CORRESPONDENCE AND OFFICE PRACTICE 2/01

12-02 Correspondence - General

Classified documents shall not be transmitted by FAX except where an encryption device is fitted on both the transmission and the receipt terminals.

2. Major Formation Commanders shall issue Standing Orders concerning the delivery of immediate correspondence within their Major Formations out of office hours.

12-03 Handling of Correspondence

Formations may deal direct with Government Departments (Government Secretariat excluded) on routine matters within the framework of existing policy. However, matters concerning the initiation of new policy or the variation of existing policy shall be referred to PHQ.

2. If correspondence is received direct by a Formation on a contentious policy or major issue, the papers shall be referred to the Major Formation Commander before a firm reply is sent.

12-04 Correspondence with the Public 6/02 06/11 07/21

Where it is anticipated that a reply cannot be made within ten calendar days of receipt of correspondence from a member of the public, an interim reply shall be sent and an endorsement made on the correspondence to show that this has been done. The interim reply shall be signed and include the contact telephone number of the officer handling the matter.

2. As a normal rule, all letters to members of the public are to be despatched on the date that they are signed. Should a Formation anticipate a time lapse between the preparation and the signing of the letter, it may adopt the practice of leaving the day numeral blank for the signatory to complete after he has signed the letter.

12-05 Correspondence with the Legislative Council and District Councils

01/07
14/18 Correspondence from the Legislative Council Secretariat, Secretary General or individual Legislative Councillors addressed to the Commissioner shall be forwarded to the appropriate Major Formation Commander directly for action. Correspondence on complaints against the police or allegation of misconduct against a member of the Police Force shall be referred to CSP C&IIB for action. Staff complaints from civilian grades referred to the Police by members of the Legislative Council shall be dealt with by CEO E&C, except where disciplined officers are the subject of complaints in which case the matter shall be referred to CAPO for investigation/follow-up.

01/07 2. Correspondence with District Councils shall be dealt with by the District Commander concerned. Matters concerning existing Force policies shall normally be referred to the Major Formation Commander who will, if necessary, refer them to the appropriate Programme Manager for advice/action. Matters involving complaints against the police shall be forwarded to CAPO.

12-06 Correspondence with Other Government Departments and Other Outside Authorities

Except as provided for in PGO Chapter 27 or in FPM Chapter 12, a police officer, other than one acting in the execution of his duty, shall not address the Chief Executive, the Chief Secretary for Administration, a Government Secretariat Secretary or a Head of a Department direct on any matter. Such correspondence shall be addressed through the Commissioner.

01/07
10/08 ## 12-07 Correspondence with Solicitors Representing Members of the Force

Letters received from solicitors employed by disciplined and civilian members of the Force on matters arising out of disciplinary proceedings shall be referred for action to the ACP P (Attn.: SP Discipline) and PCS (Attn.: SEO P&A) respectively.

12-08 Legal Advice on Disputes - Correspondence with Solicitors

01/07 Whenever it appears that a dispute concerning the Government is likely, the matter shall be referred to the Police Legal Adviser:-

(a) when correspondence, or any other form of communication, is received from solicitors acting on behalf of a person in dispute with a Government Department;

(b) when correspondence is received which appears to be drafted by a solicitor or concerns matters of a legal nature; or

(c) prior to any reply to or discussion with solicitors or their clients concerning the future conduct of legal proceedings.

12-10 Records Management

10/16
06/18

Policy Statement

Records* are valuable resources to support evidence-based decision making and to meet operational and regulatory requirements, and are essential for an open and accountable government. *The Force is committed to implementing the government's record management policy for effective and efficient management of government records as well as identification and preservation of archival records.

2. The Force policy on records management applies to all staff responsible for the creation, collection, management and disposal of records. It also applies to all recordkeeping systems, including paper-based systems and electronic information systems, which are used to keep and manage records.

3. The following laws and government policy/ regulations have implications on the Force's records management programme:-

(a) Evidence Ordinance (Cap. 8) – e.g. proper keeping of records to ensure its legal admissibility;

(b) Personal Data (Privacy) Ordinance (Cap. 486) – e.g. timely destruction of personal data in accordance with Privacy Commissioner Office's Code of Practice on Human Resource Management;

(c) Limitation Ordinance (Cap. 347) – e.g. retention of relevant records for the specified limitation periods to serve as evidence in possible legal proceedings;

(d) Electronic Transactions Ordinance (Cap. 553) – e.g. admissibility of electronic records in a court of law;

(e) Code on Access to Information – e.g. proper organization of records to facilitate their efficient retrieval to timely respond to public access requests;

(f) Government Security Regulations – e.g. Chapters 1 and 4 on handling classified documents; and

(g) General Circular No. 2/2009 – "Mandatory Records Management Requirements".

* A record is any recorded information or data in any physical format or media created or received by an organization during its course of official business and kept as evidence of policies, decisions, procedures, functions, activities and transactions.

Roles and Responsibilities

4. All officers have a role in enhancing records management in the Force. The following officers are assigned with specific roles and responsibilities:-

(a) Police Civil Secretary (PCS) oversees records management in the Force.

(b) Departmental Records Manager (DRM)

Chief Executive Officer (Personnel & General) (CEO P&G) is designated as the DRM of the Force and is responsible for assisting in establishing and implementing the Force's records management programme.

(c) Assistant Departmental Records Managers (ADRMs)

ADRMs are appointed to assist the DRM to monitor records management activities in the Force. Major Formation/ Regional Senior Executive Officers (SEOs) are the ADRMs for their respective Policy Wings and Regions.

(d) Records Managers (RMs)

RMs are assigned to control the creation, naming and coding of new files to facilitate accurate capturing and ready retrieval of records. Each Formation shall appoint officers not below the rank of Inspectorate/ Executive Officer II or equivalent as RMs to oversee records management matters in the registries of each Formation/ office.

(e) Registry Staff

Registry staff are responsible for the daily records management activities in their registries.

(f) Records Users (i.e. Subject Officers)

Records users are responsible for creation/ collection of and defining the access control for records in their daily business.

Recordkeeping

5. All records shall be captured into official recordkeeping systems, but not personal spaces/ systems (e.g. personal folder, e-mail in-box), to ensure the proper establishment and management of the following records management processes:-

(a) Creation/ collection and capture of records;

(b) Registration of records;

(c) Records classification;

(d) Records storage and preservation;

(e) Access to records;

(f) Tracking movement of records; and

(g) Retention and disposal of records.

Vital Records

6. Vital records are records containing information essential to the continued and effective operation during and after an emergency or disaster. Formations should identify their specific vital records having regard to their unique functions and responsibilities. Except for those Formations that are responsible for emergency services, vital records normally constitute about 1-5% of all records kept by each Formation.

Handling of Graded Documents

7. Files or extracts from files shall only be copied or passed to other officers on a "need-to-know" basis and in accordance with Security Regulations. Under no circumstances should they be copied or passed to any non-Government body except in accordance with the Code on Access to Information. 10/08

8. Documents relating to crime or investigations shall not be accessed by any unauthorised person. Case files and papers shall not be copied or passed to any person or any non-Government body other than in accordance with Force Policy or the authority of a Chief Superintendent of Police or above.

9. Formations may refer to FPM 12-10A for evidence of receipt. 01/07

01/07 **12-13 Data Administration**
06/11

The Crime and Crime Incident Headings abbreviation lists shall be used for Crime Report messages. Amendment, addition or deletion from these two lists shall not be made without the endorsement of the ACP CRIME.

12-15 Requests for Police Documents

Copies of Certified Documents supplied by Police

Each page of a copy of any statement or other document supplied to any person shall be endorsed 'Certified Copy' by an officer of Inspectorate rank or above who shall sign and date the endorsement under his name and designation.

CAPO Matters

2. CAPO files have public interest immunity and the Police Legal Adviser's advice shall be sought before release of documents.

Civil Matters

3. In response to a request from a member of the public for a copy of police document, an officer shall first obtain the approval from the District Access to Information Officer/ District Executive Officer. The District Access to Information Officer/ District Executive Officer shall then decide whether the document may be disclosed or withheld under the Code on Access to
06/11 information and the provisions of the Personal Data (Privacy) Ordinance (PD(P)O), Cap. 486.

4. A member of the public shall not be permitted to inspect a police report book or other official document without permission from an officer of the rank of Superintendent.

5. A police officer who receives a subpoena calling for the production of police documents should seek advice from the D of J if it is thought that the disclosure of the documents will harm or prejudice the public interest.

Security Organizations and Detective Agencies

6. Security organizations and detective agencies shall be treated in the same manner as private individuals. Information which would normally be provided to a private individual on request, may be provided to such organizations and agencies on request, except that information of a confidential nature, or which relates to a current police inquiry shall not be provided. In any case of doubt, the SP in charge of a Formation will direct whether and to what extent such a request will be acceded to.

12-16 Handling of Documents Containing Personal Data

01/07 10/08 10/10 07/21

Nothing in this order exempts officers from complying with the 'Regulations of the HKSAR - Volume V Security Regulations' ("the Security Regulations") which detail the requirements for the handling of classified documents.

Personal Data (Privacy) Ordinance ("PD(P)O"), Cap. 486 06/11

2. Data Protection Principle ("DPP") 4 of the PD(P)O requires all data users to take all practicable steps to ensure that personal data held are protected against unauthorized or accidental access, processing, erasure or other use, having particular regard to:- 06/11

(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.

3. The term "data user" refers to both the officer actually using, controlling, holding or processing the data and the Force.

Liability

4. Under s. 65 of the PD(P)O, and in respect of civil proceedings, any act done or practice engaged by an employee shall be treated as also done or engaged by the employer, whether or not such is done or engaged with the employer's knowledge or approval. It is therefore possible for both the employee and the employer to be named as defendants in a civil claim filed by a third party affected by the act done or practice engaged. However, it will be a defence under such proceedings for the employer to prove that such steps as are practicable have been taken, such as the issue of internal orders and reminders, to prevent the employee, in the course of employment, from doing an act, or engaging in a practice which may lead to an unauthorized disclosure or access, e.g. scanning and uploading an official document which contains personal data onto a website to which the members of public have access. 06/11

Responsibility

Major Formation Commanders ("MFCs")

5. MFCs are responsible for ensuring that both the PD(P)O and the Security Regulations are strictly complied with when handling manual files, records, documents and any other material which contain personal data.

Owners of Computerized Data Systems

6. Owners of computerized data systems, as defined in the Force Information Security Manual ("FISM") including any non-network systems, are responsible for ensuring compliance with this order in respect of the systems under their control.

Formation Commanders

7. Formation Commanders (not below the rank of SP) may, based upon this order and the Security Regulations (in particular Chapter III and IV), devise their own orders for handling documents which contain personal data. In doing so, due considerations shall be given to the requirement of DPP 4 (highlighted in paragraph 2 above) and the classification of the documents.

All Officers

06/11 03/15 8. When dealing with documents which contain personal data, they must comply with the PD(P)O, PGO/FPM 76 "Personal Data (Privacy) Ordinance and Code on Access to Information" and the provisions in this Order.

Marking of Documents Containing Personal Data

06/11 9. Documents containing personal data should be marked "PERSONAL DATA – 個人資料 ". This is to ensure that the officers who use, control, hold or process such documents are aware that the documents contain personal data and that they are required to take all reasonable steps to prevent any unauthorized disclosure or access.

Carriage of Documents Containing Personal Data

10. Documents which contain personal data shall not be removed from the workplace (including the office and general registry) in which they are kept unless such documents are required for the official duty that the officer is discharging, e.g. brought to another police premises for an official meeting.

11. Documents which contain personal data may only be taken away by an officer other than in the course of duty, e.g. taken home whilst off duty, when the officer has obtained prior written permission from his/her Immediate Supervisor (not below the rank of Inspector, or SSGT, in the absence of an Inspector in the sub-unit/team).

Police Notebooks

12. A blanket approval is given to officers attached to a crime formation or SDS who are required by the nature of their duty to carry with them their police notebook other than in the course of duty.

13. A Formation Commander (not below the rank of SP) who considers that officers under their command are engaged in any other duties that have a genuine need for them to routinely take their police notebook away from their workplace (including office and general registry) other than in the course of duty may consider giving written approval to those officers. If approval is given, it shall be reviewed regularly and no less than once every six months.

14. Officers who are not covered by an approval described at paragraph 14 and 15 above but are required to remove their police notebooks from the workplace shall seek prior written permission from their immediate supervisor (not below the rank of Inspector, or SSGT, in the absence of an Inspector in the sub-unit/team).

Unclassified/General Documents Containing Personal Data

15. Officers, if required to remove from their workplace unclassified or general documents which contain personal data other than in the course of duty (e.g. taking home whilst off duty), shall seek approval from their immediate supervisor (not below the rank of Inspector, or SSGT, in the absence of an Inspector in the sub-unit/team).

16. Immediate supervisors when considering request(s) for permission for removing from the workplace documents which contain personal data other than in the course of duty shall personally consider each request separately based upon the individual circumstances including the security arrangement, as follows:-

(a) whether the removal of the document(s) concerned by the officer from the workplace is essential for the officer to discharge relevant official duties;

(b) the physical location where the document(s) will be stored after having been removed from the workplace; and

(c) any security measures incorporated (whether by automated means or otherwise) into the storage location stated in (b) above.

17. If permission is given, it shall be in writing, examples of which include PEN message, memo or a countersigned entry in the police notebook of the officer given the permission.

Classified Documents Graded 'RESTRICTED' or 'CONFIDENTIAL' Containing Personal Data

18. Officers who are required to remove classified documents graded RESTRICTED or CONFIDENTIAL from the workplace other than in the course of duty shall seek prior written permission from their Formation Commander (not below the rank of SP).

19. In considering such request for permission, the Formation Commander (not below the rank of SP) shall consider the following:-

(a) whether the removal of the classified document(s) concerned by the officer from the workplace is essential for the officer to discharge relevant official duties;

(b) the physical location where the classified document(s) will be stored after having been removed from the workplace; and

(c) any security measures incorporated (whether by automated means or otherwise) into the storage location stated in (b) above.

Safekeeping of Documents Containing Personal Data

20. In order to maintain the integrity of documents which contain personal data, officers shall make reference to and comply with the DPP 4 of the PD(P)O. All documents which contain personal data shall be kept in a manner that will prevent any unauthorized disclosure or access. 06/11

21. In addition, the Security Regulations [Chapter IV 'Control of Classified Documents (196 & 197)] requires that all Classified documents graded RESTRICTED and CONFIDENTIAL are to be secured in the following manner:-

(a) CONFIDENTIAL documents must be kept in a steel cabinet fitted with locking bar and padlock;

[Note: The Government Security Officer has exempted the Force, in respect of the personal charge USB Thumb Drive with e-Cert encryption key, from complying with SR 359(a) which requires that confidential information stored on removable media must be kept in a steel filing cabinet fitted with locking bar and padlock when not attended, or when not in use. Officers are allowed to keep their personal charge USB thumb drives containing confidential information in a secure locked drawer or cabinet in their office but the office is to be locked when not attended. For officers working in a shared office, sufficient access control should be in place to prevent entry of unauthorized persons or members of the public. The officer should be the only key holder to the locked drawer/cabinet holding the USB thumb drive. The e-Cert encryption key (i.e. the e-Cert file drive) for processing confidential information is to be kept separate from the USB thumb drive and the key to the locked drawer/cabinet].

(b) RESTRICTED documents must be kept:-

(i) in a locked steel filing cabinet; or

(ii) in an office which is locked up after office hours and to which members of the public do not have access. 06/11

Transmission of Documents Containing Personal Data

22. When any documents which contain personal data are faxed, it is incumbent on officers faxing the documents to ensure that the intended recipient is ready at the receiving end to collect the document. Following the transmission, the officer shall follow up with a telephone call to confirm that the documents have been received.

Disposal of Documents Containing Personal Data

06/11
03/15 23. Once the purpose (including any directly related purpose) for which the personal data (contained in the documents) are to be used is fulfilled, the documents shall be shredded before disposal, unless otherwise exempted by the PD(P)O. Reference shall be made to the guidelines issued by the Government Logistics Department.