

**Published under Section 48(2) of the
Personal Data (Privacy) Ordinance (Cap. 486)**

**Investigation Report:
Hong Kong Police Force's Repeated Loss of
Documents Containing Personal Data**

Report Number: R13 - 0407

Date issued: 24 October 2013



**香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong**

**Hong Kong Police Force’s Repeated Loss of
Documents Containing Personal Data**

This is the result of five investigations carried out by the Privacy Commissioner for Personal Data (the “**Commissioner**”) pursuant to section 38(b) of the Personal Data (Privacy) Ordinance, Cap. 486 (the “**Ordinance**”) against the Hong Kong Police Force (“**HKPF**”) in respect of the repeated loss of police documents containing personal data. Section 48(2) of the Ordinance provides that “*the Commissioner may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, published a report -*

(a) *setting out -*

- (i) *the result of the investigation;*
- (ii) *any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and*
- (iii) *such other comments arising from the investigation as he thinks fit to make; and*

(b) *in such manner as he thinks fit.”*

ALLAN CHIANG
Privacy Commissioner for Personal Data

Hong Kong Police Force's Repeated Loss of Documents Containing Personal Data

Background

The Privacy Commissioner has served an Enforcement Notice on the HKPF following its breach of the Data Protection Principle 4 (“DPP4”) of the Ordinance relating to protecting personal data against accidental loss. The decision follows the conclusion of its investigation into a series of data breach incidents that involve the HKPF officers losing records of personal data.

2. During the period from October 2011 to January 2013, 11 data breach incidents came to the Commissioner’s notice concerning loss of police notebooks (“**notebooks**”) and copies of “Notice of particulars of alleged fixed penalty traffic offence”, usually known as Fixed Penalty Tickets (“**FPTs**”), by different police officers. The lost items contained the personal data of a total of 285 persons including crime victims, witnesses and suspects.

3. Notebooks are used by police officers to record all matters pertaining to their discharge of duties and may contain the name, address, Hong Kong Identity Card Number (“**HKID Card No.**”), date of birth (“**DOB**”) and statements made by suspects or witnesses, etc. Notebooks can, at a later time, help the police officers refresh their memory of events and particulars including relevant statements made by persons connected with any case/incident. Every notebook bears a serial number on its cover. According to the Police General Orders, every officer below the rank of Chief Inspector shall be issued with a notebook, and shall carry it at all times when on duty. Normally, an officer should only have in his possession one notebook in current use. A notebook in current use by a junior police officer shall be produced to his immediate supervising officer at the start of his shift and checked at least once during the shift.

4. FPTs are used by police officers in connection with enforcement of section 3(1) of the Fixed Penalty (Criminal Proceedings) Ordinance, Cap 240, against traffic offences. In addition to the details of the traffic offence, the amount of penalty and the vehicle number, an FPT may contain the surname and driving licence number / HKID Card No. of the offending driver. An FPT

booklet contains 10 FPTs. Each FPT has three copies all bearing the same serial number. After the first copy of an FPT is issued to the offending driver or in his absence affixed to the offending vehicle, the second copy in yellow would be passed to the Central Traffic Prosecution Division of the HKPF for further action (e.g. issuing demand note for payment). The third copy would be retained in the booklet for record purpose.

Relevant Provisions of the Ordinance

5. Data Protection Principle 4 (“**DPP4**”), concerning the security of personal data, in Schedule 1 to the Ordinance is relevant to the subject investigations. DPP4 was among the provisions amended by the Personal Data (Privacy) (Amendment) Ordinance 2012. As two of the 11 incidents occurred before the amendment of the Ordinance on 1 October 2012 and the remaining nine incidents occurred thereafter, the two versions of DPP4(1), that is, both the prevailing version and the previous version, are reproduced below with the amendments underlined.

6. DPP4(1) of the current Ordinance provides that:-

“All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to –

- (a) the kind of data and the harm that could result if any of those things should occur;*
- (b) the physical location where the data is stored;*
- (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;*
- (d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and*
- (e) any measures taken for ensuring the secure transmission of the data.”*

7. The version of DPP4(1) prior to the amendment stipulates that:-

“All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to –

- (a) the kind of data and the harm that could result if any of those things should occur;*
- (b) the physical location where the data are stored;*
- (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;*
- (d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and*
- (e) any measures taken for ensuring the secure transmission of the data.”*

8. According to section 2 of the Ordinance, “practicable” means “reasonably practicable”.

Information Collected during the Investigations

9. In the course of investigations, we collected information and documents from the HKPF including written representations, statements made by the officers concerned, extracts of the Notebook Issue and Receipt Register (Pol. 24B) (“**NIRR**”) and the Notebook On Loan Register (“**NOLR**”), extracts of Police General Orders, Force Procedures Manual (“**FPM**”), Traffic Procedures Manual (“**TPM**”), other internal memoranda and guidelines governing the use of notebooks, FPTs and relating to personal data protection. Presented below is the relevant information obtained by this Office.

10. The table below summarises the 11 data breach incidents under investigation with detailed circumstances of each incident described in the paragraphs that follow:-

Incident No.	Date of the incident	Nature of item lost	Number of items lost	Number of data subjects affected	Personal data concerned
Notebook					
1	30/10/2012	Notebook	17	41	Name, address and HKID Card No.
2	11/11/2012	Notebook	1	2	- Ditto -
3	12/12/2012	Notebook	1	130	HKID Card No.
4	31/12/2012	Notebook	1	60	Name, HKID Card No. and DOB
5	26/1/2013	Notebook	1	29	- Ditto -
FPT / FPT booklet					
6	26/10/2011	FPT copy	1	1	Vehicle No., surname and driving licence / HKID Card No.
7	14/9/2012	FPT booklet	1	2	- Ditto -
8	19/10/2012	FPT booklet	1	5	- Ditto -
9	21/10/2012	FPT booklet	1	4	- Ditto -
10	15/1/2013	FPT booklet	1	10	- Ditto -
11	21/1/2013	FPT copy	1	1	- Ditto -

11. All data subjects were identified and traceable data subjects were notified except those in Incident 3 who were involved in on-going judicial proceedings.

Data breach incidents involving police notebooks (Incidents 1 to 5)

Incident 1 (30 October 2012)

12. A police officer, on 30 October 2012, reported loss of 18 used notebooks to the HKPF. The police officer worked for a Division before being posted to another region and had been requested since mid-October 2012 by the original Division to return used notebooks. It was claimed that all 18 used notebooks were put in a paper bag when the officer went to work by bus on 30 October 2012, and the paper bag was inadvertently left on the bus. The HKPF subsequently confirmed that the number of used notebooks kept by the police officer was in fact 17 instead of 18.

13. According to the FPM, an officer shall return his used notebook at the same time as he obtains a new one. If he does not return his used notebook for any reason (e.g. kept by a court as an exhibit), the Notebook Issuing Officer (“**NIO**”) should be informed of the reason which will be entered in the NIRR. The NIO shall not issue a new notebook unless the used one has been checked and endorsed by the supervisory officer of the officer in possession of the notebook. The check is to ensure that (a) a new notebook is necessary; (b) the used notebook has been maintained in accordance with FPM; (c) supervisory checks have been correctly endorsed in the used notebook; and (d) any entries in the used notebook that require attention have been properly dealt with before the notebook is surrendered.

14. If a used notebook is kept by court as exhibit or an officer needs to retain a used notebook or to retrieve it after it has been returned for a particular police case, e.g., for preparing witness statement or attending court, a Report Number (“**RN**”) (i.e. the corresponding police case number) would be entered in the NIRR or NOLR as the reason for retaining or retrieving a used notebook. The NIO is not required by FPM to verify the alleged need for retaining such notebook. Indeed, the HKPF’s internal investigation revealed that all the notebooks lost, despite “RNs” provided as the reasons for retaining/retrieving the notebooks, were not used as case exhibits.

15. Incident 1 involved the loss of used notebooks which were issued as far back as 2007. 16 of the 17 lost notebooks were kept by the officer since the issue dates whilst the remaining one notebook, after having been returned, was withdrawn from storage on 9 January 2012 and kept by the officer since. RNs were stated in the NIRR and NOLR as the reasons for retaining or retrieving 15 used notebooks. The reason marked in the NIRR for not returning the one of the 16 used notebooks was “not signed by supervisory officer” while no reason was stated for the retention of the 17th notebook. The NIO did nothing further to follow up on these two unreturned notebooks. Appendix 1 sets out the issue/retrieval dates of each of the 17 notebooks, the number of days lapsed up to the date of loss (i.e. 30 October 2012) and the reasons for not returning the used notebooks as entered in the NIRR and NOLR.

16. The FPM states that the Notebook Storage Officer (“NSO”) shall conduct bi-annual checks of the NIRR. Details of any notebook that has not been returned within a year of issue shall be brought to the attention of the Administrative Support Sub-unit Commander (“ASSUC”) or an equivalent officer. The ASSUC shall contact the officer in possession of the notebook and ascertain its current status. Where a notebook has been used and retained by an officer for a period in excess of two years without justification, disciplinary action would be considered.

17. The HKPF confirmed that its internal investigation concluded that the officers concerned, including the officer in possession of the 17 notebooks, the NSO and the NIO concerned, had all failed to observe the provisions of the FPM. Disciplinary proceedings against the officer who retained and lost the 17 notebooks are in progress. No disciplinary action would be initiated against the NSO and the NIO as they had already retired.

18. Separately, the FPM also states that the NIRR should be checked monthly by a Chief Inspector to ensure compliance with the requirements of the FPM. However, exactly which areas the Chief Inspector needs to check are not stated in the FPM. In this incident, the HKPF confirmed that the Chief Inspector concerned had checked and signed on the record of inspection of NIRR on a monthly basis.

19. Subsequent to Incident 1, the HKPF issued a memorandum on 6 November 2012 to implement additional measures to ensure timely collection of unreturned notebooks. “Unreturned notebooks” include an old notebook not returned at the time an officer draws a new notebook, and also a used notebook retrieved by an officer from storage. Among others, the memorandum sets out the following:-

- (a) Monthly inspection of NIRR and random checks on the accuracy of information marked as the reason for not returning the used notebooks by Assistant Divisional Commander (Administration) (or equivalent) (“ADVC ADM”) are required;

- (b) For unreturned notebooks that have been outstanding for 30 calendar days without a valid reason, ASSUC (or equivalent) shall send a memorandum to request the officer's supervisor at the Station Sergeant rank or above to return the notebook or give a written explanation for not returning it within 30 calendar days (Note: valid reasons refer to situations such as where notebooks have been kept by court / police as exhibits, kept by officers for giving evidence in court and the court case is still on-going);
- (c) For unreturned notebooks that have been outstanding for 60 calendar days without a valid reason, the ADVC ADM shall report the situation of these notebooks on file to the Divisional Commander (or equivalent) ("DVC") on a monthly basis. The DVC shall direct the officer's supervisor to collect the notebooks or provide a written explanation within 30 calendar days; and
- (d) For unreturned notebooks that have been outstanding for over 60 days and possessed by an officer transferred to another Formation, DVC of the issuing Formation shall arrange for a memorandum requesting the return of the notebook to DVC of the new Formation. The latter shall arrange the return of the notebooks or provide a written reply within 30 calendar days.

20. There were further incidents of loss of notebook after the issuance of this memorandum but in no incident did the loss involve more than one notebook.

Incident 2 (11 November 2012)

21. A police officer brought a notebook to in-house training at the HKPF training college between 5 and 9 November 2012. The police officer put the notebook in a rucksack after the training on 9 November 2012. Later in the evening, the officer found the rucksack worn and thus removed all belongings to another rucksack. The worn rucksack was left at a friend's home. On 12 November 2012, the officer found the notebook missing and recalled that the notebook was placed in the worn rucksack. The officer called the friend who said that the worn rucksack had been thrown away. The HKPF's internal investigation concluded that the loss was an accident due to the officer's carelessness. The officer was given a verbal warning.

Incident 3 (12 December 2012)

22. On 12 December 2012, a police officer returned from leave and found the notebook missing from the office. The police officer recalled that the notebook was last used in the office in the afternoon before leave but had no idea where it had been placed afterwards. According to the Police General Orders, restricted documents must be kept in a locked steel filing cabinet or in an office which is locked up after office hours and to which members of the public do not have access. The HKPF's internal investigation concluded that the loss was due to the officer's carelessness. The officer was given a verbal warning.

Incident 4 (31 December 2012)

23. A police officer reported loss of a notebook on 30 December 2012. The police officer remembered that the notebook was last used in the afternoon of 29 December 2012 in a briefing room. The notebook had been put in the left pocket (with no button or zip) of the officer's uniform jacket after the briefing and the officer proceeded to crowd management tactics practice. After the practice, the officer took off the jacket and stored it in a locker. The officer did not check the whereabouts of the notebook until resuming duty on 30 December 2012. The HKPF's internal investigation concluded that the incident stemmed from the officer's inappropriate safekeeping of the notebook whilst on duty in the regional headquarters. The officer was given a verbal warning.

Incident 5 (26 January 2013)

24. On 24 January 2013, a police officer, in plain clothes, participated in an anti-crime patrol. The supervisor checked the notebook at 18:55 hours on the same day. The officer then put the notebook in the right pocket of a jacket (which was not a police uniform) and carried on patrol. The officer returned to Headquarters and signed off in the late evening. After a day off, the officer resumed duty in the afternoon of 26 January 2013 and discovered the notebook missing. The officer did not check the notebook from 18:55 hours on 24 January until 26 January 2013. It was suspected that the notebook could have fallen out of the jacket pocket when patrolling on the previous working day. The HKPF's internal investigation concluded that the incident stemmed from the officer's inappropriate safekeeping of the notebook during his execution of duty. The officer was given a verbal warning.

Data breach incidents involving FPTs/FPT booklets (Incidents 6 to 11)

Incident 6 (26 October 2011)

25. On 15 September 2011, a clerical assistant who was on relief duty for another colleague on sick leave, received 22 yellow FPT copies from a frontline unit for processing. On the following day, the clerical assistant sent a batch of only 21 FPT copies, together with a list of their serial numbers to Central Traffic Prosecution Division, without noticing that one copy had been omitted. The mistake was revealed on 26 October 2011 when payment for the omitted FPT was received. The HKPF gave advice to the clerical assistant in respect of the carelessness in handling personal data and losing the government property.

Incident 7 (14 September 2012)

26. At 15:15 hours on 14 September 2012, a police officer found the FPT booklet missing. It was last put in the officer's waist pouch, a standard gear issued by the HKPF with a zip, at 11:55 hours on the same day. As the police officer had drawn from the waist pouch another police booklet between 11:55 hours and 15:15 hours, the HKPF opined that the FPT booklet could have fallen out of the waist pouch accidentally at that time and seriously advised the police officer verbally to handle all documents containing personal data with due care.

Incident 8 (19 October 2012)

27. After a police officer issued an FPT to an offending driver at 14:36 hours on 19 October 2012, the FPT booklet was not put back in the pouch. Instead, the police officer resumed patrol by holding in hand the FPT booklet and two other police booklets. At 16:10 hours on the same day, the FPT booklet was discovered missing when the police officer was about to issue another FPT. As to why the booklets were not put back in the pouch after use, the officer said that police officers on patrol with penalty tickets in their hands could create a deterrent effect on drivers. The HKPF considered that the police officer had carelessly lost the FPT booklet and seriously advised the officer to be more cautious in the safekeeping of police documents.

Incident 9 (21 October 2012)

28. After a police officer had issued an FPT to an offending driver in the morning of 21 October 2012, the FPT booklet was put in the pannier of the officer's police motorcycle and the officer resumed patrol. At 11:38 hours, the booklet was found missing from the pannier after the officer arrived at an operation post. The police officer forgot if the pannier had been padlocked.

29. The HKPF sought assistance from the Electrical and Mechanical Services Department ("EMSD") to examine the motorcycle in issue. EMSD found that the pannier of the motorcycle was in proper condition. Nevertheless, the HKPF requested EMSD to design and install an auxiliary lock to supplement the original padlock on the pannier of the same model of motorcycles.

30. The HKPF opined that it was an accident as the FPT booklet might have been thrown out of the unlocked pannier under strong wind conditions when the police officer was driving on the highway. The police officer was verbally advised by the HKPF to exercise due care of police documents containing personal data.

Incident 10 (15 January 2013)

31. A police officer issued an FPT at 16:20 hours on 15 January 2013. The police officer then put the FPT booklet in the pannier of the police motorcycle without closing the padlock and resumed patrol. At 17:30 hours, the police officer found the FPT booklet missing from the pannier.

32. The HKPF examined the motorcycle concerned and no security deficiency was revealed. The HKPF attributed the loss of the FPT booklet to the police officer's carelessness and gave a verbal advice accordingly.

Incident 11 (21 January 2013)

33. In a police operational base, there was a lockable collection box for police officers to put in summons and FPTs for daily dispatch from the operational base to a Police Station in the same district by police vehicle. A list was attached to the box for individual police officers to record the items they had put in the box. The box could only be opened by the designated clerical assistant when it arrived at the police station. On 21 January 2013, a police officer put a yellow FPT

copy in the box at the operational base and recorded it on the list attached thereto. The box, together with the list, was then dispatched to the police station and unlocked by the clerical assistant. However, the FPT copy in question could not be found. The HKPF considered that the loss of FPT copy was likely due to misplacement at the operational base or accidental loss during transit to the police station and the officers concerned were given a verbal advice.

34. In view of the incident, the Divisional Commander formulated a standing order in April 2013 by designating the duty shift sergeant to consolidate, check and record the FPT copies collected from individual officers before depositing them in the box.

The Commissioner's Findings

35. In accordance with DPP4, data users are obliged to take all practicable steps to ensure personal data is protected against unauthorised use or accidental loss. While DPP4 does not require a data user to provide an absolute guarantee for the personal data held by it, the Commissioner considers the HKPF has failed to take all practicable steps, including putting in place a set of comprehensive procedures as well as ensuring the effective implementation of its supervision and monitoring system, to safeguard the security of police documents containing personal data. The incidents also revealed the need to review the police equipment and uniform design, as well as a general lack of awareness of the security risks associated with personal data among the officers concerned.

Policies and Procedures

36. The HKPF has in place the Police General Orders which state that the HKPF respects personal data privacy and is committed to complying with the requirements of the Ordinance. In order to maintain the integrity of documents which contain personal data, officers are required to make reference to and comply with DPP4 and keep such documents in a manner that will prevent any unauthorised disclosure or access. Despite this general policy, Incidents 1 and 11 revealed gross insufficiency in the underlying operational procedures.

37. The major deficiencies identified are:-

- (a) (as identified in Incident 1) In this incident all the RNs provided by the officer did not support the retention of notebooks. There was apparently no mechanism to verify if the reason claimed by a notebook holder to retain a used notebook was true. The NIO concerned accepted the reason as long as a police case number was provided by the officer. When the notebook has not been returned for over a year, the NSO should (but he did not) bring the matter to the attention of the ASSUC who, in turn, was only required to check the status with the notebook holder. There was no requirement for the NSO to query the notebook holder's explanation by, for example, verification with the notebook's holder's supervisor. In other words, as long as a seemingly reasonable justification for retention was given, the ASSUC had to take the notebook holder's word for it.
- (b) (as identified in Incident 1) The NIO has the duty to issue a new notebook in return for a used one, but not to accept the return of a used notebook if it is not endorsed by the supervising officer of the notebook-holder. However, there is no rule which requires the NIO or anyone else to follow up on the subsequent return of the unendorsed notebook. This procedural hiatus has in effect permitted the notebook holder to retain the notebook for no reason at all.
- (c) (as identified in Incident 1) The Chief Inspector carried out monthly checks on the NIRR to ensure compliance with the provisions of the FPM but despite the endorsement on the NIRR, he had failed to identify that 17 notebooks were retained by the same police officer for more than five years. This unacceptable failure highlights the need for the formulation of a checklist for the Chief Inspector to follow in the monthly inspection.
- (d) (as identified in Incident 11) There was no mechanism to verify the number of FPTs as claimed by individual police officers in the dispatch list were in fact the same number deposited into the collection box of an operational base and dispatched to the police station. This loophole has been plugged with the designation of a

sergeant to check and consolidate all the items before they are deposited into that collection box.

Supervision and Monitoring

38. With sound security policies and procedures in place, there is no guarantee that they will be followed. In this regard, supervision and monitoring of the implementation of the procedures are important. The police incidents, however, clearly demonstrated that the HKPF's oversight system has been far from effective.

39. Notable deficiencies identified in Incident 1 are as follows:-

- (a) The NSO failed to identify all the irregularities in the bi-annual checks for more than 5 years.
- (b) Although, according to records, the Chief Inspector did undertake monthly inspections as required by the FPM, he had failed to spot any of the numerous irregularities.
- (c) As the NIRR and the NOLR are maintained in paper form, one has to manually go through all such documents kept in a police formation in order to find out the total number of notebooks retained by a particular officer at any one time. This is not conducive to prompt identification of compliance problems. An effective system, achievable by computerisation, should enable a timely alert of all outstanding issues when an officer requests issue of a new notebook or when a check by a supervising officer is initiated.

Equipment and Uniform

40. Equipment and uniform, when properly designed with their function to carry police documents duly taken in account, should enhance the protection of such documents.

41. We have not inspected the equipment and uniform involved in the incidents and cannot therefore comment if there are deficiencies or areas where improvement in design is definitely required. However, we have the following observations:-

- (a) (as revealed in Incident 4) the lost notebook was believed to have fallen off from the pocket of the police jacket;
- (b) (as revealed in Incident 5) the lost notebook was believed to have fallen off from the pocket of the jacket of the officer wearing plain clothes;
- (c) (as revealed in Incidents 9 and 10) FPTs were believed to have fallen out from the panniers of two police motorcycles which can be secured with a padlock; in the former case an additional lock with an auto fastening function was added to the pannier but nothing similar was introduced in the latter case; and
- (d) (as revealed in Incident 11) it was believed that the FPT could have fallen out from a locked dispatch box whilst in transit from an operational base to a police station.

Awareness of Privacy and Data Protection

42. A common theme of the irregularities identified in the incidents is negligence and carelessness on the part of the police staff involved. In most cases, they could not account clearly for the loss of the documents. Some of them forgot where they had last kept the documents, others could not be sure if the documents which should have been locked were indeed locked while one (Incident 10) admitted he had not locked up the document as required. In Incident 6, the officer concerned did not reconcile the number of FPTs received from the frontline units of a district traffic formation on a particular day with the number of FPTs dispatched from that unit to the Central Traffic Prosecution Division for subsequent processing. In the extreme case of Incident 1, the staff involved blatantly failed to observe the requirements of the FPM.

43. These problems seem to indicate a lack of awareness and appreciation of the importance of privacy and data protection among some staff of the HKPF.

Conclusion and Enforcement Notice

44. In view of the HKPF's deficiencies in its procedures in safeguarding the notebooks and FPTs identified in paragraph 37 in Incidents 1 and 11 and the notable deficiencies in its supervision and monitoring systems highlighted in Incident 1, the Commissioner concluded that the HKPF has contravened DPP4 in these two Incidents for failing to take all reasonably practicable steps to protect the personal data contained in these documents against accidental loss.

45. Pursuant to section 50(1) of the Ordinance and in consequence of an investigation, if the Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the Ordinance, the Commissioner may serve on the data user a notice in writing, directing the data user to remedy and, if appropriate, prevent recurrence of the contravention.

46. In view of the Commissioner's finding of contravention on the part of the HKPF, the Commissioner has decided to serve an enforcement notice on the HKPF pursuant to section 50 of the Ordinance to remedy and prevent any recurrence of the contravention. The HKPF is directed to:-

- (a) establish a mechanism to verify the reason for retaining a used notebook as claimed by an officer;
- (b) impose a duty on the NIO (or another appropriate officer) to follow up on the return of unendorsed notebooks;
- (c) formulate a checklist for the monthly inspection to be conducted by the Chief Inspector on the NIRR and the NOLR;
- (d) establish a mechanism to ensure that the number of issued FPTs surrendered by police officers at the end of their duties in an operational base are properly checked by a supervising officer before the FPTs are dispatched to the police station for further processing; and

- (e) establish an effective system (such as a computerised system) to provide a status report and timely alert of all outstanding issues relating to notebook(s) retained by an officer when he requests issue of a new notebook, or when a check by a supervising officer is initiated.

47. All the eleven incidents (with the exception of Incident 11) involved negligence or carelessness on the part of the police officers concerned. The Commissioner accepts that human errors of this nature cannot be totally ruled out. As the requirement under DPP4 to safeguard personal data is not absolute and the data user's obligation is to take all reasonably practicable steps, the Commissioner considers that the police officers' failures in these incidents do not by themselves constitute a DPP4 contravention on the part of the HKPF. However, taking into account the very sensitive nature of the personal data involved and the frequent occurrence of these incidents, the matter has to be taken seriously.

Further Advice

48. In this regard, the Commissioner understands that the HKPF indeed takes a serious view of the data breach incidents. According to the written reply by the Secretary for Security to a Legislative Council member's questions on 21 November 2012, the HKPF's Information Security Working Group, led by the Deputy Commissioner of Police (Operations) and which includes representatives from operations, crime and security, management, training, information systems and public relations at management level, has been reviewing the relevant policies, procedures and guidelines, and would continue to adopt various measures to ensure that their systems and procedures are maintained at the highest information security level.

49. In view of the observations in paragraph 41 above, the Commissioner advises that there is a strong case for the HKPF's working group to undertake a general review of its equipment and uniform used for holding or conveying police documents with or without personal data, in order to safeguard them from unauthorised access or accidental loss.

50. Further, in view of a demonstrated lack of awareness and appreciation of the importance of privacy and data protection among the staff of the HKPF as pointed out in paragraph 43 above, the Commissioner suggests that the HKPF should step up its training, incentive and disciplinary programmes to promote compliance with the HKPF's policies and procedures in relation to privacy and data protection. The building of a privacy-respectful and data-secure culture which ensures commitment throughout the organisation is highly recommended.

Concluding Remarks

51. Data users are obliged to protect personal data by reasonable security safeguards against such risks as loss, unauthorised access, destruction, use, modification or disclosure of data. The potential harm to individuals from the misuse of their personal data, whether accidentally lost, leaked or purposely stolen, could be significant.

52. In this regard, organisations are advised to embrace data protection as part of their corporate governance responsibilities. They should have appropriate policies and procedures that promote good privacy and data protection practices. They should also ensure adequate oversight to check that security rules and procedures are fully implemented. The HKPF's deficiencies in security procedures and oversight, as revealed in this investigation, are regrettable. They represent a bad example which organisational data users should take due note of.

53. Admittedly, many security breaches are simply the result of human error which cannot be totally eliminated. Recklessness or simple carelessness of a single employee can undermine sound privacy policies and robust security practices. This underlies the importance for organisations to institute comprehensive internal training and awareness programmes for their staff. To ensure an organisation-wide commitment, the building of a culture of privacy is imperative.

Appendix 1

Details of Incident 1: Issue/retrieval date and number of days lapsed up to the date of loss

	Issue date / withdrawn from storage date	Number of days lapsed up to date of loss (30/10/2012)	Reasons recorded in registers for failing to return used notebook (or withdrawing used notebook from storage)
1	23/4/2007	5 years 6 months 7 days	Not signed by supervisory officer
2	7/6/2007	5 years 4 months 23 days	Report number (“RN”)
3	18/8/2007	5 years 2 months 12 days	- Ditto -
4	26/10/2007	5 years 4 days	- Ditto -
5	8/1/2008	4 years 9 months 22 days	- Ditto -
6	6/3/2008	4 years 7 months 24 days	- Ditto -
7	17/4/2008	4 years 6 months 13 days	- Ditto -
8	14/7/2008	4 years 3 months 16 days	- Ditto -
9	30/10/2008	4 years	- Ditto -
10	1/4/2009	3 years 6 months 29 days	- Ditto -
11	14/7/2009	3 years 3 months 16 days	- Ditto -
12	18/10/2009	3 years 12 days	- Ditto -
13	31/1/2010	2 years 9 months	Blank
14	21/4/2010	2 years 6 months 9 days	Not signed, RN
15	4/8/2010	2 years 2 months 26 days	RN
16	29/10/2010	2 years 1 day	- Ditto -
17*	9/1/2012	9 months 21 days	- Ditto -

* The 17th notebook had been returned and subsequently withdrawn from storage on 9 January 2012.