DATA BREACH REPORTING PROCEDURE

(SEE DATA BREACH POLICY FOR DETAIL)

Actual or suspected Data breach identified by Officer(s)

→

Notify Line Manager and IT (f required) and complete Staff Data Breach Report Form (SDBF)

→

Officer(s)/Line Manager sends SDBF to and notifies Information Governance and Data Protection Manager and/or FOI Officer

→

Information Governance and Data Protection Manager and/or FOI Officer and officer(s) and/or Line Manager determine if data breach is occurring. If so, put in place steps to minimise effects and stop breach

↓

If breach is low risk, Information Governance and Data Protection Manager and/or Information officer and officer(s) and/or Line Manager to complete final data breach report and include details in breach log

←

Information Governance and Data Protection Manager and/or FOI Officer and officer(s) and/or Line Manager to determine which parties need to be notified

←

Information Governance and Data Protection Manager and/or FOI Officer and officer(s) and/or Line Manager to begin investigation of breach within 24 hours of notification using a Data Breach Report Form

↓

If breach is medium-high risk then notify:

Senior Information Risk Officer

Head of Service

Deputy Chief Exec/Chief Exec

The Police(if required)

Affected Third Parties

→

If breach is deemed high risk then ICO and/or data subjects to be notified within 72 hours. ICO breach form to be completed for ICO notification

→

Information Governance and Data Protection Manager and/or FOI Officer and officer(s) and/or Line Manager and Head of Service (if required) to evaluate response using Data Breach Report Form

↓

All data breaches reported to:

Leadership team – half yearly

Audit and Governance Committee – half yearly

←

Information Governance and Data Protection Manager and Line Manger, officer(s) and Head of Service (where required) to ensure improvements are implemented

←

Final breach report (including possible improvements) circulated with informed parties (ICO and Date Subjects if required)