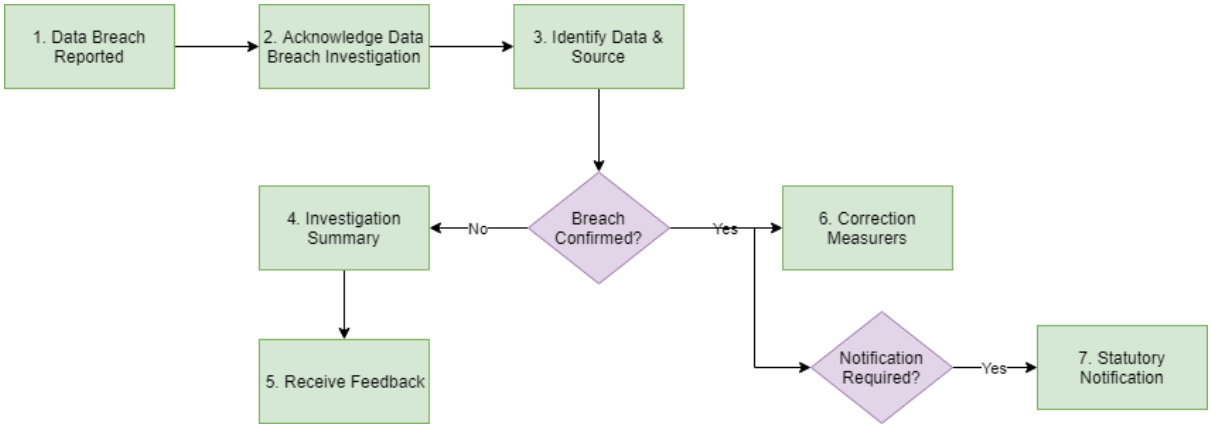
Northstone Systems
Data Breach Reporting Policy

Version 1: April 2018

1 About this policy

This policy defines how Northstone Systems Ltd will manage personal data breaches in accordance with our Data Protection Policy. This policy outlines the policy we will follow in the unlikely event that a data breach should occur within our systems.

2 Data Breach Flowchart



Step	Description
1. Data Breach Suspected / Reported	If a data breach is reported, either from an external source or from an internal employee then a full investigation should be carried out. The directors of the company should be alerted immediately that there has been a suspected breach.
2. Acknowledge Data Breach Investigation	An investigation will be started by a number of senior employees to ensure that the process is fully followed. During the initial investigation, the following information will be recorded: • Time / Date of reported breach • Steps taken to identify breach • Whether or not a breach did occur A full log of the tools used and tasks completed should also be logged.
3. Identify Data & Source	If the suspicion is that systems have been breached, then an audit should be carried out to identify which data and the possible source of the data. After this stage we can confirm or deny if the breach has taken place. If the breach is confirmed to be true, then a full investigation should be carried out immediately to see what the full extent of the breach is.

	The following statement is used to define if personal information has been breached. "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned." Where possible, immediate steps should be taken to halt or minimise the scale of the data breach. This could include taking the systems offline whilst correcting any known mistakes.
4. Investigation Summary	If the suspicion is false, then a summary report should be compiled including lessons learnt.
5. Receive Feedback	Policies and procedures can then be amended if required.
6. Correction Measurers	If personal information WAS breached then a full root cause analysis should be conducted to identify what went wrong, when it went wrong and how it went wrong. This may include the involvement of outside data protection companies and security auditors.
7. Statutory Notification	If personal data WAS breached, then under GDPR the breach should be reported to the ICO. The breach should be reported to the ICO within 72 hours (https://ico.org.uk/for-organisations/report-a-breach/). Following the breach report to the ICO, we will contact our customers who have been affected by the breach. Should their customer information also be affected then we will provide advice and guidance which they can use to contact their customers.