Pol Community Care Ltd
Office 2, Caradon Enterprise Centre, 1 Holman Road, Liskeard Business Park, Liskeard, Cornwall, PL14 3UT

Review Sheet

Last Reviewed	Last Amended	Next Planned Review
15 Jan '20	15 Jan '20	in 12 months, or sooner as required.

Business impact	**MEDIUM IMPACT** Changes are important, but urgent implementation is not required, incorporate into your existing workflow.
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/ [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 [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.

Pol Community Care Ltd
Office 2, Caradon Enterprise Centre, 1 Holman Road, Liskeard Business Park, Liskeard, Cornwall, PL14 3UT

1. Purpose

1.1 To explain what a breach of GDPR may consist of and to ensure that all staff at Pol Community Care Ltd know how to recognise a breach or potential breach, and how they will deal with it.
1.2 To support Pol Community Care Ltd in meeting the following Key Lines of Enquiry:

Key Question	Key Lines of Enquiry
WELL-LED	W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?

1.3 To meet the legal requirements of the regulated activities that Pol Community Care Ltd is registered to provide:

- General Data Protection Regulation 2016
- Data Protection Act 2018

2. Scope

2.1 The following roles may be affected by this policy:

- All staff at Pol Community Care Ltd who process personal data about other staff, Service Users and other individuals.

2.2 The following Service Users may be affected by this policy:

- Service Users

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 Pol Community Care Ltd 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).
3.2 This policy will encourage GDPR compliance at Pol Community Care Ltd by ensuring that breaches of GDPR (and "near misses") are dealt with appropriately by staff and by the Data Protection Officer at Pol Community Care Ltd.
3.3 This policy will facilitate the process of dealing with breaches of GDPR which will improve the compliance of Pol Community Care Ltd with GDPR and will also benefit Data Subjects affected by a breach, including Service Users.

4. Policy

4.1 The Data Protection Officer, Miss Rebecca Russell at Pol Community Care Ltd 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 Pol Community Care Ltd breaches GDPR.
4.2 Pol Community Care Ltd 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.
4.3 Pol Community Care Ltd 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. Pol Community Care Ltd recognises that failure to report a breach may result in significant fines being imposed on Pol Community Care Ltd, as well as reputational damage.
4.4 Pol Community Care Ltd recognises that it is reliant on its employees notifying Miss Rebecca Russell if they breach or think they may have breached GDPR. Pol Community Care Ltd will therefore encourage all of its staff to review the policy and understand their obligations in terms of reporting a breach to Miss Rebecca Russell who is the Data Protection Officer.
4.5 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

Pol Community Care Ltd recognises that the above list is by way of example only and is not exhaustive or definitive.
4.6 Pol Community Care Ltd will ensure that its staff members understand that if they breach or think they may have breached GDPR, they must immediately notify Miss Rebecca Russell, Data Protection Officer, who will determine the next steps to take. Pol Community Care Ltd understands that, once its employees are aware of a breach of GDPR, Pol Community Care Ltd is deemed to be aware of the breach, at which point the 72-hour timescale for notifying the ICO will begin.

5. Procedure

5.1 Process Map: Stage 1 - Log breach

- Pol Community Care Ltd understands that it must maintain a log of breaches. Pol Community Care Ltd 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
- Pol Community Care Ltd 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

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

Pol Community Care Ltd 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. Pol Community Care Ltd understands that the notification requirements focus on the loss of, or unauthorised access to, personal data. Pol Community Care Ltd will therefore consider:

- Whether personal data has been affected by the breach (if, for example, only business data has been disclosed then Pol Community Care Ltd 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

Pol Community Care Ltd 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), Pol Community Care Ltd 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

Pol Community Care Ltd 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.

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

Pol Community Care Ltd understands that the ICO must be notified within 72 hours of becoming aware of the breach. Pol Community Care Ltd 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. Pol Community Care Ltd 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. Pol Community Care Ltd 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

Pol Community Care Ltd 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. Pol Community Care Ltd 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.

Pol Community Care Ltd 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.

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

Although Pol Community Care Ltd 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 breach, notify the ICO

Pol Community Care Ltd 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.

Pol Community Care Ltd 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

5.9 Stage 8 - Consider whether affected individuals should be notified

Pol Community Care Ltd 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.

Pol Community Care Ltd 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 Pol Community Care Ltd 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.

5.10 Stages 9 and 9a - Notify data controller

If Pol Community Care Ltd is acting as a data processor rather than a data controller, it will notify the relevant data controller of the breach. Pol Community Care Ltd 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

Pol Community Care Ltd will have taken all possible steps to mitigate the effect of the breach in accordance with Stage 5 above. Pol Community Care Ltd 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, Pol Community Care Ltd will consider how and why the breach happened. Pol Community Care Ltd will consider whether further training or guidance would be beneficial, either for the member of staff or for Pol Community Care Ltd more widely.

5.13 Stage 12 - Log all actions and decisions

Pol Community Care Ltd 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. Pol Community Care Ltd 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

Pol Community Care Ltd 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 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

6.2 Data Subject

- The individual about whom Pol Community Care Ltd has collected personal data

6.3 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

6.4 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

6.5 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

6.6 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 Pol Community Care Ltd 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:

- Pol Community Care Ltd 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/

Pol Community Care Ltd
Office 2, Caradon Enterprise Centre, 1 Holman Road, Liskeard Business Park, Liskeard, Cornwall, PL14 3UT

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
- Pol Community Care Ltd has created a detailed log for breaches and the steps taken in respect of those breaches
- Pol Community Care Ltd provides training to all staff to ensure that they understand how to deal with a breach or potential breach of GDPR
- Procedures at Pol Community Care Ltd and embedding of GDPR has meant that there have been no breaches
- Pol Community Care Ltd 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 GDPR compliance) each time a breach of GDPR or a "near miss" occurs.	QCS

Breach Notification Process Map