Volunteer Cornwall
Information Security Incident Management and Reporting Procedures

Information security incidents are any event that has resulted or could have resulted in the disclosure of confidential information to an unauthorised individual, the integrity of the system or data put at risk or the availability of the system of information being put at risk. Incidents may include theft, misuse or loss of equipment containing confidential information or other incidents that could lead to unauthorised access to data.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Introduction
Information security is everyone's responsibility; this policy has been developed to ensure Volunteer Cornwall employees identify information security incidents, suspected information security weaknesses or near misses or security threats to services or systems and report these incidents through appropriate management channels for investigation and follow up.

Considering the tight timescales for reporting a breach, it is important that Volunteer Cornwall has robust breach detection, investigation, and internal reporting procedures in place.

Information Security Incidents
An information security incident is any violation of Volunteer Cornwall's Data Security and Protection Policy. The term information security incident and suspected incidents is very broad and includes, but is not limited to, incidents that relate to the loss, alteration, disclosure, denial of access to, destruction or modification of Volunteer Cornwall's information, or information systems.

An information security incident can be defined as any event that has resulted or could result in:
- The disclosure of confidential information to an unauthorised individual
- The integrity of a system or data being put at risk.
- The availability of the system or information being put at risk.

An adverse impact can be defined for example as:
- Threat to personal safety or privacy
- Legal obligation or penalty
- Financial loss
- Disruption of Volunteer Cornwall
- An embarrassment to Volunteer Cornwall

Examples of security incidents:
- Using another user's login id/swipe card
- Unauthorised disclosure of personal information
- Leaving confidential / sensitive files out
- Theft or loss of IT equipment
- Theft or loss of computer media, i.e., floppy disc or memory stick

- Accessing a person's record inappropriately
- Writing passwords down and not locking them away
- Identifying that a email has been sent to the wrong recipient.
- Sending/receiving a sensitive email to/from "all staff" by mistake
- Giving out or overhearing personal information over the telephone
- Giving out personal information via social media and promotional campaigns without consent and permission
- Positioning of pc screens where personal information could be viewed by the public.
- Software malfunction
- Inadequate disposal of confidential material

Diligent employees should question procedures, protocols, and events that they consider could cause damage, harm, distress, break of compliance or bring Volunteer Cornwall's name into disrepute.

Procedures for Dealing with Various Types of Incidents
All staff should report any suspicious incidents to their senior manager in the first instance.

Incidents should always be investigated immediately whilst there is still the possibility of collecting as much evidence as possible. Investigations should normally be co-ordinated by the relevant senior manager and the Data Security and Protection Lead.

The following procedures should be followed for breaches:

Physical security including the theft of equipment holding confidential information and unauthorised access to an area with unsecured confidential information:

- Check the asset register to find out which equipment is missing.
- Investigate whether there has been a legitimate reason for removal of the equipment (such as repair or working away from the usual office).
- If the cause is external inform the Police and ask them to investigate.
- If the cause is internal, establish the reason for the theft/ unauthorised access.
- Consider the sensitivity of the data and the risk that it will be mis-used to support assessing whether further action is appropriate (e.g., informing the Police, Information Commissioner).
- Consider whether there is a future threat to system security and the need to take protective action e.g., change passwords.
- Categorise and report the incident as described as per 'recording and reporting' requirements.

Access to records by an authorised user who has no work requirement to access the record:

- Interview the person reporting the incident to establish the cause for concern.
- Establish the facts by.
  - Asking the IT Officer to conduct an audit on activities by the user concerned.
  - Interviewing the user concerned.
- Establish the reason for unauthorised access.
- Consider the sensitivity of the data and the risk to which Volunteer Cornwall has been exposed and consider whether any clients should be informed.
- Take appropriate disciplinary action and action with the client where appropriate.

- Categorise and report the incident as described as per 'recording and reporting' requirements.

Inadequate disposal of confidential material (paper, PC hard drive, disks/tapes):
This type of incident is likely to be reported by a member of the public, a client who has been affected, or a member of staff.

- Investigate how the data came to become inappropriately disposed.
- Consider the sensitivity of the data and the risk to which the clients have been exposed and consider whether the clients should be informed.
- Take appropriate action to prevent further occurrences. (e.g., disciplinary, advice/training, contractual)
- Take appropriate action with the client as appropriate.
- Categorise and report the incident as described as per 'recording and reporting' requirements.

Procedure for dealing with complaints about client confidentiality by a member of the public, client, or member of staff:

- Interview the complainant to establish the reason for the complaint.
- Investigate according to the information given by the complainant and take appropriate action.
- Take appropriate action with the client as appropriate.
- Categorise and report the incident as described as per 'recording and reporting requirements.

Loss of data in transit
Investigate, as far as possible what has gone missing and where.

- Consider the sensitivity of the data and the risk to which the clients have been exposed and consider whether the clients should be informed.
- Take appropriate action to prevent further occurrences. (e.g., process (was the envelope correctly addressed, are there further safeguards that could be introduced).
- Take appropriate action with the client as appropriate.
- Categorise and report the incident as described as per 'recording and reporting' requirements.

Reporting of Security Incidents
All information security incidents should be reported to your senior manager who will ascertain the level of risk and ensure any immediate action is taken appropriate to the level of risk. All incidents will need to be formally recorded on an incident report form and, if appropriate logged to Volunteer Cornwall's risk management or incident reporting system. The senior manager will investigate, document and if necessary, provide feedback on the outcome of the incident.

All significant incidents relating to information security should be reported to Volunteer Cornwall's Chief Executive and Data Security and Protection Lead, particularly in instances where these involve bulk data loss or confidentiality breaches. The Chief Executive and Data Security and Protection Lead will determine whether there is also a need to report the incident to others depending on the type and likely consequences of the incident, e.g., inform the Police, Commissioning Organisation, Information Commissioner, the insurer etc.

Breaches only have to be notified to the relevant supervisory authority where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals, for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage. This must be assessed on a case-by-case basis.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, those individuals must be contacted directly. A high risk means that the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

A log will be kept of all incidents reported, irrespective of whether they lead to a complaint or not.

All incidents should be considered as to whether they indicate a need for improvement in arrangements. The log may be incorporated into other incidents logs as appropriate. A regular report on the number, type and location of information security incidents should be made, allowing any trends to be picked up and addressed.

By reporting such incidents or near misses it allows Volunteer Cornwall to relate to similar occurrences and highlights any areas of vulnerability, identifying where greater awareness is needed, or procedures/ protocols that require reviewing. Good reporting generates better statistical data thus, keeping Volunteer Cornwall informed.

When reporting an information security incident, it is important to ensure sufficient information is given to the DSP lead to enable them to understand and respond appropriately to the report. Users can report security related incidents in confidence; no information about a user's involvement in a security incident will be released without explicit permission.

If reporting software malfunctions, symptoms of the problem and any messages appearing on the screen should be noted. The PC should be isolated and the use of it stopped, until reported. Users must not attempt to remove suspected software or attempt to 'repair/mend' equipment unless authorised to do so.

Incidents should be classified in the log according to severity of risk to clients and Volunteer Cornwall using the following incident classification system described below. For near misses, consider the likely impact if the breach had occurred.

Incident Classification:

Insignificant: Minimal discernible effect on clients or Volunteer Cornwall.	**Minor:** Minor breach, for example data lost but files encrypted, less than 5 clients affected.	**Moderate:** Moderate breach, for example unencrypted records lost, up to 20 clients affected.	**Major:** Serious breach, for example unencrypted records lost, up to 100 clients affected or particular sensitivity.	**Critical:** Serious breach in terms of volume of records, for example over 100 clients affected or particular sensitivity of records.

	Inconvenient to Volunteer Cornwall but manageable.	**Potential for damage to Volunteer Cornwall's reputation.**	**Potential for damage to Volunteer Cornwall's reputation and/or local media coverage.**	**Damage to the reputation of the charitable sector and Volunteer Cornwall. Potential for national media coverage.**

Description of Incident
It is important that the information security incident reports give as much detail as possible, including a description of activities leading up to the security incident, information about circumstances prevailing at the time, how the incident came about, how the incident was detected.

The information security incident or suspected incident report should include full details of the incident in as much details as possible to enable a full investigation to be carried out if necessary. However, when logging incidents, personal details should, wherever possible, be omitted.

Whenever possible when reporting information security incidents, any protocols or procedures which may have been compromised should be referenced on the report.

All information security incidents will be prioritised in accordance with the severity of the incident by the person logging these on the risk or incident reporting system.

Information security incidents are to be reported as soon as possible after they occur or have been identified. Reports sent immediately after the incident are likely to be the most valuable; if there is a delay between an incident occurring and the discovery of said incident, the incident should still be reported.

Security Incidents Reported to Relevant Supervisory Authorities
Information security incidents classified as moderate to critical may need to be reported to the Information Commissioners Office (ICO). It will be the responsibility of the Chief Executive and the Data Security and Protection Lead to decide whether this is necessary.

Breaches only have to be notified to the relevant supervisory authority where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals, for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage. This has to be assessed on a case-by-case basis.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, those individuals must be contacted directly. A high risk means that the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

A breach notification must contain:

- The nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned.
  - The categories and approximate number of personal data records concerned.
- The name and contact details of the Data Security and Protection Lead.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

A notifiable breach must be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows information to be provided in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Failure to notify a breach when required to do so can result in a significant fine.

Staff Training

Staff must be trained so that they understand what constitutes a data breach, and that it is more than a loss of personal data. They must also understand the internal breach reporting procedure that is in place.

Incidents should be used in training sessions about security and confidentiality as using 'real life events' relevant to Volunteer Cornwall can always be related to by staff, a lot better than in imaginary events. This will give the attendees and example of what could occur, how to respond to such event and how to avoid them in the future.

Signed:  Date:

Ian Jones
On behalf of Volunteer Cornwall Review due: 04/25