POLICY

PRIVACY AND DATA SECURITY

RECO RD DET AI LS

Policy	Privacy & Data Security Policy
Date authorised by Executive	August 2017
Review responsibility	Quality and Risk Manager
Date last reviewed	February 2018
Next review date	February 2021
Version	V 1

PURPOSE

To protect the fundamental right to privacy concerning the processing and storage of personal, financial or sensitive information;

To ensure compliance with relevant privacy and data protection legislation;

To ensure transparency and fairness for the management of personal, financial, sensitive or other confidential information that could be considered private at Haven; Home, Safe.

POLICY

Haven; Home, Safe is committed to the safe and secure handling and management of all personal, sensitive, financial and confidential information that it may collect.

Haven Home, Safe is committed to protecting the right to privacy of all individuals whose information it holds.

Haven; Home, Safe staff or any contractors it engages will not act or engage in any practice that breaches any relevant federal or state privacy or data protection legislation.

The following basic privacy principles must be applied at all times

Haven; Home, Safe staff and contractors must:

1. Collect only that information necessary to fulfil Haven; Home, Safe functions and activities
2. Advise individuals of the purpose of collection and their rights to access that information
3. Use the information only for the purpose for which it was collected, for related secondary purposes, with consent or as required or permitted by law
4. Manage all data or privacy breaches in accordance with the Compliance Breach Reporting Procedure (as per below) and notify all and any impacted individuals in the event of a breach
5. Not use or disclose any personal information for purposes other than what it was intended unless an exemption applies or unless express consent has been obtained from the individual.
6. Make every effort to ensure that information is accurate, complete and up-to-date.
7. Ensure the security of information and its proper storage, archiving or disposal in accordance with appropriate recordkeeping standards and information technology safeguards.
8. Be open and transparent about the Haven; Home, Safe Privacy and Data Protection Policy.
9. Be transparent and open about the type of personal information they hold and what is done with such information.
10. Enable individuals to access their data and make appropriate corrections, in accordance with relevant legislation
11. Only share information with appropriate permissions to legitimate recipients, after appropriate risk assessment of privacy protections, and when equivalent safeguards are accorded to the information/data by the recipient

12. Collect and use sensitive information only in accordance with the relevant policy and procedures or where it is required or permitted by law.

The Privacy Act defines personal information as:
…information or an opinion, whether true or not and whether recorded in a material form or not, about an identified individual, or an individual who is responsibly identifiable.

Sensitive information is a type of personal information and includes information about an individual's:

- health
- racial or ethnical origin
- political opinion
- membership of a political association, professional or trade association or trade union
- religious beliefs of affiliations
- philosophical beliefs
- sexual orientation or practices
- criminal records

PROCEDURE

A privacy or data breach occurs when there is a failure to comply with one or more of the privacy principles set out in the basic privacy principles as outlined above. These types of breaches often result in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

Breaches can occur because of a technical error, human error, inadequate policies and procedures, a misunderstanding of the law, a deliberate act or a lack of training. Some of the more common privacy breaches happen when personal information is lost, stolen or mistakenly disclosed.

Staff and contractors engaged by HHS must be vigilant in their handling of sensitive or confidential information at all times.

1. All hardcopy materials that contain information of a sensitive or personal nature that have been collected by HHS must be kept in locked storage at all times
2. Information of a sensitive or personal nature must not be left unattended on desks or in workspaces
3. Computers must be in lock mode if your workspace is not attended
4. All care must be taken to ensure that information sent electronically is only provided to the intended recipient

IN THE EVENT OF A BREACH:

1. Identify and Notify

The Line Manager must be notified as soon as possible of the breach and how it has occurred. This information will then be passed onto the Quality and Risk Manager.

2. Containment

The Line Manager in consultation with the Quality and Risk Manager should take immediate action (based on the type of breach) to limit or contain any further breaches.

Care must be taken not to compromise any investigation that may be required or to remove or damage any evidence that might be part of that investigation.

3. Assessment and escalation

A risk assessment to determine the seriousness of the breach and the degree of associated risk must be undertaken by the Quality and Risk Manager.

Senior management must be advised of all actual and potential breaches.

If the breach is likely to receive adverse media attention, it should also be reported to the Director Communications and Marketing.

HIGH-RISK BREACHES:

High-risk breaches are considered those which may have a serious impact on the Organisation and may include the risk of:

- statutory investigations or sanctions/penalties
- serious reputational damage
- interruption to business continuity

If a breach constitutes a critical incident or severe crisis, the Critical Incident Management Policy should be followed.

4. Investigating the Breach

If it is determined that the breach warrants an investigation, then the type and intensity of investigation to be undertaken will be determined by the degree of risk and the seriousness of the breach.

All investigations must take into account:

- The root cause of the breach
- Identify whether it was a systemic breach, an isolated incident or a deliberate act
- Identify appropriate corrective actions to prevent the breach recurring or escalating
- Outcomes and recommendations of all investigations must be reported to Senior Management

In the event that it is determined that there has been criminal activity, it must be referred to appropriate law enforcement agencies or authorities for investigation

5. Corrective Action

Based on the outcomes of any investigations, recommended preventative or corrective actions will be immediately put in place to prevent further or escalated breaches. Responsibility for these actions will be determined by Management.

Where systemic issues are identified, a thorough policy and/or process improvement review will be undertaken to prevent further breaches. Ongoing monitoring and review of systems, policies and procedures will be undertaken by the Quality and Risk Manager regularly to ensure compliance and quality.

6. Recording Breaches

All breaches must be recorded in the Data/Information Breach Register as maintained by Corporate Services.