

Barth Syndrome UK Data Breach Policy

Reviewed: **04.11.2019 / 02.12.2020 / 02.12.2021 / 15.03.2023 / 23.03.2024**

Next Review Date: 23.03.2025

1 Introduction

- 1.1 The Data Protection Act 2018 (DPA) is based around six principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations upon organisations that are responsible for processing it. An overview of the main provisions of DPA can be found in The Guide to Data Protection:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>
- 1.2 Occasionally things will go wrong and mistakes will be made. Sometimes this may entail significant financial or reputational risk for charities. It is vital that we can identify, evaluate and contain data breaches as soon as they occur.
- 1.3 Consistent governance and control arrangements are also a regulatory requirement. Where a breach has occurred and/or where you have failed to mitigate the impact quickly, the Information Commissioner (ICO) may intervene and may use its powers to issue a substantial fine.
- 1.4 Identifying data breaches quickly and effectively to limit any impact is critical to our success. Equally we need to understand where there are areas of weakness within our operating processes and continuously improve to reduce the risk of significant control failures leading to data breaches.
- 1.5 This policy meets the guidance provided by the ICO on data security breach management.

2 Aims and objectives

- 2.1 This policy sets out: -

Policy statement on data breaches.

Definitions.

Reporting responsibilities.

- 2.2 This policy aims to ensure that adequate controls are in place so that: -

Data breaches are identified and action is taken quickly. Actions should be proportionate, consistent and transparent.

An assessment is completed to ensure that any major data breaches are reported to the Chairperson or other Trustee or member of staff.

All data breaches and near misses are recorded and regularly reported.

Lessons are learned to ensure similar mistakes are not repeated and appropriate control mechanisms are put in place.

3 Policy Statement

- 3.1 This policy is in place to raise awareness of data breach cases and to ensure that all staff, trustees and volunteers can identify a case and understand the steps required for dealing with it.
- 3.2 This policy identifies inherent risk of a data breach and/or near-miss, which will ensure that appropriate staff or trustees are informed, able to manage actions relating to any real or potential serious data breach and be in a position to report to the ICO and affected individuals as appropriate.

4 Definitions

4.1 What is a data breach?

- 4.1.1 According to the ICO, organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.
- 4.1.2 A data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.
- 4.1.3 A personal data breach may mean that someone outside the organisation gets unauthorised access to personal and/or special category (sensitive) data. But a personal data breach can also occur if there is unauthorised access within the organisation, for example where someone accidentally or deliberately alters or deletes personal data.
- 4.1.4 A data security breach can happen for many reasons:
- Loss or theft of data or equipment on which data is stored
 - Inappropriate access controls allowing unauthorised use
 - Equipment failure
 - Human error
 - Unforeseen circumstances such as a fire or flood
 - Hacking attack
 - ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.
- 4.1.5 Human error is the most common cause of data breaches. These can happen for many reasons:
- Theft or loss of paperwork
 - Data posted to incorrect recipient
 - Data sent by email to incorrect recipient
 - Failure to redact personal/sensitive data.

4.2 What is a near miss?

- 4.2.1 A near miss is an event that does not result in a data breach, but which had the potential to do so.
Examples of such events might include data that was misplaced but found quickly internally or data that was sent out but was identified and returned.
- 4.2.2 We will record all near misses in order to understand patterns, learn lessons and implement improvements.

5 Training

- 5.1 Training will be offered to all staff and key volunteers/trustees on data protection regulations.
- 5.2 Training will be offered to all new employees including temporary and contracted staff.
- 5.3 All employees will be offered refresher training annually.

6 Identification

- 6.1 Where a data breach is identified, the Chair of the organisation must be informed immediately. The Chair will investigate the occurrence and complete a risk assessment to determine the notification requirements.
- 6.2 The controls in place must be reviewed. Where no controls are in place, consideration must be given to introducing them. Was this an exceptional case that could not have reasonably been avoided, or does action need to be taken to avoid a recurrence?

7 Risk Assessments

- 7.1 When a data breach is identified, a risk assessment should be completed.
- 7.2 Depending on the risk assessment, the data breach will be reported to, owned and investigated at the specified levels within the organisation.

NOTE: The relevant data breach owner should be notified immediately that a data breach has been identified or as a minimum within the timescales set out. This is a mandatory requirement.

8 Containment & Recovery

- 8.1 Containment and recovery involve limiting the scope and impact of the data breach, and stemming it as quickly as possible.
- 8.2 The data breach owner must quickly take appropriate steps to ascertain full details of the breach, determine whether the breach is still occurring, recover any losses and limit the damage. Steps might include: -
- Attempting to recover any lost equipment or personal information.
 - Shutting down an IT system.

- Contacting other key departments so that they are prepared for any potentially inappropriate enquiries about the affected data subjects.
- The risk owner organising, with the approval of the Chair, for an organisation-wide email to be sent.
- Putting in place a plan to handle any press enquiries or to make any press releases.
- The use of back-ups to restore lost, damaged or stolen information.
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant organisations and members of staff informed.

9 Investigation

9.1 If a data breach is identified, then a formal investigation should be commenced by the data breach owner who should determine the seriousness of the breach and the risks arising from it. Specifically, the data breach owner should identify:-

- Whose information was involved in the breach?
- What went wrong?
- The potential effect on the data subject(s)?
- What immediate steps are required to remedy the situation?
- What lessons have been learnt to avoid a repeat incident?

In order to support this process, the data breach owner should complete the Data Breach Report form.

9.2 The investigation should consider: -

- The type of information.
- Its sensitivity.
- How many individuals are affected by the breach?
- What protections are in place (e.g., encryption)?
- What happened to the information?
- Whether the information could be put to any illegal or inappropriate use.
- What could the information tell a third party about the individual?
- How many people are affected?
- What types of people have been affected (affected individuals and their family members, staff, trustees and volunteers etc.)?

- Whether those affected have any special needs/vulnerabilities.

NOTE: Actions to contain and recover data as well as mitigate any risk should be taken immediately. The investigation is to ensure that the case is being managed and any improvement actions agreed are implemented. The investigation should be proportionate to the breach identified and risk of harm.

- 9.3 The initial investigation should be completed urgently and wherever possible within 24 hours of the breach being discovered / reported. A further review of the causes of the breach and recommendations for future improvements can be made once the matter has been resolved.
- 9.4 However, some level of investigation might be required to carry out the Risk Assessment and determine the most appropriate route of escalation. If, once identified, risk of a data breach is contained and does not pose immediate further threat to the organisation and/or members, timeframes for official escalation/notification can be extended to allow for a more thorough investigation. Extensions must be agreed upon at each stage and noted in the report.
- 9.5 As an investigation proceeds the risk may change and the reporting requirements should be amended in line with the change in risk. For example, a case identified as a significant risk initially may increase to a major risk and therefore should be escalated to the ICO.

10 Informing affected individuals

- 10.1 The ICO requires us to inform those affected where there is a significant breach of personal and sensitive data and the risk of harm to those individuals is high.
- 10.2 Clearly if there was a high risk of further harm the organisation would have an obligation to disclose the breach to each individual affected. However, this must be balanced against the risk of causing further distress and anxiety to the families by informing them about the breach.
- 10.3 The ICO guidance states that “informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.”
- 10.4 Only the data breach owner and/or DPO can decide whether to advise affected individuals of a data breach and therefore the reasons for deciding to do this should be clearly set out in the investigation report and discussed with the data breach owner and other involved parties before affected parties are informed.
- 10.5 Further advice on whether to disclose to individuals is contained in the ICO Guidance on Assessing Disclosure to Individuals affected by a data breach.

11 Learning Lessons

- 11.1 The Lessons Learnt Action Plan for data breaches and near misses should be completed and will form part of the investigation process.
- 11.2 The action plan should clearly outline the lessons learnt, the controls agreed to reduce the risk of

a further recurrence, a lead member of staff and a completion date.

12 Performance monitoring and responsibilities

12.1 90% of investigations should be completed within 10 working days of the data breach being identified.

12.2 Where a major risk has been identified: -

An interim report should be presented to the Chair within 10 working days even when the case cannot be concluded within this timescale.

Further reports should be presented to the Chair at least every 10 working days until the case is concluded.

13 Data Breach Log

13.1 All data breaches, including near misses, will be recorded on the data breach log. All issues identified by the application of this policy will be recorded in the data breach log and categorised according to whether it is a data breach or near miss.

13.2 This information will be reviewed and analysed by the Chair at least monthly to identify patterns and to monitor the implementation of agreed service improvements.

13.3 The Chair will collate all data breach reports and will report trends and lessons learnt quarterly to the Board.