

Data Breach Process

- When a data breach is identified the Incident should be reported to the Data Protection Officer DPO who is the SMASH CEO
- A data breach Incident Report Form (DB1) should be completed
- The DPO determines whether the breach is still occurring and if it is will immediately take steps to rectify.
- If the breach is not ongoing, the DPO will appoint a Lead Investigating Officer (LIO)
- The DPO and LIO will determine whether anything can be done to recover the loss of data and minimize the damage of the breach.
- The LIO will identify who needs to be notified as part of the containment
- The LIO will determine suitable cause of action to resolve the solution, consulting experts if required.
- Once the incident has been contained the LIO will commence and incident immediately
- The LIO and DPO will determine whether the Information Commissioners Office need to be notified and if so should do so within 72 hours of the incident being identified.
- LIO should inform any and all individuals affected by the breach and give advice on how they can protect themselves.
- LIO and DPO consider notifying police, bank, insurers if they believe illegal activity occurred.
- LIO and DPO consider whether a press release is necessary and plan response to the press if believe it may be required
- The data breach should be recorded in the data breach log, which is held by the Administrator
- The LIO and DPO should evaluate the incident and the response to determine whether a change to policy or procedure is required. If a requirement is determined, then they should propose updated policies and procedures to the Trustee Board
- The Trustee Board should consider and should sanction the update if appropriate