Appendix A

RUSHMOOR BOROUGH COUNCIL

DATA PROTECTION BREACH POLICY

There is potentially a **72 hour** timeframe in which information about a data breach needs to be reported to the ICO

Author: Nikki Hughes, Audit Manager

October 2018
Version: 1.1
Endorsed by: Licensing, Audit and General Purposes Committee – November 2018

Contents

1. What is personal data

1.1 Personal data is information relating to natural persons who can be identified or identifiable directly from the information or who can be indirectly identified from the information in combination with other information. For example, name, identification number, location data.

1.2 You do not have to know someone's name for them to be directly identifiable, a combination of other identifiers may be sufficient to identify the individual.

1.3 Information must 'relate to' the identifiable individual to be personal data. This means it does more than simply identifying them – it must concern the individual in some way. For example, bank details.

1.4 Information about companies or public authorities is not personal data. However, information about individuals acting as sole traders, employees, partners and company directors, where they are individually identifiable and the information relates to them, as an individual may constitute personal data.

1.5 Information about a deceased person does not constitute personal data.

1.6 The following personal data is classified as special category data:

- Racial/ethnic origin
- Political opinions
- Religious/ philosophical beliefs
- Trade union membership
- Genetic or biometric data for the purpose of identifying a person
- Data concerning a person's health, sex life or sexual orientation

2. What is a personal data breach?

2.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. Examples include:

- Sending personal data to an incorrect recipient
- Electronic devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Deliberate or accidental action (or inaction) by a controller or processor

2.2 A personal data breach can be paper or electronic documents.

3. Reporting data breaches

3.1 The following processes should be carried out when a data breach has been identified by Rushmoor Borough Council and details recorded in the form in Appendix A. It should be noted that where a data breach is likely to result in a risk to the rights and freedoms of one or more people then this will need to be reported to the ICO **WITHIN 72 HOURS** (this includes weekends) Therefore the matter should be treated urgently:

- ***Containment and recovery***
  You should notify your Line Manager or for Members the Head of Democracy, Strategy and Partnership and the Data Protection Officer (DPO) when a data breach has been identified. Action should be taken immediately if it is identified that the breach is still occurring, so that the damage caused by the breach is minimised. This may require input from different services such as IT, Legal services or may even require contacting suppliers.

  It should also be established by the Manager and DPO if there is anything that can be done to recover any losses to minimise any damage the breach could cause. For example, the physical recovery of equipment or wiping of a lost mobile device.

- ***Assessing the risk***
  Once the breach has been contained, the Manager and DPO need to assess the risk associated with the breach. This should include an assessment of the potential adverse consequences for individuals, how serious these are and how likely they are to happen.

- ***Notification of breaches***
  Where necessary Rushmoor Borough Council will need to inform people and organisations that we have experienced a data security breach. 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. If the breach presents a high risk to individuals then they must be notified without undue delay unless measures have been put in place, which have removed or substantially reduced the risk.

  The Manager and DPO also need to consider who to notify, what they are going to tell them and how they are going to communicate the message. Any notification should include a description of how and when the breach occurred and what data was involved.

  If it is determined that there is a risk to people's rights and freedoms then the Information Commissioner (ICO) must be notified. If it is unlikely then you do not have to report it however

you will need to justify this decision. Notification must be made to the ICO **within 72 hours** of finding out about the breach (this timeframe includes weekends). Although, it is recognised that it might not possible to investigate a breach within this timeframe therefore you can provide the required information in phases as long as it is done without undue further delay. Not notifying the ICO of the breach when required could result in a significant fine.

If malicious cyber activity has resulted in the data breach then the details must be reported to the IT Network Manager so that the details can be reported to the National Cyber Security Centre and the Public Sector Network.

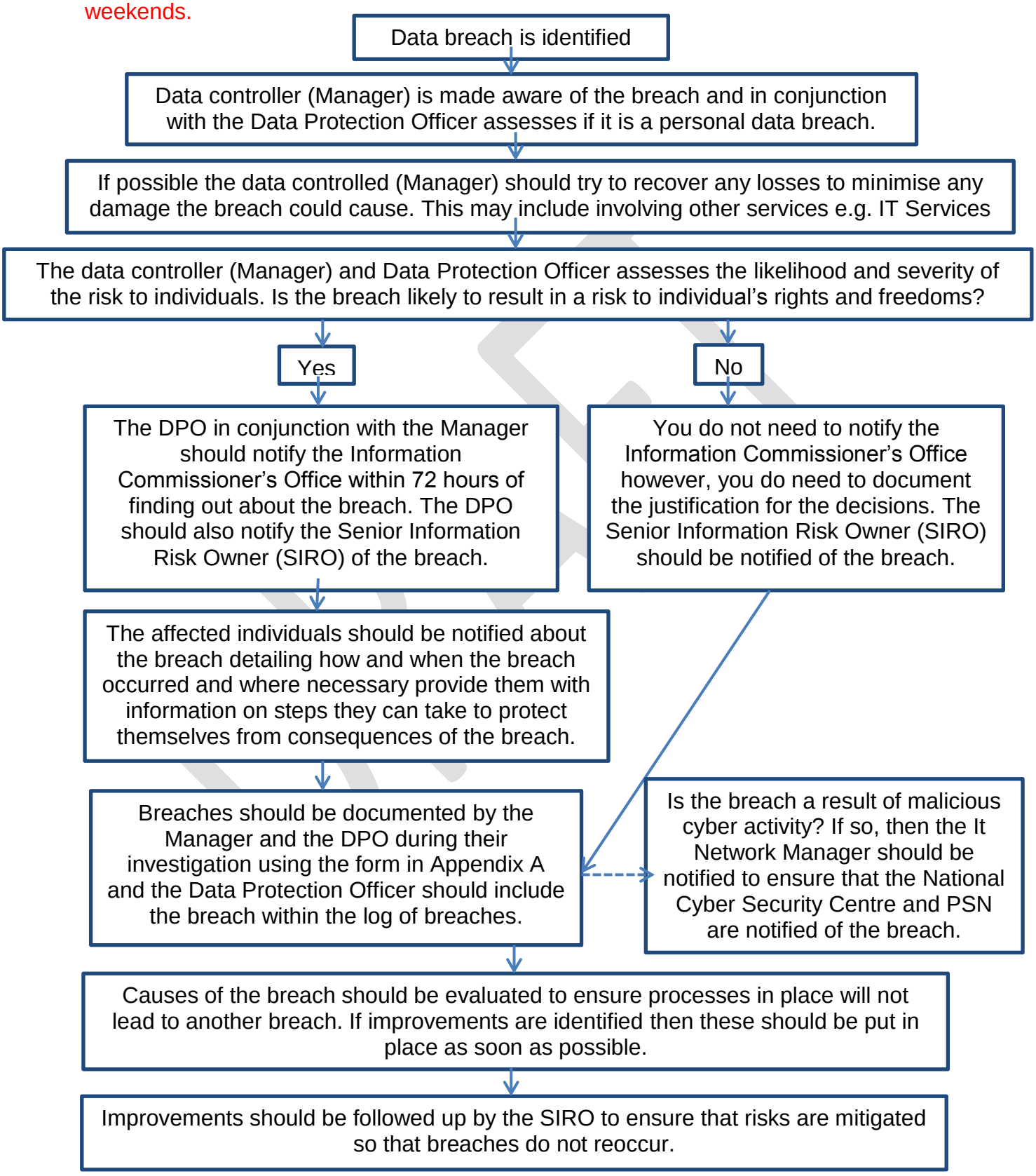
The DPO should notify the Senior Information Risk Officer (SIRO) of any breaches that have occurred.

- ***Evaluation and response***
  The Manager and DPO should evaluate the effectiveness of the response to the breach. The cause of the breach should be evaluated to ensure processes in place will not lead to another breach. If improvements are identified then these should be put in place as soon as possible.

  The SIRO should ensure that vulnerabilities are followed up to ensure risks of future breaches are mitigated.

Notification requirement flow chart

NB: If the data breach is likely to result in a risk to the rights and freedoms of individuals then the ICO should be notified **within 72 hours**, this timeframe includes weekends.



Appendix A

Organisational Details
Rushmoor Borough Council Council Offices Farnborough Road Farnborough Hants GU14 7JU
DPO contact details
Data.protection@rushmoor.gov.uk

Investigating officer(s)	
Contact details	

Timeline of data breach	
Date/ time of the breach	
Date became aware of the breach	

Details of data breach	
Description of the breach and how it occurred detailing: - What type of data is involved - Is it special category data - If the data has been lost/stolen are there any protections in place e.g. encryption - What has happened to the data - What was the cause of the breach e.g. human error - How many individuals are affected by the breach - Who are the individuals whose data has been breached	

Likely consequences of the data breach	
Assessment of the likely consequences: - What could the data tell a third party about the individual - What harm could come to the individuals affected - Are there wider consequences to consider e.g. risk to public health or loss of public confidence? - How likely are the consequences to the individuals	

Notification of the breach	
Are there any legal or contractual requirements to notify individuals of the breach	
Can notification help the individuals? Consider the dangers of over notifying	
After considering the above: Are the data subjects to be notified of the breach?	Y/N
If so, how will the data subjects be notified (What is the most appropriate method based on the group of individuals affected e.g. Children or vulnerable adults)	
Date individuals notified	
Is the ICO to be notified of the data breach?	
If not, what is the reason for not notifying them	
Date ICO notified	
Have the appropriate regulatory bodies been notified?	
If so which ones have been notified?	
Date notified	
Is the breach a result of malicious cyber activity?	Y/N
If so, has the national cyber security centre and PSN been notified by the IT Network Manager	
Date National cyber security centre notified	
Date PSN notified	

Action Taken	
Details of action taken to mitigate the effect to the individuals involved	
Has the data that was breached been recovered? If so, please provide details as to how and when.	

Evaluation	
Details of the investigation of the cause -How and why it occurred	
Details of the steps to be taken to prevent a reoccurrence of this incident.	