

|  |
| --- |
|  **Review Sheet** |
| Last Reviewed Last Amended Next Planned Review in 12 months, or15 Jan '20 15 Jan '20 sooner as required. |
| Business impact | Changes are important, but urgent implementation is not required, incorporate into your existing workflow.**MEDIUM IMPACT** |
| Reason for this review | Scheduled review |
| Were changes made? | Yes |
| Summary: | This policy supports how to recognise a breach or potential breach and how this must be dealt with. It has been reviewed with an expansion of the explanation of when an organisation becomes aware of a breach, which is in line with recent guidance. References have also been checked to ensure they remain current. |
| Relevant legislation: | * General Data Protection Regulation 2016
* Data Protection Act 2018
 |
| Underpinning knowledge - What have we used to ensure that the policy is current: | * Author: Information Commissioner's Office, (2018), *Data breach reporting*. [Online] Available from: [https://ico.org.uk/for-organisations/report-a-breach/personal-data- breach/](https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/) [Accessed: 15/1/2020]
* Author: UK Government, (2018), *Guide to the General Data Protection Regulation*. [Online] Available from: [https://www.gov.uk/government/publications/guide-to-the- general-data-protection-regulation](https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation) [Accessed: 15/1/2020]
 |
| Suggested action: | * Encourage sharing the policy through the use of the QCS App
* Ensure the policy is discussed in planned supervision sessions with relevant staff
* Ensure relevant staff are aware of the content of the whole policy
 |
| 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. |

**1. Purpose**

* 1. To explain what a breach of GDPR may consist of and to ensure that all staff at Holbeach Hospital & Nursing Home know how to recognise a breach or potential breach, and how they will deal with it.
	2. To support Holbeach Hospital & Nursing Home in meeting the following Key Lines of Enquiry:

## Key Question Key Lines of Enquiry

W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?

WELL-LED

* 1. To meet the legal requirements of the regulated activities that Holbeach Hospital & Nursing Home is registered to provide:
		+ General Data Protection Regulation 2016
		+ Data Protection Act 2018

**2. Scope**

* 1. The following roles may be affected by this policy:
		+ All staff at Holbeach Hospital & Nursing Home who process personal data about other staff, Service Users and other individuals.
	2. The following Service Users may be affected by this policy:
		+ Service Users
	3. The following stakeholders may be affected by this policy:
		+ Family
		+ Advocates
		+ Representatives
		+ Commissioners
		+ External health professionals
		+ Local Authority
		+ NHS

**3. Objectives**

* 1. This policy will assist with defining accountability and establishing ways of working in terms of Holbeach Hospital & Nursing Home appropriately dealing with breaches of GDPR and any notifications that need to be made as result of the breach (e.g. to the ICO and to affected Data Subjects).
	2. This policy will encourage GDPR compliance at Holbeach Hospital & Nursing Home by ensuring that breaches of GDPR (and "near misses") are dealt with appropriately by staff and by the Trustee and Financial Director at Holbeach Hospital & Nursing Home.
	3. This policy will facilitate the process of dealing with breaches of GDPR which will improve the compliance of Holbeach Hospital & Nursing Home with GDPR and will also benefit Data Subjects affected by a breach, including Service Users.

**4. Policy**

* 1. The Trustee and Financial Director, Michael Brett at Holbeach Hospital & Nursing Home will read and understand this policy and procedure together with the process map set out in the form attached, and will ensure that they adhere to the process map if Holbeach Hospital & Nursing Home breaches GDPR.
	2. Holbeach Hospital & Nursing Home acknowledges that if its processes differ from those set out in this policy, it will modify them to the extent necessary to reflect its processes and procedures.
	3. Holbeach Hospital & Nursing Home understands that if it breaches GDPR, it may be required to notify the ICO as well as the Data Subjects who have been affected by the breach. Holbeach Hospital & Nursing Home recognises that failure to report a breach may result in significant fines being imposed on Holbeach Hospital & Nursing Home, as well as reputational damage.
	4. Holbeach Hospital & Nursing Home recognises that it is reliant on its employees notifying Michael Brett if they breach or think they may have breached GDPR. Holbeach Hospital & Nursing Home will therefore encourage all of its staff to review the policy and understand their obligations in terms of reporting a breach to Michael Brett who is the Trustee and Financial Director.

## What is a Breach?

A breach of GDPR is any breach of security that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

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 Service User 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

Holbeach Hospital & Nursing Home recognises that the above list is by way of example only and is not exhaustive or definitive.

* 1. Holbeach Hospital & Nursing Home will ensure that its staff members understand that if they breach or think they may have breached GDPR, they must immediately notify Michael Brett, Trustee and Financial Director, who will determine the next steps to take. Holbeach Hospital & Nursing Home understands that, once its employees are aware of a breach of GDPR, Holbeach Hospital & Nursing Home is deemed to be aware of the breach, at which point the 72-hour timescale for notifying the ICO will begin.

**5. Procedure**

## Process Map: Stage 1 - Log breach

* + - Holbeach Hospital & Nursing Home understands that it must maintain a log of breaches. Holbeach Hospital & Nursing Home will also record any potential breaches notified to it by employees or third parties which it determines not to be a breach, setting out its rationale for such a decision
		- Holbeach Hospital & Nursing Home will record the date of the breach, the date of notification of the breach (i.e. by the relevant employee) and actions taken in respect of the breach, using the process map attached to this policy

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

Holbeach Hospital & Nursing Home recognises that not every breach of 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. Holbeach Hospital & Nursing Home understands that the notification requirements focus on the loss of, or unauthorised access to, personal data. Holbeach Hospital & Nursing Home will therefore consider:

* + - Whether personal data has been affected by the breach (if, for example, only business data has been disclosed then Holbeach Hospital & Nursing Home understands that GDPR will not apply and there will be no requirement to notify the ICO)
		- Whether the personal data has been destroyed, lost, altered, disclosed or accessed as a result of the breach

Holbeach Hospital & Nursing 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), Holbeach Hospital & Nursing 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).

## Stage 3 - Identify the relevant team to investigate

Holbeach Hospital & Nursing Home anticipates 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.

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

Refer to further information at Stage 5.

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

Holbeach Hospital & Nursing Home understands that the ICO must be notified within 72 hours of becoming aware of the breach. Holbeach Hospital & Nursing 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 the unlawful disclosure, use etc. of Personal Data. Holbeach Hospital & Nursing 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. Holbeach Hospital & Nursing 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.

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

Holbeach Hospital & Nursing 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. Holbeach Hospital & Nursing 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.

Holbeach Hospital & Nursing 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.

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

Although Holbeach Hospital & Nursing 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.

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

Holbeach Hospital & Nursing Home acknowledges that the ICO has provided a notification template for serious breaches under the Data Protection Act 2018 that must be notified to the ICO, a link to which can be located within the Further Reading section of this policy.

Holbeach Hospital & Nursing 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 Privacy 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

## Stage 8 - Consider whether affected individuals should be notified

Holbeach Hospital & Nursing 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.

Holbeach Hospital & Nursing Home recognises that the threshold is higher than the threshold for notifying the ICO. It will be determined on a case-by-case basis. Examples may be loss or disclosure of Special Categories of Personal Data, or the potential for significant financial impact.

If Holbeach Hospital & Nursing 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.

## Stages 9 and 9a - Notify data controller

If Holbeach Hospital & Nursing Home is acting as a data processor rather than a data controller, it will notify the relevant data controller of the breach. Holbeach Hospital & Nursing Home will, if necessary, refer to the guidance note entitled "GDPR - Key Terms" for further information.

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

Holbeach Hospital & Nursing Home will have taken all possible steps to mitigate the effect of the breach in accordance with Stage 5 above. Holbeach Hospital & Nursing 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.

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

If the breach was caused by a member of staff, Holbeach Hospital & Nursing Home will consider how and why the breach happened. Holbeach Hospital & Nursing Home will consider whether further training or guidance would be beneficial, either for the member of staff or for Holbeach Hospital & Nursing Home more widely.

## Stage 12 - Log all actions and decisions

Holbeach Hospital & Nursing 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. Holbeach Hospital & Nursing 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.

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

Holbeach Hospital & Nursing 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**

## 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 General Data Protection Regulation and implements the EU's Law Enforcement Directive

## Data Subject

* + - The individual about whom Holbeach Hospital & Nursing Home has collected personal data

## GDPR

* + - General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It became enforceable on 25 May 2018

## Personal Data

* + - Any information that identifies a living person including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV and Special Categories of Data, defined below

## 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

## Special Categories of Data

* + - Has an equivalent meaning to “Sensitive Personal Data” under the Data Protection Act 2018. 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)
			* Information about a person’s religious beliefs, ethnic origin and race, sexual orientation and political views

**Key Facts - Professionals**

Professionals providing this service should be aware of the following:

* + - All staff at Holbeach Hospital & Nursing Home will follow the guidelines set out in this policy to ensure that breaches are dealt with appropriately and in compliance with GDPR

**Key Facts - People affected by the service**

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

* + - Holbeach Hospital & Nursing Home has processes in place to ensure that any breaches of GDPR are appropriately dealt with and the risk to the relevant Data Subject (including Service Users) is mitigated

**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:

## ICO Notification Online Template:

<https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>

**Outstanding Practice**

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

* + - The wide understanding of the policy is enabled by proactive use of the QCS App
		- Holbeach Hospital & Nursing Home has created a detailed log for breaches and the steps taken in respect of those breaches
		- Holbeach Hospital & Nursing Home provides training to all staff to ensure that they understand how to deal with a breach or potential breach of GDPR
		- Procedures at Holbeach Hospital & Nursing Home and embedding of GDPR has meant that there have been no breaches
		- Holbeach Hospital & Nursing 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** |
|  | The process map must be |  |
|  | followed by the Data Protection |  |
| Breach Notification Process Map- GDPR06 | Officer (or other person with responsibility for data protection and GDPR compliance) each | QCS |
|  | time a breach of GDPR or a |  |
|  | "near miss" occurs. |  |

**Breach Notiﬁcation Process Map**

# 1

Log breach - if notiﬁcation is required, the ICO must be notiﬁed within 72 hours.

**2**

Has the breach resulted in the destruction, loss or unauthorised disclosure of or access to personal data?

NO YES

Log decision and **2a**

rationale - no need to notify ICO but consider Steps 4

and 5.

**3**

Identify relevant people to investigate breach.

**6**

Determine whether the

**5**

Take all necessary

**4**

Identify cause of

breach is likely to result in a risk to the rights and freedoms of individuals.

NO YES

**6a**

No need to notify ICO - log decision.

steps to prevent further loss / disclosure - log action.

**7**

No later than 72 hours after becoming aware of breach, notify ICO.

breach and whether breach has been contained - log ﬁndings.

**8**

Consider whether affected individuals should be notiﬁed.

**11**

Consider whether

additional internal

**10**

Establish whether there is a risk of a

**9**

If you are the data processor,

training or guidance is necessary.

future breach occurring and take steps to mitigate risks.

consider whether the data controller needs

NO to be notiﬁed.

YES

**12**

Log all actions and decisions taken.

**13**

Action and log any related future correspondence from the ICO.

Notify the data **9a** controller without undue delay.