# Data Breach Process

## 1. Introduction

CVS Cheshire East (CVS) collects, holds, processes, and shares personal data, a valuable asset that needs to be suitably protected.

Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

## 2. Purpose and Scope

CVS is obliged under the General Data Protection Regulation (GDPR) to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

This process sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across CVS.

This process relates to all personal and special categories (sensitive) data held by CVS regardless of format.

This process applies to all staff, volunteers and contractors of CVS. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of CVS.

The objective of this process is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

## 3. Definitions / Types of breach

For the purpose of this process, data security breaches include both confirmed and suspected incidents.

An incident in the context of this process is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the CVS's information assets and / or reputation.

An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
- equipment theft or failure;
- system failure;
- unauthorised use of, access to or modification of data or information systems;
- attempts (failed or successful) to gain unauthorised access to information or IT system(s);
- unauthorised disclosure of sensitive / confidential data;
- website defacement;
- hacking attack;
- unforseen circumstances such as a fire or flood;
- human error, including confidential information left unsecured in accessible areas misdirected emails, publication of confidential data online or accidental disclosure of passwords;
- 'blagging' offences where information is obtained by deceiving the organisation who holds it.
- Inappropriate access controls allowing unauthorised use of information
- The insecure storing and disposal of confidential paper waste

## 4. Reporting an incident

Any individual who accesses, uses or manages CVS's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (Chief Executive).

Overall the Chief Executive is accountable for managing data breaches and must report this to the Trustee Board providing assurance that this is being investigated, managed and resolved.

In line with best practice, these five steps should be followed when responding to a data security breach:



### Step 1: Identification and initial Assessment

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (refer to Appendix 1).

All staff should be aware that any breach of Data Protection legislation may result in CVS's Disciplinary Procedures being instigated.

## Step 2: Containment and recovery

The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with relevant officer(s) to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Staff member Investigating Officer (this will depend on the nature of the breach; in some cases it could be the DPO).

The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

Advice from experts within CVS, including third party suppliers may be sought in resolving the incident promptly.

The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

## Step 3 Investigation and risk assessment

An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following (refer to Appendix 1):

- the type of data involved;
- its sensitivity;
- the protections are in place (e.g. encryptions);
- what has happened to the data (e.g. has it been lost or stolen;
- whether the data could be put to any illegal or inappropriate use;
- data subject(s) affected by the breach, number of individuals involved and the potential
- effects on those data subject(s);
- whether there are wider consequences to the breach.

The results of the assessment will follow the overall organisations risk  matrix scoring.

## Step 4 Notification

The LIO and / or the DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation;
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- whether there are any legal / contractual notification requirements;
- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks.

Individuals will also be provided with a way in which they can contact CVS for further information or to ask questions on what has occurred.

The LIO and / or the DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, trade unions or funding bodies. 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 LIO and or the DPO will consider whether the Marketing Manager should be informed regarding a press release and to be ready to handle any incoming press enquiries.

A record will be kept of any personal data breach, regardless of whether notification was required.

## Step 5 Evaluation and response

Once the initial incident is contained, the DPO 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 and procedures should be undertaken.

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

The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing
- security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;

- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Process subcommittee / Trustee Board.

## Process Review

This process will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

**APPENDIX 1**
**DATA BREACH REPORT FORMS**

Please act promptly to report any data breaches. If you discover a data breach, please notify one of the management team immediately, complete Section 1 of this form and email it to the Data Protection Officer (Chief Executive).

| **Step 1: Identification and initial Assessment** | |
|---|---|
| **Notification of Data security breach** | **To be completed by a member of the Management Team** |
| Date incident was discovered: | |
| Date (s) of incident: | |
| Name of person reporting incident: | |
| Brief description of the incident or details of the information lost: | |
| Number of data subjects affected, if known: | |
| Has any personal data been placed at risk? If, so please provide details: | |
| Brief description of any action taken at the time of discovery | |
| For use by the Data Protection Officer | |
| Received from: | |
| On date: | |
| Forwarded to officer to investigate: | |
| Date forwarded: | |

| **Step 3 Investigation and risk assessment** | |
|---|---|
| **Assessment of severity** | **To be completed by Lead Investigation Officer and other experts where required** |
| Details of the IT systems, equipment, devices, records involved in the security breach | |
| Details of information loss | |
| What is the nature of the information lost? | |
| How much data has been lost? If laptop lost/stolen: how recently was the laptop | |

| | |
|---|---|
| backed up onto central IT systems? | |
| Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the organisation or third parties? | |
| How many data subjects are affected? | |
| Is the data bound by any contractual security arrangements? | |
| What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories: | |
| HIGH RISK personal data<br>o Sensitive personal data (as defined in the Data Protection Act) relating to a living, identifiable individual's<br>a) racial or ethnic origin<br>b) political opinions or religious or philosophical beliefs<br>c) membership of a trade union<br>d) physical or mental health or condition or sexual life<br>e) commission or alleged commission of any offence, or<br>f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings | |
| o Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as National Insurance Number and copies of passports and visas | |
| o Personal information relating to vulnerable adults and children | |
| o Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed | |
| o Security information that would compromise the safety of individuals if disclosed | |
| Category of incident (Low - Severe): | |
| Reported to Trustee Board on: | |
| If Material or above, date escalated by the DPO to the ICO: | |
| If relates to data held linked to a contract: | |

| | |
|---|---|
| Date reported to the Funder/Contractor manager: | |

| Risk Impact – Category of Incident | |
|---|---|
| Low | • Would have a limited impact on service/reputation<br>• Minor impact on staff/volunteer<br>• Minor breach of confidentiality – less than 5 affected or risk assessed as low (e.g. files were encrypted) |
| Moderate | • Would have some impact on service/reputation but manageable<br>• Negative impact on staff/volunteer/service user<br>• Minor negative media/relationship impact<br>• Moderate breach and risk asses (e.g. unencrypted files up to 20 individuals affected) |
| Material | • Service reduction/limited ability to deliver the service<br>• Harm to staff/volunteer/Service user<br>• Negative media/relationship impact<br>• Serious breach e.g. up to 1000 individuals/ special category data shared |
| Severe | • Lead to service closure or legal challenge<br>• Death to staff/volunteer/service users<br>• Prominent Negative Impact/ end relationship with major funder<br>• Financial impact – Fine potential<br>• Serious breach over 1000 individuals affected, potential for ID theft |

| **Step 5 Evaluation and response** | |
|---|---|
| **Action taken** | **To be completed by the Executive Committee** |
| Incident number | e.g. DB/year/001 |
| Report received by: | |
| On (date): | |
| Action taken by responsible officer/s: | |
| Was incident reported to police? | Yes/No<br>If YES, notified on (date): |
| Follow up action required/recommended:<br>The review will consider: | |

| | |
|---|---|
| • where and how personal data is held and where and how it is stored;<br>• where the biggest risks lie including identifying potential weak points within existing<br>• security measures;<br>• whether methods of transmission are secure; sharing minimum amount of data necessary;<br>• staff awareness;<br>• implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security | |
| Reported to the Board of Trustees on (date): | |
| Reported to other internal stakeholders (details, dates): | |
| For use of the LIO | |
| Notification to ICO | YES/NO If YES, notified on:<br>Details: |
| Notification to data subjects | YES/NO If YES, notified on:<br>Details: |
| Notification to other external, regulator/stakeholder | YES/NO If YES, notified on:<br>Details: |