



PC02/2009 – RESPONDING TO LOSS OF DATA

IMPLEMENTATION DATE: Immediate

EXPIRY DATE: January 2014

FOR ACTION: Chairs of Probation Boards/Trusts, Chief Officers/Executives, Secretaries of Probation Boards/Trusts

FOR INFORMATION: Board/Trust Treasurers, Improvement and Development Managers, Regional Offender Managers, Directors' of Offender Management

CONTAINS MANDATORY ACTIONS

AUTHORISED BY: Michael Spurr, Chief Operating Officer, NOMS

ATTACHED: N/A

RELEVANT PREVIOUS PROBATION CIRCULARS

N/A

CONTACT FOR ENQUIRIES

MOJ Information Directorate – Tel: 020 7210 2190

PURPOSE

This Circular sets out the action to be taken in the event of an actual or suspected loss of data.

2. A loss of data could take many forms and you could discover it in different ways. The list below is not exhaustive but examples include:

- loss of an offender file, or one turning up where it should not be;
- Information missing in the post or from a fax transmission
- theft of a computer or memory stick containing personal data
- loss of a mobile phone containing personal data
- leaving a computer disk or laptop containing personal information on a train or in any non-secure environment.

3. Personal data compromise can occur through theft, loss or deliberate or unintentional damage or destruction. The NPS definition of 'personal' data is defined in the NPS 'Data Protection Policy', available on EPIC. Personal data relates to any information which identifies an identifiable living individual, including any expression of opinion about that person or

UNCLASSIFIED

expression of intentions towards them. The NPS will hold personal data on offenders, victims, witnesses, staff and stakeholders.

4. How “significant” a compromise is will depend on a number of factors and on the individual circumstances of a case. In all cases you should refer immediately to:

- your manager;
- your most local senior manager who will inform;
- your local member of the Senior Civil Service (SCS) (i.e. Regional Director, Area Director, Chief Probation Office, Regional Offender Manager, Director of Offender Management etc).

5. Ultimately a member of the Senior Civil Service in the relevant business area will be responsible for determining the gravity of the situation and whether the procedures below need to be followed. Some of the factors you and they will need to consider include:

- number of individuals involved;
- possible impact of the breach, including the apparent risk to the individuals; members of the public and Probation Service/NOMS/MoJ operations or reputation; and
- necessary actions to be taken to mitigate the risk.

MANDATORY ACTIONS

6. *If you identify a data loss, become aware of or suspect a data loss, you must immediately (within one hour) bring it to the attention of your line manager, or in their absence, another manager. You or your manager must then inform your local Information Security Representative, who will liaise with your most senior local manager (eg a local Senior Probation Officer) and inform your Area’s designated Information Security Incident Manager and Chief Officer. At Area level, the Chief Officer, Data Protection Officers and local Information Security Representatives and Information Security Forums must be informed as soon as possible.. Chiefs have ultimate responsibility for deciding whether or not the incident needs to be escalated to Regional Offender Managers and equivalents. Delays in identifying incidents may lead to vital information being forgotten or lost. In all cases you should refer in the first instance to your line manager or the most appropriate manager available.*

7. *Chief Officers must ensure that all staff are aware of and have access to this instruction, and know what to do in the event of an incident. This includes contractors, temporary staff and third parties who handle personal information.*

8. *On being notified of a loss or potential loss of personal information, and then subject to para 5 above the Chief Officer or Deputy must within one hour inform :-*

- *the Director-General for NOMS - (Phil Wheatley - 020 7217 6777) ;*
- *the Chief Operating Officer*
- *Justice Secretary’s and Permanent Secretary’s office;*
- *junior Ministers’ offices and Special Advisers ;*
- *Director of Offender Management/Regional Offender Manager ;*
- *the MoJ Information Director;*
- *the MoJ Director of Communications and Head of News;*
- *the NOMS Senior Information Risk Owner (SIRO); (Director of Finance and Performance - Ann Beasley 020 7217 6822)*
- *the NOMS Chief Information Officer (CIO); (Philip French - 020 7217 6486)*
- *Director of Probation – Roger Hill (020 7217 0650)*
- *the Head of NOMS IT Security; (Bob Nicholls - 020 7217 8062)*

UNCLASSIFIED

- NOMS Information Security Team (Stan Cook 07768 811932)
- your local security representative; and
- the News Desk in MoJ Press Office (by phone on 020 3334 3536 / out of hours pager 07659 173 270).

9. Contact may be made by email or telephone and must not wait until the full facts of the case are known. It is not enough to send an email and assume someone else will take responsibility. If you send an email you must check that it has been received - if in doubt, please make a call to confirm receipt of your email.

10. While some assessment of the significance of the loss will be apparent in making the initial report, it is important that all losses or potential losses are reported immediately, without waiting for the results of investigations or risk assessments. If in doubt, the loss must be reported.

11. It is the responsibility of the Chief Officer to inform the right people within the organisation, to initiate an investigation into the circumstances surrounding the incident and to ensure that it is handled correctly and closed down swiftly, with lessons learnt and next steps documented and followed through. If you are in any doubt about the process at any stage, your local Information Security Representative, local Information Security Incident Manager or ultimately the MoJ Information Directorate on 020 7210 2190 can provide advice and guidance throughout the process.

12.. You are advised to keep notes, especially if the incident is complex or developments are moving fast and details need to be captured.

13. Data loss is a sensitive issue and a local incident may be of national media interest and certainly of interest to Ministers. Public lines to take must be cleared through the MoJ Press Office. The News Desk will facilitate this and can be contacted on 020 3334 3536.

14. Within the first day of becoming aware of an incident, an investigation into the case should begin with a view to completing and submitting a Security Incident Tracker Form in liaison with the appropriate security team for your part of the business. The NPS 'Incident Management' Policy on EPIC and local policies and intranets provides details on reporting incidents.

15. The investigation will inform a risk assessment which should cover the following points:

- numbers and status (eg victims) of individuals affected
- type of data compromised (eg personal data, sensitive corporate data, non-sensitive data)
- circumstances of the incident (including physical environment, time of day)
- whether the incident concerns or affects non-NPS organisations
- full assessment of the possible risks arising, covering risks to data subjects, the public, Ministry of Justice or government operations and reputation
- the risk of additional loss from a vulnerability being further exploited.

16. Taken together, these assessments should inform recommendations for next steps and press handling, regardless of whether or not the incident is likely to become public knowledge.

17. Next steps must include recommendations on:

- whether and how to inform data subjects (those whose data has been lost/compromised) or other parties. These should be based on an objective and accurate assessment of the statutory duties, the potential risks and the benefits of disclosure.

UNCLASSIFIED

- *locally, your Area's legal representative and Data Protection Officer can advise on whether the Information Commissioner's Office should be informed, in liaison with the MoJ Information Directorate. If in any doubt or for further guidance the Information Director's team should be contacted. The Commissioner can often provide practical advice on handling breaches and where the breach (or potential breach) is very serious we have a duty to inform him*
- *whether the police need to be involved. For example if the incident involves MAPPA case information or where the loss involves possible theft of data from premises or systems.*

Day 2 and beyond

- *Keep updating the Incident Tracker Form.*
- *As with all security breaches, your local Information Security Incident Manager will work with staff in the relevant unit to investigate the circumstances and ensure that lessons are learned for the future.*
- *Private Office, Press Office, the Director General's Office and the Information and Communication Directors should be kept informed of any new developments that may have an impact on the advice provided earlier, and if necessary supplementary advice should be provided.*