

University of Lincoln Personal Data Breach Response Flowchart

Identification and initial assessment

Breach or suspected breach identified

Report breach in person or by telephone to Information Compliance Officer or ICT Help Desk (available out of hours too)

Information Compliance Officer gathers information and requires Reporter to complete Breach Notification Form if not already completed

Information Compliance Officer assesses incident and determines next steps

Containment and recovery

Information Compliance Officer initiates mitigating actions that have not already been carried out, involving Communications team and senior managers as appropriate

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals, the individuals will be informed in an appropriate manner without undue delay, and providing advice to help them protect themselves from its effects.

Risk Assessment

Assess Severity of Breach using agreed methodology – generates a risk severity rating

Is severity close to or exceeding threshold to report to ICO?

Yes

No

Discuss with SIRO (or delegate as available) and contact ICO reporting helpline

Information Compliance Officer decides whether to report to ICO

No

Yes

Notification

Make notification to ICO
* This must be done within 72 hours of breach being identified *

Evaluation and Response

Prepare report with recommendations to prevent reoccurrence

Apply any sanctions deemed appropriate

Monitor and review ICO case

SIRO or Registrar to review after 6 months to ensure recommendations have been incorporated into practice

Prepare report with recommendations to prevent reoccurrence

Apply any sanctions deemed appropriate

Information Compliance Officer to review after 6 months to ensure recommendations have been incorporated into practice

Refer to Information Compliance Committee if recommendations have not been followed