Data Breach Reporting Procedure
for Pennine District

Issue 1 Draft 1 : March 2018

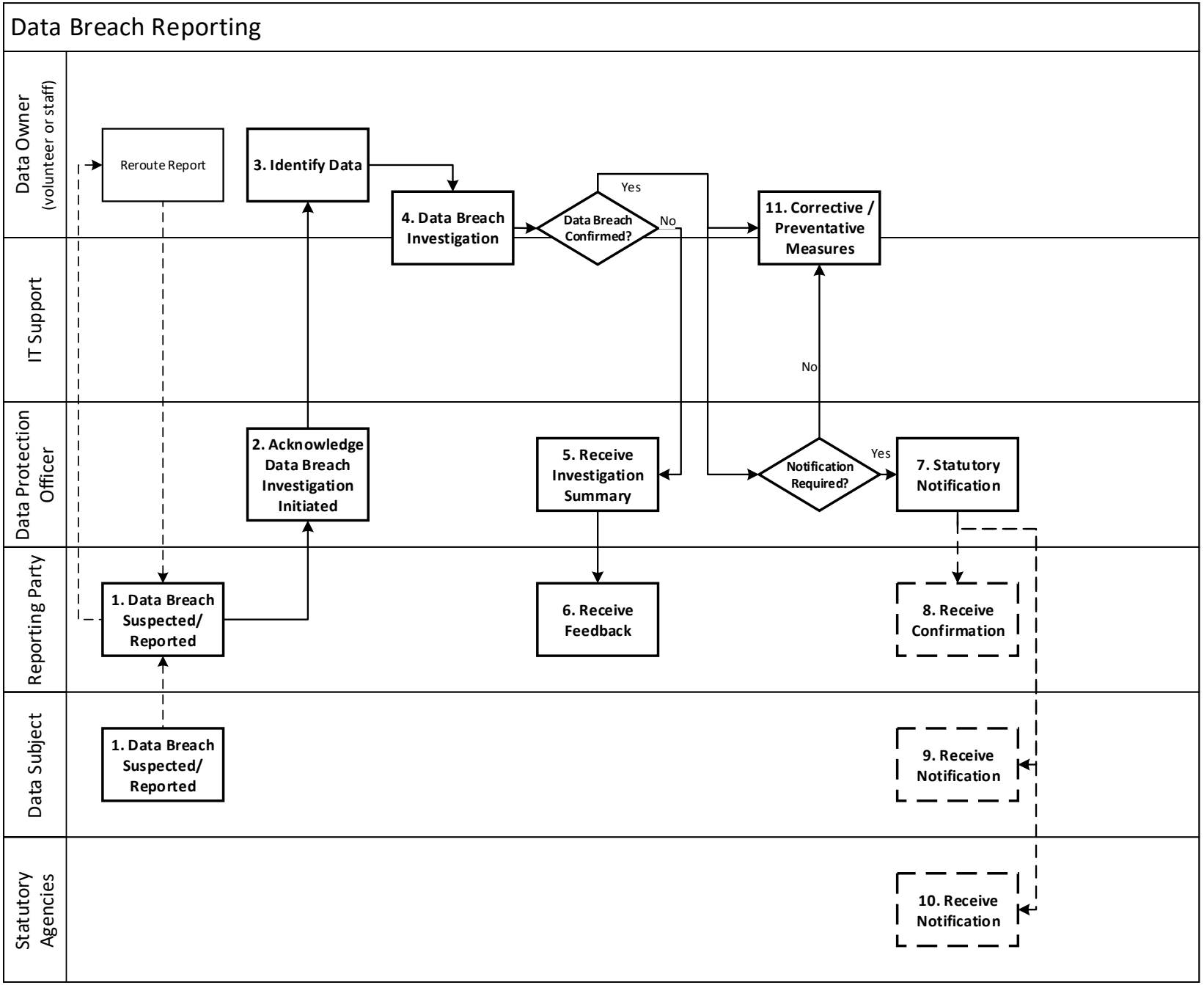
About this procedure

This procedure defines how Pennine District will manage personal data breaches in accordance with the UK Data Protection Bill 2017. It should be read in conjunction with current information and guidance published by the UK Information Commissioner's Office (ICO – http://ico.org.uk/)

Note that once the UK leaves the European Union, additional requirements of the European Union General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) may continue to apply with respect to data processed relating to EU citizens, which may include youth members and volunteers. As Pennine District does not regularly process data relating to citizens of the EU as a matter of course, it is considered that the UK Data Protection Bill 2017 will meet the requirements of the EU GDPR regulation. Should this position change this procedure will be reviewed.

The general requirements for data protection are defined in the Pennine District Data Protection Policy.

Note that any subprocessors engaged on behalf of Pennine District (e.g. Online Scout Manager, Compass etc.) are required to report ALL data privacy breaches. They should be considered as reporting parties with respect to this procedure.


Data Breach Reporting
Data Owner (volunteer or staff)
IT Support
Data Protection Officer
Reporting Party
Data Subject
Statutory Agencies
Reroute Report
3. Identify Data
4. Data Breach Investigation
Data Breach Confirmed?
Yes
No
11. Corrective / Preventative Measures
No
2. Acknowledge Data Breach Investigation Initiated
5. Receive Investigation Summary
Notification Required?
Yes
7. Statutory Notification
1. Data Breach Suspected/ Reported
6. Receive Feedback
8. Receive Confirmation
1. Data Breach Suspected/ Reported
9. Receive Notification
10. Receive Notification

This process is described in more detail below

Step	Description
1. Data Breach Suspected / Reported	The data subject, or any other party reports a suspected or actual personal data breach. All volunteers of Pennine District have a responsibility to immediately report any actual or suspected data breach. Failure to do so may result in disciplinary action being taken. These should be reported to the Data Protection Officer. Any volunteer receiving such a report should request the reporting party to report the matter to the Data Protection Officer and copy the Data Protection Officer will all correspondence.
2. Acknowledge Data Breach Investigation Initiated	Upon receiving any report of an actual or suspected data breach, the Data Protection Officer will initiate an investigation and will acknowledge that the investigation has been initiated to the reporting party. All such investigations will be logged, including • Time and date of suspected breach being reported • Whether or not an actual breach occurred • Whether or not any breach was reportable (and if not, why not) • When the breach was reported If further information is required (scope, nature, time/date and suspected cause of the actual or suspected breach) this will be requested from the reporting party. Note that if the reporting party is NOT the data subject, the data subject may not be notified at this stage. The appropriate Data Owner (Responsible Officer) should be informed of the actual or suspected breach. The Pennine District Commissioner and Pennine District Chair should also be informed.
3. Identify Data	The Data Owner(s) (Responsible Officers) will identify the scope of the actual or suspected data breach. The Pennine District IT Support will provide support to identify the IT and information assets potentially involved.
4. Data Breach Investigation	The Pennine District IT Support will provide support to identify the IT and information assets potentially involved. The Data Owner(s) (Responsible Officers) and the Pennine District IT Support, assisted by other volunteers as required, will investigate the data breach to determine whether or not there has been a data privacy breach. The following definition of a personal data breach should be considered. *"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, 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."* For data privacy to have been breached it must affect the confidentiality, integrity or availability of personal data (relating to a natural individual) which involves e.g.: • Access by an unauthorised third party; • Deliberate or accidental action (or inaction) by a controller or processor; • Sending personal data to an incorrect recipient; • Computing devices containing personal data being lost or stolen; • Alteration of personal data without permission; or • Loss of availability of personal data Where possible, immediate steps should be taken to halt or minimise the scale of the data breach.

Step	Description
5. Receive Investigation Summary	If personal data privacy was NOT breached, the Data Owner(s) (Responsible Officers) should send a brief summary of the investigation to the Data Protection Officer, including the reasons for concluding that personal data privacy was not breached
6. Receive Feedback	If personal data privacy was NOT breached, the Data Protection Officer should send a brief summary of the investigation to the reporting party, including the reasons for concluding that personal data privacy was not breached. The Pennine District Commissioner and Pennine District Chair should also be informed.

7. Statutory Notification	If personal data privacy WAS breached, the impact of the breach should be determined by the Data Protection Officer. If the Data Protection Officer determines that the rights and freedoms of the data subject have been infringed it is likely that the breach should be reported.
	If it is considered that the breach is *not* reportable to the ICO, the reason for this conclusion must be logged.
	If the breach is reportable (via https://ico.org.uk/for-organisations/report-a-breach/) it should be reported to the ICO within 72 hours where feasible. If this is not feasible, the reasons for the delay should also be reported.
	The following information should be reported to the ICO:
	• A description of the nature of the personal data breach including, where possible:
	  ○ The categories and approximate number of individuals concerned; and
	  ○ The categories and approximate number of personal data records concerned;
	• The name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
	• A description of the likely consequences of the personal data breach;
	• A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects
	Where this information is not fully available, reporting may be completed in phases with a minimal delay.
	Evidence of notification, including time and date of notification, should be retained in all cases.

8. Receive Confirmation	If personal data privacy WAS breached, the Data Protection Officer should send a brief summary to the reporting party, confirming that the matter is being treated as a data privacy breach. The Pennine District Commissioner and Pennine District Chair should also be informed.
9. Receive Notification	If personal data privacy WAS breached and the breach is considered of sufficiently high risk to the rights and freedoms of the individual such that they may need to take steps to further protect themselves (e.g. loss of financial, health or confidential contact details, or where safety or safeguarding is at risk) the data subject(s) must be advised. Such notification should include: • The name and contact details of our Data Protection Officer or other contact point where more information can be obtained; • A description of the likely consequences of the personal data breach • A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Step	Description
	Evidence of notification, including time and date of notification, should be retained in all cases
10. Receive Notification	The ICO should acknowledge receipt of any data breach notification and a record of receipt should be retained with time and date evidence.
11. Corrective / Preventative Measures	If personal data privacy WAS breached, in additional to any immediate action taken a full root cause analysis should be conducted. Corrective actions should be taken to secure any further personal data breaches. Based upon the root cause analysis, preventative measures may be taken to prevent or minimise the likelihood or the same or any similar reoccurrences.