The Haven Pregnancy Counselling Centre
54A Church Road
Burgess Hill, RH15 9AE

info@havencentre.org.uk
01444 233333

Information Security Incident Policy

Reviewed annually in January

Purpose

This document defines an Information Security Incident and the procedure to report an incident. This policy applies to all staff, trustees, volunteers, contractual third parties and agents of The Haven who have access to Information Systems or information used for Charity purposes.

Definition

An information security incident occurs when data or information is transferred or is at risk of being transferred to somebody who is not entitled to receive it, or data is at risk from corruption.

An Information Security Incident includes:

- The loss or theft of data or information
- The transfer of data or information to those who are not entitled to receive that information
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system
- Changes to information or data or system hardware, firmware, or software characteristics without The Haven's knowledge, instruction, or consent
- Unwanted disruption or denial of service to a system

- The unauthorised use of a system for the processing or storage of data by any person.

When to report

All events that result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems should be reported as soon as they happen. If the breach occurs or is discovered outside of normal working hours, it must be reported as soon as is practicable.

Action on becoming aware of the incident

- The Centre Manager must be contacted by email or telephone
- You will need to supply the Centre Manager with further information, which will depend on the nature of the incident. However, the following information must be supplied:
    - full and accurate details of the incident
    - when the breach occurred (dates and times)
    - who is reporting it
    - the nature of the personal data information
    - how many individuals are involved

The outcomes of these actions are to be reported to the Manager who will notify The Haven's designated Data Protection Officer.

Containment and recovery

The Manager will first determine if the breach is still occurring. If so, together with the Data Protection Officer and, if appropriate, a representative from the IT support company (the Response Team), the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the Response Team to establish the severity of the breach and whether there is anything that can be done to recover any losses and limit the damage of the breach. That group will also establish who may need to be notified as part of the initial containment and will inform the Chair of The Haven and, where appropriate, the police.

Investigation and Risk Assessment

An investigation will be undertaken as soon as reasonably possible, but, generally, within 24 hours of the breach being discovered/reported.

The investigation will focus on the cause of the breach, the risks associated with it, and will consider:

- the type of personal data involved
- its sensitivity
- the protections in place (e.g., encryptions)
- what happened to the data, whether it has been lost or stolen
- whether the data can be put to any illegal or inappropriate use
- the affected individuals, and the potential adverse consequences to them (including how serious/substantial these consequences could be, and the likelihood of occurrence)
- whether there are wider consequences to the breach
- other relevant considerations

Notification

The Response Team will determine who needs to be notified of the breach.

Every incident will be assessed in regard to notification on a case-by case-basis, including consideration of the following:

- are there any legal/contractual notification requirements
- will notification assist the individuals affected – can they take actions in relation to the information to mitigate risks
- will notification help prevent the unauthorised or unlawful use of personal data
- will notification help The Haven to meet its obligations under data protection law

- if many individuals are affected or the consequences are very serious, does the ICO need to be notified.

If the Response Team discovers a personal data security breach that poses a risk to the rights and freedoms of individuals, it will report it to the ICO within 72 hours (3 days) of discovery.

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the data involved. Where feasible, specific, and clear advice will be given on what they can do to protect themselves, including what actions have already been taken to mitigate the risks. Individuals will also be provided with contact details to allow them to contact The Haven for further information or to ask questions about what has occurred.

The Response Team must also consider notifying third parties such as the police, insurers, banks, or credit card companies, etc. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The Response Team will also consider whether it is appropriate to issue communications to other interested parties.

All actions will be recorded by the Centre Manager.

Evaluation and Response

Once the initial incident is contained, the Response Team will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies or procedures are required.

Existing controls will be reviewed to determine their adequacy, and whether any corrective actions should be taken to minimise the risks of similar incidents occurring.

The review will consider:

- where and how personal data is held, stored, and secured
- where the biggest risks lie, including any further potential weak points within the existing systems / data protection framework
- whether methods of transmission are secure, and compliant with the principle of data minimisation (only sharing the minimum amount of data necessary)

- identifying weak points within existing security measures
- staff awareness and training
- implementing a personal data breach plan and identifying individuals / functions responsible for reacting to reported breaches of security

Any report recommending changes to systems, policies and procedures relating to personal data protection will be considered and approved, as appropriate, by The Haven trustees.

Examples of Information Security / Misuse Incident Protocols

Information Security Incidents are not limited to this list, which contains examples of some of the most common incidents.

Malicious Incident

- Computer infected by a virus or other malware, (for example spyware or adware)
- An unauthorised person changing data
- Receiving and forwarding chain letters including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others
- Social engineering - unknown people asking for information which could gain them access to Charity data (e.g. a password or details of a third party)
- Unauthorised disclosure of information electronically, in paper form or verbally
- Falsification of records / inappropriate destruction of records
- Denial of Service, for example - damage or interruption to Charity equipment or services caused deliberately e.g. computer vandalism
- Connecting non-Charity equipment to the Charity network
- Unauthorised Information access or use

- Giving information to someone who should not have access to it - verbally, in writing or electronically
- Printing or copying confidential information and not storing it correctly or confidentially

Access Violation

- Disclosure of logins to unauthorised people
- Disclosure of passwords to unauthorised people e.g., writing down your password and leaving it on display
- Accessing systems using someone else's authorisation e.g., someone else's user id and password
- Inappropriately sharing security devices such as access tokens
- Other compromise of user identity e.g., access to network or specific system by unauthorised person
- Allowing unauthorised physical access to secure premises e.g., server room, scanning facility, dept area.

Environmental

- Loss of integrity of the data within systems and transferred between systems
- Damage caused by natural disasters e.g., fire, flooding, lightning etc.
- Deterioration of paper records
- Deterioration of backup tapes
- Introduction of unauthorised or untested software
- Information leakage due to software errors.

Inappropriate use

- Accessing inappropriate material on the internet
- Sending inappropriate emails

- Personal use of services and equipment in work time
- Using unlicensed software
- Misuse of facilities, e.g., phoning premium line numbers

Theft / loss Incident

- Theft / loss of data – written or electronically held
- Theft / loss of any Charity equipment including computers, monitors, mobile phones, tablets, memory sticks, CDs.

Accidental Incident

- Sending an email containing sensitive information to 'all staff' by mistake
- Receiving unsolicited mail of an offensive nature, e.g., containing pornographic, obscene, racist, sexist, grossly offensive or violent material
- Receiving unsolicited mail which requires you to enter personal data

Mis-keying

- Receiving unauthorised information
- Sending information to wrong recipient.