

Data Security Breach Procedure

Introduction

All information security incidents must be reported to the Legal Team. This enables an internal investigation, with a view to determining what action should be taken and whether the incident should be reported to the Information Commissioner's Office.

Even if information has not been lost, but the incident may be classed as a 'near miss' this should be reported to your manager. An example here might be a member of staff taking sensitive information home without authority, but returning it safely the next day.

Note: if we need to self-report to the ICO this must be done within 72 hours

| Actions | Responsibilities and Duties |
|---|---|
| 1 Employee | All identified incidents must be reported to the Council's Legal Team as soon as they are detected. The Legal Team will notify the DPO |
| 2 CIP Team | If the incident is identified via a complaint, the CIP Team will appoint an investigating officer from the service area where the incident has originated, and the matter will be managed under the Corporate Complaints Procedure |
| 3 DPO | If the incident has not been reported through the Complaints process, the DPO will appoint a senior officer within the service area to investigate the incident and establish why it happened, whether or not it constitutes a breach and what remedial action is necessary. The investigating officer will keep the Legal Team regularly updated on progress. |
| 4 Investigating Officer | The investigating officer will take professional advice as required from the DPO, CIP Team, Legal Services, and HR. |
| 5 Employee Investigating Officer | Establish the following and advise the Legal Team as soon as possible: <ul style="list-style-type: none">• The extent of the breach• The amount of information involved• The sensitivity of information involved• A timeline of dates and times concerning the incident• The potential for loss or damage to individuals, the Council or any other body• What measures need to be taken and how quickly (for example: can the information be recovered? Do any individuals or organisations need to be notified? Do the Police need to be notified?) |

| Actions | Responsibilities and Duties |
|------------------------------------|---|
| 6 Investigating Officer | Unless considered to be a very minor breach of security, carry out and document a risk assessment. Depending upon the outcome of the risk assessment, use the letter template in Annex 1 to inform those affected by the breach. |
| 7 Investigating Officer | Report the loss of data to the police as required, and notify the Council's DPO whenever the police are involved. |
| 8 DPO | Consider convening a meeting as appropriate involving people who are likely to have an active role in remedying the breach or dealing with any of the outside parties involved. Maintain an action plan tasking individuals with assisting the investigation as necessary. |
| 9 Investigating Officer | Consider whether written statements may be needed. If so, first consult with the Legal Team and the HR Team if it is considered that Disciplinary action may be required at some point. |
| 10 Investigating Officer | If information has been sent to the wrong address, retrieve the information as soon as possible, using the letter template in Annex 1 or via a home visit as appropriate. |
| 11 Investigating Officer | Always consider involving the Council's Communications team early on and keeping them updated. |
| 12 Investigating Officer | As part of the process of identifying the cause of the breach, try to consider measures that can be put in place to eliminate or reduce the chances of a reoccurrence. Where these are obvious, put them in place straight away; where these would need further discussion, report them to the DPO. |
| 13 Investigating Officer | Where the incident has been treated as a complaint, the investigating officer will draft a response for the complainant and have it reviewed by the Legal Team and the DPO. The response will be sent to the complainant by the CIP Team. |

| Actions | Responsibilities and Duties |
|--|---|
| 14 Investigating Officer | Provide a final written briefing to the DPO. If the DPO concludes that the breach should be reported to the Information Commissioner, complete a formal breach notification form and send it to the Legal Team and the DPO for review |
| 15 Legal team/ DPO | Submit ICO Breach notification form (if required) and address any outstanding legal issues (e.g. injunction proceedings). https://ico.org.uk/for-organisations/report-a-breach/personal-databreach/ Notify the relevant portfolio holder(s) where a breach notification is submitted. |

| | |
|---|---|
| Further guidance available (links to useful documents) | https://ico.cloud.panopto.eu/Panopto/Pages/Viewer.aspx?id=778fb8a9-4095-4db5-aacb-a914009d53af |
| Related policies & procedures | Disciplinary Procedure Data Protection Policy |

Golden rules for reporting and investigating data breaches

Remember:

- Do not keep a breach to yourself, even if you feel there has been no harm arising.
- Do not seek to apportion blame – the main object of this procedure is to address the breach and improve our processes.
- This procedure is not confined to breaches involving personal data only. Any uncontrolled information loss is important.
- Be honest with the facts.
- Be thorough in investigating or assisting with any investigation.

Contact details

Mark Stinson
Data Protection Officer
Tel: 07899 061277

Sarah Wolstenholme-Smy
Legal Services Manager
Tel: 07970 248422