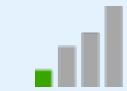
Digby Manor Residential Care Home
908 Chester Road, Erdington, Birmingham, West Midlands, B24 0BN

Review Sheet

Last Reviewed	Last Amended	Next Planned Review
28 Jun '23	28 Jun '23	in 12 months, or sooner as required.

Business impact	 **LOW IMPACT** Minimal action required circulate information amongst relevant parties.
Reason for this review	Scheduled review
Were changes made?	Yes
Summary:	This policy will support staff to understand and recognise a data breach. It has been reviewed with minor content changes and references checked and updated.
Relevant legislation:	• Data Protection Act 2018 • UK GDPR
Underpinning knowledge - What have we used to ensure that the policy is current:	• Author: ICO, (2021), *UK GDPR Data Breach Reporting (DPA 2018)*. [Online] Available from: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/ [Accessed: 28/6/2023] • Author: ICO, (2021), *Guide to the UK General Data Protection Regulation (UK GDPR)*. [Online] Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ [Accessed: 28/6/2023]
Suggested action:	• Encourage sharing the policy through the use of the QCS App
Equality Impact Assessment:	QCS have undertaken an equality analysis during the review of this policy. This statement is a written record that demonstrates that we have shown due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations with respect to the characteristics protected by equality law.

Digby Manor Residential Care Home
908 Chester Road, Erdington, Birmingham, West Midlands, B24 0BN

1. Purpose

1.1 To explain what a breach of UK GDPR means.
1.2 To ensure that all staff at Digby Manor Residential Care Home know how to recognise a breach or potential breach, and how to deal with it.
1.3 To support Digby Manor Residential Care Home in meeting the following Key Lines of Enquiry/Quality Statements (New):

Key Question	Key Lines of Enquiry	Quality Statements (New)
WELL-LED	W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?	QSW5: Governance, management and sustainability

1.4 To meet the legal requirements of the regulated activities that {Digby Manor Residential Care Home} is registered to provide:

- Data Protection Act 2018
- UK GDPR

2. Scope

2.1 The following roles may be affected by this policy:

- All staff at Digby Manor Residential Care Home who process personal data about other staff, Residents and other individuals.

2.2 The following Residents may be affected by this policy:

- Residents

2.3 The following stakeholders may be affected by this policy:

- Family
- Advocates
- Representatives
- Commissioners
- External health professionals
- Local Authority
- NHS

3. Objectives

3.1 This policy will assist with defining accountability and establishing ways of working in terms of Digby Manor Residential Care Home appropriately dealing with breaches of personal data and any notifications that need to be made as result of the breach (e.g. to the ICO and to affected data subjects).
3.2 To encourage UK GDPR compliance at Digby Manor Residential Care Home by ensuring that breaches of personal data (and "near misses") are dealt with appropriately by staff and by the Data Protection Officer at Digby Manor Residential Care Home.
3.3 This policy will facilitate the process of dealing with breaches of personal data to improve compliance at Digby Manor Residential Care Home. This will also benefit data subjects affected by a breach, including Residents.

4. Policy

4.1 Jane Farr will read and understand this policy and procedure together with the process map set out in the form attached, ensuring that they adhere to the process map if Digby Manor Residential Care Home becomes aware of a personal data breach.
4.2 Digby Manor Residential Care Home acknowledges that if their processes differ from those set out in this policy, they must modify them to reflect their own processes and procedures.
4.3 Digby Manor Residential Care Home understands that if a personal data breach occurs then it may be required to notify the ICO as well as the data subjects who have been affected by the breach.
Digby Manor Residential Care Home recognises that failure to report a personal data breach may result in significant fines being imposed, as well as reputational damage.
4.4 Digby Manor Residential Care Home recognises that it is reliant on its employees notifying Jane Farr if they become aware of a personal data breach or suspect a personal data breach.
Digby Manor Residential Care Home must encourage all of its staff to review the policy and understand their obligations in terms of reporting a personal data breach to Jane Farr who is the Data Protection Officer.
4.5 What is a Breach?
A personal data breach is any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Personal data breaches can be either accidental or deliberate acts and can be carried out by third parties. Examples of a breach may include:

- Sending an email to the incorrect recipient
- Copying rather than blind copying recipients of an email
- Losing a USB device containing personal data
- Leaving a hard copy of personal data (e.g. a Resident record or employee file) in an easily accessible area so that details can be viewed or recorded, or the document taken
- Leaving a laptop or documents containing personal data on a train or other public transport
- Leaving a cupboard or filing drawer unlocked that contains personal data
- Altering personal data without consent/permission to do so, or
- Loss of availability/access to personal data

Digby Manor Residential Care Home recognises that the above list is by way of example only and is not exhaustive or definitive.
4.6 Digby Manor Residential Care Home must ensure that its staff members understand that if they become aware of or suspect a personal data breach they must immediately notify Jane Farr, who will determine the next steps to take.
Digby Manor Residential Care Home understands that, once its employees are aware of a personal data breach of UK GDPR, they have a 72-hour timescale for notifying the ICO.

5. Procedure

5.1 Process Map: Stage 1 - Log breach

- Digby Manor Residential Care Home understands that it must maintain a log of all breaches irrespective of whether it requires notification to the ICO. They must also record any potential breaches notified by employees or third parties
- Digby Manor Residential Care Home will record the date of the breach, the date of notification of the breach (i.e. by the relevant employee), the facts regarding the breach and actions taken in respect of the breach, using the process map attached to this policy
- If it is decided there has not been a breach, the rationale must be explained on how this decision was reached

5.2 Stage 2 and 2a - Has the breach resulted in the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data?

Digby Manor Residential Care Home recognises that not every breach of UK GDPR must be notified to the ICO. For example, there is no requirement to notify the ICO of a failure to respond to a Subject Access Request.

Digby Manor Residential Care Home understands that the notification requirements focus on the loss of, or unauthorised access to, personal data, as described earlier in this policy. Digby Manor Residential Care Home will therefore consider:

- Whether personal data has been affected by the breach (if, for example, only business data has been disclosed then Digby Manor Residential Care Home understands that UK GDPR will not apply and there will be no requirement to notify the ICO); and
- Whether the personal data has been destroyed, lost, altered, disclosed or accessed as a result of the breach

Digby Manor Residential Care Home will record information about the breach and decisions taken for future reference. If there has been a security breach (irrespective of whether it requires notification to the ICO), Digby Manor Residential Care Home will consider whether, from a best practice perspective, it will proceed with Stages 4 and 5 to identify the cause of the breach and whether further steps can be taken to prevent further loss and disclosure of data (whether the data is personal data or otherwise).

5.3 Stage 3 - Identify the relevant team to investigate

Digby Manor Residential Care Home recognises that more than one team or individual may need to be involved or lead the investigation into the breach, and it will ensure that the appropriate people are involved at an early stage in the process.

5.4 Stage 4 - Identify the cause of the breach and whether the breach has been contained

Refer to further information at Stage 5.

5.5 Stage 5 - Take all steps necessary to prevent further loss/disclosure

Digby Manor Residential Care Home understands that the ICO must be notified within 72 hours of becoming aware of the breach.

Digby Manor Residential Care Home understands that it will be deemed to be "aware" of a breach when it has a reasonable degree of certainty that a security incident has occurred that may have led to a breach of personal data.

Digby Manor Residential Care Home recognises the importance of taking prompt action to investigate an incident and ensuring that any breach is contained to prevent it worsening prior to notification.

Digby Manor Residential Care Home will, where possible, notify the ICO in its initial notification of the steps it has already taken to mitigate the impact of the breach and will record all actions it has taken.

5.6 Stage 6 - Identifying if the breach is likely to result in a risk to the rights and freedoms of individuals

Digby Manor Residential Care Home understands that the ICO must be notified of the breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. Digby Manor Residential Care Home recognises that guidance provided by the ICO explains that a breach is likely to result in a risk to the rights and freedoms of individuals if, left unaddressed, it is likely to have a significant detrimental effect on individuals in terms of, for example, discrimination against that individual, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Digby Manor Residential Care Home recognises that if the lost data is business personal data (i.e.

individuals' work email addresses or phone numbers), it is unlikely that such loss will result in a risk to the rights and freedoms of those individuals, particularly if the information is publicly available elsewhere.
If Digby Manor Residential Care Home decides that a personal data breach is unlikely to result in a risk to the rights and freedoms of individuals, and does not report a breach to the ICO, they must be able to justify this and as such should document the decision.

5.7 Stage 6a - No need to take further action if response to Stage 6 is negative

Although Digby Manor Residential Care Home may not be required to notify the ICO if there is no risk to the rights and freedoms of individuals, it must take steps to avoid a similar breach occurring in the future, particularly if a similar breach in the future may result in a risk to the rights and freedoms of individuals – see Stage 10.

5.8 Stage 7 – Within 72 hours of becoming aware of the data breach, notify the ICO

Digby Manor Residential Care Home acknowledges that the ICO has provided a helpline and a notification template for reporting breaches under the Data Protection Act 2018 that must be notified to the ICO, a link to this information can be located in the Underpinning Knowledge section of this policy.
Digby Manor Residential Care Home will ensure that any breach notification it submits includes:

- The nature of each breach, including the categories and approximate numbers of individuals concerned and the categories and approximate numbers of personal data records concerned
- The name and contact details of the Data Protection Officer/point of contact for the breach
- A description of the likely consequences of the breach; and
- A description of measures taken or proposed to be taken to deal with the breach and any measures taken to mitigate effects of the breach

5.9 Stage 8 - Consider whether affected individuals should be notified

Digby Manor Residential Care Home understands that if the breach is likely to result in a "high" risk to the rights and freedoms of individuals, those individuals must be notified directly.
Digby Manor Residential Care Home recognises that the threshold is higher than the threshold for notifying the ICO and Digby Manor Residential Care Home will need to assess the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurs (this will be determined on a case-by-case basis). Examples of breaches that may need to be notified to individuals include loss or disclosure of special categories of personal data, or the potential for significant financial impact.
If Digby Manor Residential Care Home is unable to notify affected data subjects individually (because, for example, of the number of data subjects affected), it will take out a public notice, e.g. in a national newspaper, informing affected individuals of the breach.
If Digby Manor Residential Care Home decides they do not need to notify the individual of the breach they may still need to notify the ICO, each of these notifications should be considered separately, and Digby Manor Residential Care Home must make a record of the decision-making process.

5.10 Stages 9 and 9a - Notify data controller

If Digby Manor Residential Care Home is acting as a data processor rather than a data controller, they will notify the relevant data controller of the breach. Digby Manor Residential Care Home will, if necessary, refer to the guidance note entitled "GDPR - Key Terms" for further information.

5.11 Stage 10 - Check if there is a risk of a future breach occurring

Digby Manor Residential Care Home will have taken all possible steps to mitigate the effect of the breach in accordance with Stage 5 above.
Digby Manor Residential Care Home will also consider the breach more widely, in particular whether the breach may occur again and take the steps necessary to prevent such recurrence.

5.12 Stage 11 - Consider whether further internal training or guidance for staff is necessary

If the breach was caused by a member of staff, Digby Manor Residential Care Home will consider how and why the breach happened. Digby Manor Residential Care Home will consider whether further training or guidance would be beneficial, either for the member of staff or for Digby Manor Residential Care Home more widely.

5.13 Stage 12 - Log all actions and decisions

Digby Manor Residential Care Home will document all decisions taken in respect of any breaches, including whether or not to notify the ICO and/or affected individuals, steps taken to mitigate the breach and steps taken to prevent future recurrence and additional training. Digby Manor Residential Care Home will keep a record of all relevant dates and copies of relevant documents such as the initial report from the relevant member of staff and the notification to the ICO.

5.14 Stage 13 - Action and log any related future correspondence from the ICO

Digby Manor Residential Care Home will record any correspondence it receives from the ICO in respect of breaches and comply with any suggestions and requirements of the ICO.

6. Definitions

6.1 UK GDPR

- The UK GDPR is the retained EU law version of GDPR that forms part of English law

6.2 ICO

- The Information Commissioner's Office
- Upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals

6.3 Special Categories of Data

- A term for personal data that is sensitive and personal in nature
- Special categories of data include but are not limited to:
  - Medical and health records and Care Plans (including information collected as a result of providing health care services), generic and biometric data; and
  - Information about a person's religious beliefs, ethnic origin and race, sexual orientation, trade union membership and political views

6.4 Process or Processing

- Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending or transferring it. An organisation does not need to be doing anything actively with the personal data - at the point it collects it, it is processing it

6.5 Data Subject

- The identified or identifiable individual about whom Digby Manor Residential Care Home has collected personal data

6.6 Data Protection Act 2018

- The Data Protection Act 2018 is a United Kingdom Act of Parliament that updates data protection laws in the UK. It sits alongside the UK GDPR and implements the EU's Law Enforcement Directive

6.7 Personal Data

- Any information about a living person from which that person can be identified directly or indirectly, including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV, online identifiers, and special categories of data, defined below

Key Facts - Professionals

Professionals providing this service should be aware of the following:

- All staff at Digby Manor Residential Care Home will follow the guidelines set out in this policy to ensure that breaches are dealt with appropriately and in compliance with UK GDPR

Key Facts - People affected by the service

People affected by this service should be aware of the following:

- Digby Manor Residential Care Home has processes in place to ensure that any breaches of personal data are appropriately dealt with and the risk to the relevant data subject (including Residents) is mitigated

Digby Manor Residential Care Home
908 Chester Road, Erdington, Birmingham, West Midlands, B24 0BN

Further Reading

As well as the information in the 'underpinning knowledge' section of the review sheet we recommend that you add to your understanding in this policy area by considering the following materials:

NHS England - Transformation Directorate - Personal Data Breaches:
https://www.nhsx.nhs.uk/information-governance/guidance/personal-data-breaches/
NHS Digital - Data Security and Protection Toolkit:
https://www.dsptoolkit.nhs.uk/

Outstanding Practice

To be ' outstanding ' in this policy area you could provide evidence that:

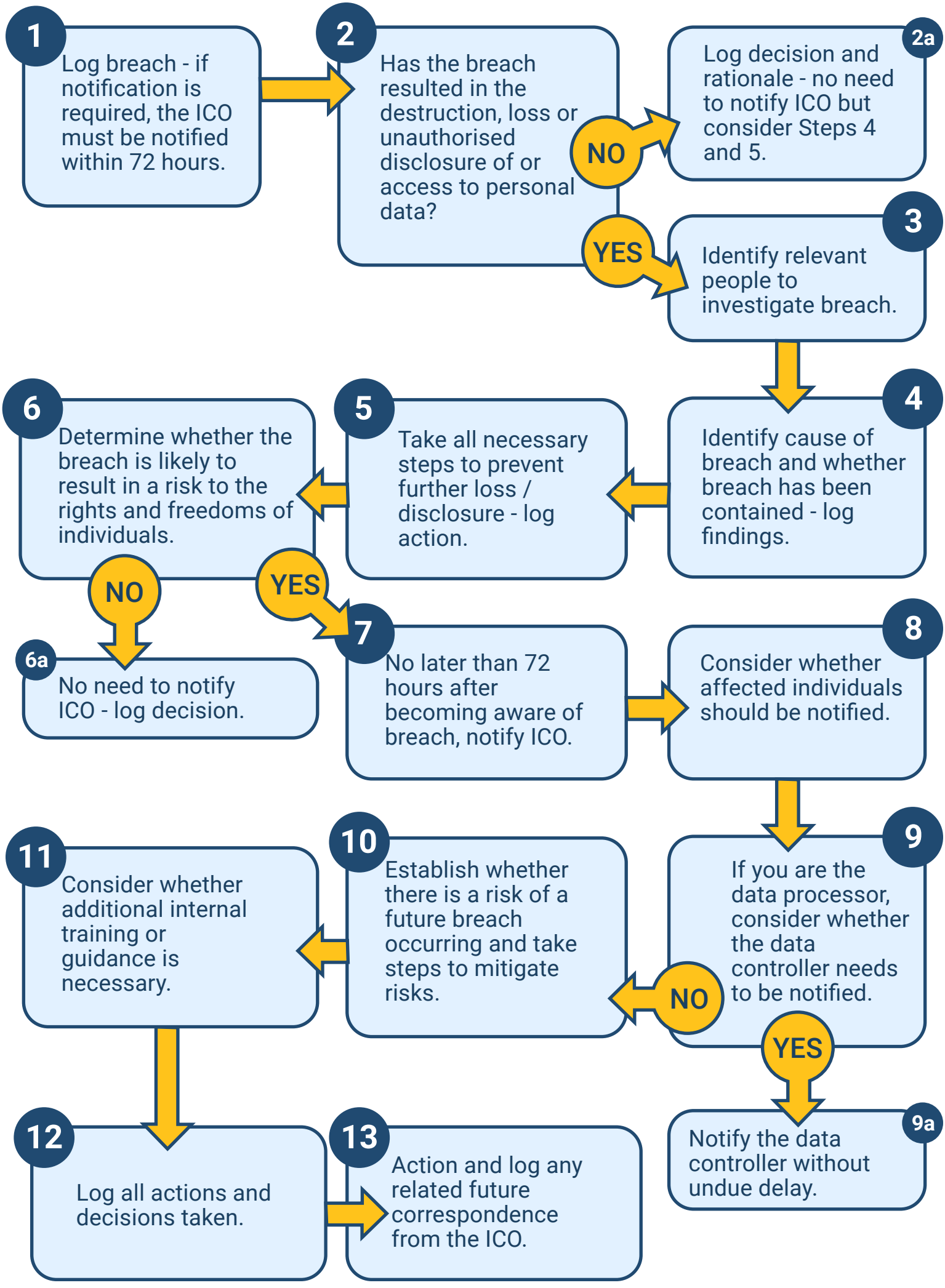
- Digby Manor Residential Care Home has created a detailed log for breaches and the steps taken in respect of those breaches
- Digby Manor Residential Care Home provides training to all staff to ensure that they understand how to deal with a breach or potential breach of UK GDPR
- The wide understanding of the policy is enabled by proactive use of the QCS App
- Procedures at Digby Manor Residential Care Home and embedding of UK GDPR has meant that there have been no breaches
- Digby Manor Residential Care Home shares understanding and knowledge with other organisations and is seen as a beacon of good practice in regard to data protection

Forms

The following forms are included as part of this policy:

Title of form	When would the form be used?	Created by
Breach Notification Process Map - GDPR06	The process map must be followed by the Data Protection Officer (or other person with responsibility for data protection and UK GDPR compliance) each time a breach of UK GDPR or a "near miss" occurs.	QCS
Data Breach Log - GDPR06	This form should be used when there has been a breach of data within the service.	QCS

Breach Notification Process Map



Digby Manor Residential Care Home
908 Chester Road, Erdington, Birmingham, West Midlands, B24 0BN

ICO Notification Type/Timescales	Date	Time	Sent By
Initial notification of a security breach (within 24 hrs)			
Second notification with further detail (within 3 days)			
Follow-up notification with outstanding details			
Has all the information asked for by the ICO been provided?		Yes	No
Has a lesson learnt exercise been carried out following this breach?		Yes	No

Notification to other data protection authorities / Regulatory Bodies (if so, which ones)?	Date	Time	Sent By

(continued on next page)

Digby Manor Residential Care Home
908 Chester Road, Erdington, Birmingham, West Midlands, B24 0BN

Data Breach Event			
When did the breach occur?	On	Or Between	
Time, if known?			
When was the breach first detected?			
Breach detected by?			
How many individuals were affected?			
Did the breach occur in response to a Regulation of Investigatory Powers Act request?		Yes	No
Summary of the incident that caused the breach?			
Briefly describe the breach (e.g. theft, loss, copying)			

(continued on next page)

Digby Manor Residential Care Home
908 Chester Road, Erdington, Birmingham, West Midlands, B24 0BN

What was the physical location of the breach and the storage media involved?		
What is the nature and content of the personal data concerned?		
What technical and organisational security measures have been applied (or were to be applied) to the affected personal data?		
Were other providers involved? If so, who?	Yes	No
What are the potential consequences and adverse effects on those individuals?		
What technical and organisational measures have been taken to mitigate any potential adverse effects?		
Copy of any Breach Notification sent to those affected is attached?	Yes	No

How were customers notified (circle)? If other, specify:					
Email	Letter	Text	Phone call	Other:	
How many customers were notified in total?					

Completed By:		**Signed:**	
Position:		**Date:**	
Organisation:			
ICO Registration:			