Data breach process

Step 1– Potential data breach identified

Step 2 – Notify the Data Protection Officer (DPO) – James Bottomley

Step 3 – Is the breach notifiable to the ICO? DPO judges if breach is notifiable

- 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
- When deciding if the breach is notifiable we must consider the likelihood and severity of any risk to people's rights and freedoms
- If it's likely there will be a risk then we must notify the ICO. If it's unlikely then we don't have to report the breach
- We do not need to report every breach to the ICO
- See the ICO website for further information

If yes go to step 4a. If no go to step 4b.

If yes:

Step 4a – Notify the SIRO, Paul Wylie, who must notify the ICO within 72 hours of the breach coming to light

- Call the ICO on 0303 123 1113
- We need to provide:
    - details of what happened
    - when and how we found out about the breach
    - the people that have been, or may be, affected by the breach
    - what we are doing as a result of the breach
    - who the ICO should contact if they need more information and who else we have told

Step 5a – SIRO notifies SLT and CEO

Step 6a – Notify individuals involved, if necessary, by phone or email

- If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says we must inform those concerned directly as soon as possible
- A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. We will need to assess both the severity of the potential, or actual, impact on individuals as a result of a breach and the likelihood of this occurring
- One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach
- See the ICO website for further information

Step 7a – DPO logs the breach

Step 8a - DPO works with staff to ensure learning is shared so there are no more breaches of this type. If necessary delivering a training refresh

Step 9a - Breaches raised at monthly SLT meeting to share learning

If no:

4b – Notify SIRO and DPO logs the breach

5b – DPO works with staff to ensure learning is shared so there are no more breaches of this type

6b – Breaches raised at monthly SLT meeting to share learning

Key contacts

Data Protection Officer – James Bottomley
GDPR Project Manager – [redacted]
SIRO – Paul Wylie

Out of hours

If out of hours call Paul first then try and contact each of the other directors until you speak to one of them. You do not need to speak to all of them, just one.

Data Protection Officer – James Bottomley
GDPR Project Manager – [redacted]
SIRO and Director of Strategy – Paul Wylie
Director of Finance – Siobhan Peters
Director of Criminal Justice and Commissioning – Sam Cunningham
Director of DARA – Julie Norgrove

Policy Review Log

Updated by	Date	Next review
[redacted]	11 May 2018	May 2019