhhs.vic.gov.au>  Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.  © State of Victoria, Department of Health and Human Services October 2020.  Available at <dhs.vic.gov.au/facs/bdb/fmu/service-agreement> |

1. Phishing is a method of trying to gather personal information using deceptive e-mails and websites [↑](#footnote-ref-2)