Process

Reporting a Data Breach

Definition of a data breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. It is a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Disclosing information to someone within Barnardo's that shouldn't see it, or someone in Barnardo's accessing information that they shouldn't, is still a breach, and should be reported.

Why do I need to reporting a breach?

It is important to report a data breach to your line manager or Data Protection Manager
as soon as you become aware of it. Even if you just suspect there has been a breach you should still report it. You may have been made aware of it by a customer or service user who feels that their data has got into the wrong hands because of some action Barnardo's has taken, by another member of staff or volunteer, or through some other external source.

The decision about whether to report a breach to the Inforation Commissioner's Office (ICO) is determined by Barnardo's Data Protection Officer (DPO) in discussion with the appropriate Data Protection Manager (DPM) after an investigation. However, if we decide we don't need to report the breach, we need to be able to justify this decision, so should document it.

We have to make these decisions quickly because we only have 72 hours from discovering the breach to report it to the ICO, this includes evenings and weekends. So, if we discover the breach at 3pm on a Friday evening, and it's a serious one, we've only got until 3pm on Monday to report it.

The UK General Data Protection Regulation (UK-GDPR) recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Therefore, Article 34(4) allows us to provide the required information in phases, as long as this is done without undue further delay.

How do I report a data breach?
Reporting a breach can be done in one of two ways. Firstly by clicking on the link Report a Breach on Inside Barnardos in the Data Protection area or by going to OneTrust via OKTA. In OneTrust yo will have the option of using the "self service portal" which will be on the front page once you have logged in.

The form is straightforward and easy to complete, however, a guidance document is available on Inside Barnardo's to help you with the process.

Once submitted the relevant DPM will assess the seriousness of the breach to determine whether it needs escalating to the DPO. If you have not provided enough information for the DPM to make a decision, they can either add a comment to the assessment, which you will receive via email with a link to respond. Or they can send the assessment back for review with comment on additional information required. Please ensure you response to any requests for further information as soon as possible.

Notifying Supervisory Authorities and Data Subjects
The DPO is the only person who can report a data breach to the ICO., and at the same time the Company Secretary should inform the Charity Commission. In some cases when dealing with a serious breach it will be necessary to inform the person whose personal data has been affected. Your DPM or the DPO will let you know if you need to do this – it's important that you don't inform the data subject before taking advice, as this may cause them unnecessary distress.

Martine King
Data Protection Officer
February 2022