

Police Authority Data Security Breach Procedure

The Data Protection Act 1998 came into force on 1 March 2000. It is concerned with the rights of individuals to gain access to personal information held about them by an organisation or individual within it, and the right to challenge the accuracy of data held. The terms of the Act relate to data held in any form, including written notes and records as well as electronic data.

The Act also requires that all staff and others who process or use any personal information must ensure that they adhere to the eight data protection principles. In summary, these require that personal data shall:

- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
- be adequate, relevant and not excessive for those purposes;
- be accurate and kept up-to-date;
- not be kept for longer than is necessary (NB Retention of data for historical or statistical research is allowed under Section 33 of the Act);
- be processed in accordance with the data subject's rights;
- be kept safe from unauthorised access, accidental loss or destruction;
- not be transferred to a country outside the EEA (the EU member states, plus Norway, Iceland and Liechtenstein), unless that country has adequate levels of protection for personal data.

Lancashire Police Authority is fully committed to compliance with the requirements of the Data Protection Act 1998 which came into force on 1 March 2000.

Lancashire Police Authority processes personal data about members of the public only in very limited circumstances.

Most of the personal data that we process relates to members and officers of the Authority; and to officers and support staff of Lancashire Constabulary.

The Authority will therefore follow procedures which aim to ensure that all employees, members, and service providers, who have access to any personal data held by or on behalf of the Authority, are fully aware of and abide by their duties under the Data Protection Act 1998.

Data Security Breach Procedure

When an incident occurs which affects (either internally or by its external providers) the Police Authority which breaches any of the eight principles set out in the Act it is the responsibility of all Members of the Authority, staff and Service Providers to inform the Resources Manager of possible or actual breaches of the Data Protection Act, who will then brief the Chief Executive.

It is the responsibility of the Chief Executive to ensure that the breach is recorded and acted upon in line with the Authority's Security Breach Procedure.

1. An incident occurs.

For example:

- A break in, theft of equipment, files or records.
- The loss of electronic records, files, disks, USB memory sticks, especially anything containing personal data.
- The loss of paper records especially anything containing personal data, for example files left in cafes, cars, at home, discarded filing cabinets.
- The unauthorised access to any records, equipment or network files.
- An information system becoming inaccessible for any reason including through damage to a building.
- An attempt to hack into a system.
- A virus or any other form of damaging software.
- An abuse of access rights by staff, including the unauthorised browsing of information or copying of information or using another person's username and password to access systems.
- Any breaches of the acceptable use of email and internet by sending excessive amounts of non work related emails or browsing unacceptable internet web sites.
- A weaknesses in systems which might lead to a security issue especially those relating to passwords and user accounts.

2. Is the incident likely to result in any of the following:

- A criminal act.
- An unauthorised disclosure of confidential information particularly personal data.
- A risk of damage to the Authority's information, records or systems.
- A risk of an interruption to the availability of the Authority's systems or information held on them.
- An adverse impact (associated with the operation of information systems, whether ICT or other) such as:
 - ▶ embarrassment to a directorate or the Authority as a whole
 - ▶ threat to personal safety
 - ▶ threat to personal privacy or human rights
 - ▶ breach of a legal obligation or incurring of a penalty
 - ▶ inability to support partnership working
 - ▶ inability to demonstrate good information governance and partnership working reasons.

- A Complaint or adverse report from an external source about an incident: a member of
 - ▶ the public, a whistleblower, a partner organisation, the Information Commissioner,
 - ▶ External Auditor or Inspector, The Surveillance Commissioner, the Interception Commissioner, the Police or the media are examples.

3. If no, talk to the Resources Manager about how the incident might be managed.

4. If yes, inform the Resources Manager and complete a security breach form.

5. If it is difficult to involve the Resources Manager then use the security breach form and indicate the difficulty. Alternatively report via the Authority's Whistle Blowing Policy or the Deputy Chief Executive.

Mrs C Durber
Deputy Chief Executive
Lancashire Police Authority
PO Box 653
Preston
PR2 2WB

Tel:- 01772 533415

e-mail:- christine.durber@lancashire.gov.uk

6. The Resources Manager receives the security breach form and assesses whether the impact could be serious (using government public impact level information, and advice from the Monitoring Officer if necessary).

7. The Resources Manager grades the incident impact as either:

NOT SERIOUS

The Resources Manager advises the Chief Executive that the incident is not classed as "serious" and then the Resources Manager develops and implements an action plan to address the incident. The Resources Manager also completes a Lessons learnt Log Form.

The Resources Manager feeds back the security breach form and the lessons learnt log form at the next staff team meeting.

IF IT IS SERIOUS

The Resources Manager informs the Chief Executive that the incident is classed as serious and then the Resources Manager contacts the relevant service expert:

- Human resources
- Internet Audit
- Police
- ICT
- Finance

A collective decision is taken to resolve the incident and reduce the level of impact. The action plan should include clearly defined timescales, deadlines and responsibilities.

The Resources Manager also completes a Lessons learnt Log Form.

The Resources Manager feeds back the security breach form and the lessons learnt log form at the next staff team meeting.

The Chief Executive will report to the next available Audit and Standards Committee e.g. if any breach and or lessons learnt impacts on one or more of them.

Roles

- Members, staff and service providers : to notify the Resources Manager of any data breach or suspected data breach
- Resources Manager: To grade the seriousness of the impact of all information security breaches and to advise the Chief Executive accordingly. To oversee the management of any information security breaches and give advice on actions to be taken. To report security breaches to the Information Commissioner's office in line with ICO guidance. Also to collect and review all security breach forms and lessons learnt forms.
- Monitoring Officer: To review all information security breaches and provide the policy framework to mitigate risk to the Authority, its partners and its customers. For example, if there are a high number of thefts highlighted, then the physical security policy may need to be addressed; if email abuse rises then the IT acceptable use policy may need to be addressed.

Security Breaches 2010/11

Security breaches recorded in 2010/11

The statistics for information collected by Lancashire Police Authority about incidents in 2010/11 are as follows:

Reported via intranet	1
Engineers incident reports	0
Total	1

The breakdown by type is as follows

Abuse by staff (mainly email etc)	0
Theft (mainly laptops)	0
External hacking	0
Internal unauthorised access	0
Virus clean up events (not detections)	0
Bad practice by end user	0
Security related procedural breach	1
Significant near miss	0
Data loss	0
EIR what's this/	0