Policy No: 03-1516	Authorised:	Date:05/02/2020

DATA BREACH POLICY
(GDPR)

This policy sets out the procedure to be followed to ensure a consistent and effective approach in place for managing a data breach and information security incidents within the Organisation. This policy relates to all personal and sensitive categories of data held by the Organisation, regardless of format:

POLICY IMPLEMENTATION:

1. Objectives and Scope:

1.1 The Organisation collects, holds, processes, and shares personal data. The Organisation acknowledges that such data is valuable and that every care must be taken to protect it from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

1.2 It is recognised that compromise of information, confidentiality, integrity, or availability could result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and / or financial costs or penalties.

1.3 The objective of this policy 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.

2. Definitions - *Data Security Breaches* and *Incidents:*

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

2.2 In the context of this policy, an **incident** 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 Organisation's information assets and / or reputation.

2.3 **A data security breach ("data breach")** includes, but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored; for example, loss of laptop, memory stick / flashdrive, tablet device, or paper records.
- Equipment theft or failure.
- System failure.
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s).
- Unauthorised use of, access to or modification of data or information systems.
- Unauthorised disclosure of sensitive / confidential data.
- Website defacement.
- IT hacking - "ransom" / virus / malware attack.
- Unforeseen circumstances, such as a fire or flood, leading to serious business interruption.
- "Blagging" offences where information is obtained by deceiving the organisation who holds it.
- Human error.

3. Reporting the Breach:

3.1 For the purposes of this Policy, the Managing Director is the Organisation's nominated Data Protection Officer (DPO).

3.2 Any person who accesses, uses or manages data within the Organisation is responsible for reporting a data breach and information security incidents immediately to the DPO. If the breach occurs or is discovered outside normal (day shift) working hours, it should be reported as soon as is practical.

3.3 Details of the breach will be recorded on a Data Breach Report Form *(Form No: 1-504)*, and will include the following information:

- full and accurate details of the breach;
- when the breach occurred (dates and times);
- the name of the person(s) reporting the breach;
- whether or not the data relates to people;
- the nature of the data breached.

4. Assessment and Investigation:

4.1 As a priority, the Data Protection Officer (DPO) will determine if the breach is still occurring, and if it is to take immediate action in order to contain its effect on the daily operations of the Care Service.

4.2 An initial assessment will be made by the DPO in coordination with the Domiciliary Care Manager or designate to establish the severity of the breach and to establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

4.3 The DPO will conduct an investigation within 24 hours of the breach being discovered. This will focus upon assessing the breach and the risks associated with it; for example, the potential adverse consequences for data subjects, how serious or substantial they may be, and how likely they are to occur. An investigation will consider the following:

- the type of data involved;
- sensitivity of data;
- safeguards that are installed; e.g. encryptions;
- what has happened to the data; e.g. lost, stolen etc;
- whether the data could be put to any illegal or inappropriate use;
- the data subjects affected by the breach;
- the number of data subjects involved;
- impact assessments on those data subjects;
- whether there are wider consequences to the breach;
- details of any action taken to contain the breach, and to minimise the risk of a recurrence.

5. Notifications:

5.1 The DPO, in consultation with Senior Management of the Service, will determine if the *Information Commissioner's Office* will need to be notified of the breach, and if so to notify them within 72 hours of becoming aware of the breach.

5.2 The following factors will be considered:

5.2.1 Whether the breach is likely to result in a high risk of adversely affecting the rights and freedoms of the data subjects under current Data Protection legislation;

5.2.2 Whether notification would assist the data subjects affected (e.g. could they act on the information to mitigate risks?);

5.2.3 Whether notification would help prevent the unauthorised or unlawful use of personal data;

5.2.4 Whether there are any legal or contractual notification requirements;

5.3 Data subjects whose personal data have been affected by the breach, 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 as a priority. 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 what action has already been taken to mitigate the risks.

5.4 Where illegal activity is believed to have occurred, or where there is a significant risk that illegal activity may occur in the future, the DPO and Senior Management will consider notifying interested third parties such as the police, insurance companies, banks or credit card companies as appropriate.

6. Corrective and Preventive Actions:

6.1 Once the initial breach 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 are indicated.

6.2 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.

6.3 The review will address the following:

- where and how personal data is collected, processed and stored;
- identifying potential risks 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.

FORMS REFERENCES:

Form No: 1-504 Data Breach Report