College of Professional and Continuing Education

Guidelines on
Handling Staff Personal Data

Human Resources Office

June 2006

Table of Contents

Chapter 1

Data Privacy Compliance and Responsibilities of Unit Personal Data Officers

a. Data Privacy Compliance.

The Personal Data (Privacy) Ordinance ("Privacy Ordinance") places a legal duty on all units and staff of the College of Professional and Continuing Education (CPCE) to properly handle personal data relating to other members of staff.

Unit personal data officers have been appointed from each unit throughout the CPCE for the purposes of ensuring that the staff personal data is handled consistently and in accordance with the Privacy Ordinance and the policies and Guidelines issued by the CPCE.

These Guidelines have been compiled for the purpose of enabling staff who handle staff personal data to comply with the requirements of the Privacy Ordinance.

By reason that the Privacy Ordinance imposes criminal liability on both the CPCE and individual staff who fail to comply with the statutory requirements applying to personal data, it is the responsibility of unit personal data officers to ensure that all staff who handle staff personal data within each unit fully observe these Guidelines.

b. Responsibilities of Unit Personal Data Officers.

The responsibilities of the Unit Personal Data Officers include:

1. Ensuring that all staff personal data is collected by the unit in a manner and for a purpose that does not contravene the Privacy Ordinance.

2. Implementing procedures within each unit to enable staff personal data to be maintained accurately and kept up to date.

3. Taking appropriate steps to ensure that staff personal data is retained by each unit for a period no longer than is necessary to fulfill the purpose for which the personal data was collected.

4. Ensuring that staff personal data is used by each unit for only those purposes for which the data was collected.

5. Implementing measures to ensure that staff personal data that is held by each unit is held securely so as to protect such data against unauthorized or accidental accessing, processing and erasure.

6. Circulating policies and practices relating to staff personal data throughout each unit including the notification of information concerning the kind of personal data held and the main purposes for which such data is held.

7. Co-ordinating data access requests made by staff seeking access and/or corrections to personal data held by each unit.

8. Acting as a liaison officer between the CPCE and its other units.

9. Generally to ensure that each unit fully comply with all policies, Guidelines and legal requirements applying to the handling of staff personal data.

c. What are the consequences in not complying with these Guidelines?

These Guidelines have been compiled to enable units to comply with their legal obligations in handling staff personal data. Staff (including unit personal data officers) who are found not to have complied with these Guidelines may be subject to disciplinary proceedings and/or termination of employment in appropriate cases.

Failure to fully comply with these Guidelines could also result in an investigation by the Privacy Commissioner ("PCO") and legal proceedings being commenced against the CPCE.

The PCO has the power to investigate suspected breaches of the Privacy Ordinance either on complaint being made or on his own initiative.

Responding to an investigation undertaken by the PCO can be a time-consuming and costly matter for the CPCE.

In addition, in the event of the PCO coming to an adverse decision in any investigation involving the CPCE, such a finding would clearly not reflect well on the responsible staff or the CPCE as a whole.

An adverse finding by the PCO could also be used against the CPCE in any subsequent legal proceedings involving the subject-matter of the investigation.

Both criminal and civil legal proceedings may be commenced in the event of there being any failure to comply with the Privacy Ordinance. Some criminal offences are punishable by a fine and in some cases imprisonment.

d. Who is liable for non-compliance?

The CPCE is liable for any non-compliance with the Privacy Ordinance with respect to any staff personal data that it controls, holds, processes or uses.

Because the CPCE acts through its agents, officers and employees, the CPCE will also be liable for any breach of the Privacy Ordinance caused through any act or omission on the part of its staff concerning personal data.

An individual officer or employee of the CPCE may be held personally liable for any unauthorised act or omission relating to staff personal data that is controlled, held, processed or used by the CPCE. For example, if a staff member, for personal reasons, discloses staff personal data to a third party, the staff member concerned may be held personally liable for any breach of the Privacy Ordinance.

e. Where can I go for additional advice?

The Human Resources Office (HRO) is the office designated to co-ordinate the functions and activities of other unit personal data officers throughout the CPCE.

Unit personal data officers can contact the HRO officer serving their respective units in the event of requiring further advice or guidance on their responsibilities as a unit personal data officer.

Chapter 2

Staff Personal Data

a. What is staff personal data?

For the purposes of these Guidelines, staff personal data may be regarded as any information:

- that is recorded in any document, and,
- that relates to any:
    - job applicant (present or past)
    - staff member (part-time, temporary or full-time)
    - former staff member
    - honorary and visiting academic staff members, and,
- that directly or indirectly identifies such job applicants, staff members, former staff members, honorary or visiting academic staff members.

For the purposes of these Guidelines, staff personal data does not include the personal data of students.

b. Common examples of staff personal data.

Staff personal data takes a wide range of forms, common examples of staff personal data likely to be encountered within a unit include:

- photographs of staff
- personnel records
- staff identity cards
- medical records
- payroll records
- job applications
- staff references
- staff appraisals

- minutes of staff committee meetings
- minutes of course meetings
- student evaluations of staff
- curriculum vitae
- e-mail exchanges between staff and other third parties
- video tape recordings

c. Categories of staff personal data.

The categories of staff personal data typically take many forms such as:

- Statements of fact concerning staff: e.g. completed conference application forms; grant application forms; staff leave records; staff disciplinary proceedings; staff resignation notices, etc.
- Statements of both fact and opinion: staff evaluations; records of a recruitment board's assessment of a job applicant's suitability for employment or promotions; minutes of staff or course committee meetings, etc.

d. Location of staff personal data.

Staff personal data is typically located in numerous different locations within a unit. Common examples of where staff personal data is located include:

- general office
- head of unit's office
- course supervisor's office
- administrative officer/executive officer's office
- within individual offices of teaching staff
- internal or external storage facilities
- shared with other units within the CPCE

e. The Data Protection Principles.

The main requirements of the Privacy Ordinance are set out in six data protection principles ("the DPPs"), which are reproduced in **Appendix A.**

The DPPs may be summarised as follows:

DPP 1: Rules applying to the collection of staff personal data

DPP 2: Accuracy requirement and duration of retention of staff personal data

DPP 3: Rules governing use of staff personal data

DPP 4: Security requirements in handling staff personal data

DPP 5: Openness requirement relating to staff personal data policies and practices

DPP 6: Compliance with requests for access and correction of staff personal data

Each one of these six principles is explained in further detail in the chapters that follow.

Chapter 3

Data Protection Principle 1 (DPP1): Collection of staff personal data

Guideline 1 **Data may only be collected if necessary but not excessive.**

Staff personal data may only be collected by a unit if such data is both:

- necessary for, or directly related to, the staff-related purpose for which the data is collected, and
- adequate, but not excessive, for carrying out that purpose

Guideline 1 Compliance Requirement (a):

To comply with Guideline 1 it is necessary that a review be undertaken of every form or document generally used within each unit that is used to collect staff personal data to ensure that the collection process meets the above requirements of necessity and non-excessiveness**.**

While it is the responsibility of each unit personal data officer to ensure that such a review is undertaken, in practice, it will be sufficient if such a review is undertaken under the supervision of a unit personal data officer.

Guideline 1 Compliance Requirement (b):

While it will not usually be feasible for a unit personal data officer to ensure that every form or document used within each unit to collect staff personal data complies with the requirements of necessity and non-excessiveness, it is the responsibility of the unit personal data officer to ensure that staff within the unit are made aware of such requirements.

A statement reminding staff of their obligations under this Guideline should be posted up in a prominent place within each unit.[1]

Guideline 1 Compliance Requirement (c):

[1] See Appendix B for a sample statement.

The necessity and non-excessiveness requirements do not apply only to the collection of staff personal data using forms and documents. They also apply to where staff personal data is collected by the compilation of notes and records of oral interviews and meetings. When conducting interviews for staff management purposes, keep the questions relevant to the purpose of the interview.

Guideline 1 Compliance Requirement (d):

Where unsolicited staff personal data of a job-seeker is received by a unit, steps must be taken to ensure that such data is only used for assessing that applicant's suitability for employment or a directly related purpose.[2]

Guideline 1 Compliance Requirement (e):

The collection of staff personal data of a job applicant concerning the applicant's health by means of a pre-employment medical examination may not be undertaken by a unit any earlier than at the time of making a conditional offer of employment and only if:

- the staff personal data concerned is relevant to determining whether the applicant is medically fit to undertake the inherent requirements of the job

- the offer of employment is conditional upon applicant undergoing the medical examination[3]

Guideline 1 Compliance Requirement (f):

Staff personal data relating to the health condition of any employee must not be collected by a unit unless the purpose for which the data is to be used is directly related to either:

- an assessment of the employee's suitability for continued employment; or

- the administration of the CPCE's medical scheme or provision of other benefits or payment of compensation[4]

[2] para: 2.4.2.1 of the Code of Practice on Human Resource Management
[3] para: 2.9.1 of the Code of Practice on Human Resource Management

[4] para: 3.2.4 of the Code of Practice on Human Resource Management

When the health condition of staff is collected, it is necessary to ensure that the staff concerned are informed of the CPCE's policy covering medical checking[5]

Guideline 1 Compliance Requirement (g):

The collection of information about a job applicant's family may only be undertaken by a unit to the extent that is necessary for the purpose of determining whether any conflict may arise if the applicant is offered the job.[6]

Guideline 1 Compliance Requirement (h):

The collection of staff personal data to facilitate integrity checking must not be undertaken by a unit unless:

- the data is important to the CPCE in relation to the inherent nature of the job for which the employee is appointed
- the collection is undertaken in accordance with the CPCE's policy covering such practices
- the employee concerned has been informed of the policy[7]

Illustration of DPP1 Guideline 1:

The application form that XYZ Unit requires staff to complete in order to attend overseas conferences necessitates the inclusion of details of the applicant's family members.

The application form used by PQR Unit for recruitment purposes requires job applicants to provide details of their religion.

Unless both units can demonstrate a valid need to be provided with such information, the collection of data relating to family members or religion by both units would be regarded as excessive and unnecessary.

[5] para: 3.2.5 of the Code of Practice on Human Resource Management
[6] para: 2.2.5 of the Code of Practice on Human Resource Management

[7] para: 3.2.3 of the Code of Practice on Human Resource Management

Guideline 2 **Data may only be collected by means that are lawful and fair.**

The means by which staff personal data is collected within each unit must be both lawful and fair.[8]

Guideline 2 Compliance Requirement (a):

Each unit needs to ensure that both lawful and fair means are used to collect staff personal data. For example, if a unit wishes to monitor which Internet sites staff visited, such an exercise might be regarded as unfair unless staff were informed beforehand that their on-line activities were being monitored.

Illustration of DPP1 Guideline 2:

Danny Leung is a lecturer in XYZ Unit. Danny has consistently refused his head of unit's request for him to provide details of his home address and mobile telephone number to allow his unit to maintain contact with him.

Gillian Mok, who is the administrative officer of the unit, obtained Danny's contact details from his wife by pretending that Danny had won a free holiday to Japan. Danny's wife had provided his home address and mobile telephone number after being assured that that information was to be used only for verification purposes.

Gillian's method of collection would not be regarded as either lawful or fair under the provisions of the Privacy Ordinance

.

Guideline 3 **Manner of collecting data.**

As a general rule, staff personal data should only be collected by a unit in the following manner:

- directly from the individual who is the subject of the data
- from third parties with the knowledge of the individual who is the subject of the data
- in accordance with established CPCE, unit procedures that are known (or capable of being known) to the individual: e.g. the CPCE performance appraisal system.

[8] Data Protection Principle 1(2)

DPP1 Guideline 3 compliance requirement 1:

As a general rule, staff personal data from third parties should not be collected:

- without the knowledge of the individual who is the subject of the data, or
- other than in accordance with established CPCE or unit procedures that are known, (or capable of being made known), by the individual.

Guideline 3 Compliance Requirement (a):

Staff personal data may be collected:

- from third parties without the knowledge of the individual who is the subject of the data, or
- other than in accordance with established CPCE or unit procedures that are known (or capable of being known) to the individual

only if the collection can be justified because of some overriding public interest reason that is recognised by the Privacy Ordinance. For example, if at an early stage of an investigation of an allegation of wrongdoing against a staff member the investigation would be compromised by informing the individual of the investigation, it would be justifiable to collect the staff personal data for the purposes of the investigation without the knowledge of the individual concerned.

If there is any doubt about whether it is justifiable to collect staff personal data without the knowledge of the individual who is the subject of the data, the unit personal data officer should seek advice from the HRO.

Illustration of DPP1 Guideline 3:

TUV Unit received an employment application from Eddie Ho. Eddie's application named two referees. Without either consulting Eddie or informing him that it wished to do so, the unit contacted the referees for the purposes of obtaining written references.

Unless the unit suspects, on reasonable grounds, that Eddie is, or was, engaged in some wrongdoing it should not have contacted the referee without informing Eddie of that fact.

Guideline 4 Job advertisements.

Advertisements for job vacancies must not be placed by a unit, whether directly or through an agency, unless they identify the CPCE (or its agent) as the party placing the notice.[9]

Illustration of DPP1 Guideline 4:

HIJ Unit placed an advertisement in the Economist seeking to recruit staff without stating the name of the CPCE. Guideline 4 will be contravened by reason that the advertisement did not state that the CPCE was the employer.

Guideline 5 **Genuine vacancy requirement.**

An advertisement for a job vacancy within a unit must not be placed unless there is, or will be, a vacancy of the sort advertised.[10]

Illustration of DPP1 Guideline 5:

EFG Unit is considering running a course on biotechnology in the new year. In order to ascertain how many qualified biotechnologists there were available in the marketplace, the unit ran a "dummy" advertisement that requested applications for a non-existent post.

The unit has contravened the Guideline 5 by advertising a non-existent position.

Guideline 6 **Notification requirements on collecting data.**

Whenever staff personal data is collected directly from an individual who is the subject of the personal data, the individual concerned must be informed of various matters in the form of a printed personal information collection statement.[11]

Guideline 6 Compliance Requirement (a):

The information to be included in the personal information collection statement that must be provided on or before collecting staff personal data includes:

9 para: 2.3.3 of the Code of Practice on Human Resource Management
10 para: 2.3.4 of the Code of Practice on Human Resource Management
11 Data Protection Principle 1(3)

- Details of the purpose or purposes for which the staff personal data is to be used.
- Details of the classes of persons (if any) outside the CPCE to whom the staff personal data may be transferred.
- Details whether it is obligatory or voluntary for the individual to provide the data unless this is obvious from the circumstances.
- Details if it is obligatory for the individual to provide the data, the consequences in the event that the individual fails to do so.[12]

Guideline 6 Compliance Requirement (b):

The information in the personal information collection statement that must be provided before the staff personal data is used includes:

- Notification of the right of individuals to request access to, and correction of, their personal data.
- Notification of the name and address of the person to whom such requests should be made.[13]

Guideline 6 Compliance Requirement (c):

Every form (including on-line forms) used throughout each unit to collect staff personal data, must include either a personal information collection statement or a sufficient reference to a personal information collection statement.[14]

Guideline 6 Compliance Requirement (d):

While it is permissible for a personal information collection statement to be stated in general terms by making explicit reference to other more detailed personal information collection statements or staff personal data policies issued within the unit or CPCE, it is the responsibility of each unit personal data officer to ensure that such

[12] See Appendix C for a sample of Personal Information Collection Statement

[13] See Appendix C for a sample of Personal Information Collection Statement

[14] See Appendix C for a sample of a Personal Information Collection Statement and Appendix D for a sample of a reference to Personal Information Collection Statement

personal information collection statement or policies are made readily available to all individuals from whom staff personal data is collected.[15]

Illustration of DPP1 Guideline 6:

BCD unit operates a clinic which staff of the CPCE and members of the public are permitted to attend.

The unit requires individuals who attend the clinic to complete a form detailing personal data.

The unit had previously posted up a personal information collection statement in the reception area. During the course of renovations the statement was inadvertently removed.

In this example, the unit no longer complies with the Privacy Ordinance by reason that staff and members of the public are not in any way informed of the purposes for which their personal data is collected.

Guideline 7 Collection of staff personal data in interviews.

The personal information collection statement requirements also apply to the collection of staff personal data as a result of face-to-face interviews or meetings, i.e. where personal information given by an interviewee is recorded in a record or summary of the interview or meeting.

Guideline 7 Compliance Requirement (a):

Where an interview is preceded by the completion of a form, such as may occur in the case of a job application, it should be made clear in the form that the personal information collection statement also applies to the collection of staff personal data in any subsequent interview arising from the application. Alternatively, an appropriately worded personal information collection statement may be included in a letter inviting the job applicant to an interview.[16]

Guideline 7 Compliance Requirement (b):

[15] See Appendix C for a sample of a PICS and Appendix D for a sample of a reference to Personal Information Collection Statement

[16] See Appendix C for a sample of Personal Information Collection Statement that included a statement of purpose in the event of the form being processed or given further effect.

If an oral interview is undertaken as part of an internal staff management process, such as a performance appraisal process, an appropriately worded personal information collection statement should be included in the guidance material relating to the process. It should be made clear in the material that the personal information collection statement applies to all aspects of the process, including the interview.[17]

Illustration of DPP1 Guideline 7:

KLM Unit included a personal information collection statement in its research application forms but made no reference to such a statement during the course of conducting oral interviews with staff whose research proposals had been short-listed.

In order for the unit to properly comply with Guideline 7 it is necessary to bring a personal information collection statement to the attention of staff attending the interview.

The unit's failure could result in a compliant being made to the PCO.

Guideline 8 Collection of staff personal data through job advertisements.

The personal information collection statement notification requirements also apply to the collection of staff personal data by means of a job advertisement.

Guideline 8 Compliance Requirement (a):

Any advertisement for a job vacancy that directly solicits the submission of personal data by job applicants, must either:

- include a personal information collection statement in the advertisement; or
- invite the applicants to respond by completing a job application form that includes a personal information collection statement; or
- include in the advertisement an appropriate statement.[18]

Illustration of DPP1 Guideline 8:

[17] See Appendix E for a sample of Personal Information Collection Statement

[18] para: 2.3.2 of the HR Code and see Attachment F for a sample of such a statement

CDE Unit advertised vacancies in a local newspaper with the statement. "All personal information provided by candidates for the purposes of this recruitment exercise will be used solely for the purposes of this exercise."

By reason that this personal information collection statement is sufficiently explicit the notification provisions of Guideline 8 will have fully complied with.

Guideline 9 Sharing data.

In the event that a unit shares staff personal data with other units make sure that the fact is brought to the attention of the individual from whom the personal data is collected.

Guideline 9 Compliance Requirement (a):

If it is intended to share staff personal data that is collected directly from an individual with other units within the CPCE, as a matter of good practice, the individual concerned ought to be informed of such an intention. It should be noted that consent of staff is not required. For example, it is sometimes the case that a unit may wish to share the personal data of staff for the purposes of course validation. If so, the applicants should be informed of such a practice in advance.[19]

Illustration of DPP1 Guideline 9:

IJK Unit has a close relationship with the TLM Unit, which operates as a separate and distinct entity within the unit.

For some years, the unit has freely exchanged staff personal data with the unit without the knowledge or consent of staff employed by the unit.

In order to comply with the Guideline, the unit ought to inform staff that staff personal data is shared with the unit.

[19] See Attachment C for a sample of such a statement

Chapter 4

Data Protection Principle 2 (DPP2): Accuracy of staff personal data

Guideline 1 **Accuracy of data.**

It is necessary for units to take all reasonably practicable steps to ensure that staff personal data is accurate having regard to the staff management purpose for which the data is to be used.[20]

Guideline 1 Compliance Requirement (a):

To ensure that the personal particulars of staff personal data (whether full-time, part-time or temporary staff) is accurate, it is necessary for each unit to institute a system of periodic reminders to the staff to submit updates of the information they have previously provided. As a general rule, an annual or, better still, six-monthly circulation of such a reminder should be sufficient.

Guideline 1 Compliance Requirement (b):

The accuracy of staff personal data that is of significance to a decision-making process should be subjected to cross-checking. For example, claims about an individual's qualifications should be checked against original certificates or with the authority granting the qualification concerned. Past work experience should be checked against references from past employers. Before a unit undertakes any such checks it is necessary that such staff or applicants are informed that checking of that kind may be undertaken.

Illustration of DPP2 Guideline 1:

PQR Unit collected data concerning Winifred Leung in 1983 when she first joined the unit. The unit recently received a request from the Official Receivers Office requesting specific data concerning Winifred. Prior to releasing such data to the Official Receiver, the unit must undertake a review of Winifred's data to ensure that it is accurate and up-to-date.

[20] Data Protection Principle 2(1)(a)

Guideline 2 **Data correction or erasure.**

Where there are reasonable grounds for believing that staff personal data is not accurate, such data must not be used until the data is either corrected or erased.[21]

Guideline 2 Compliance Requirement (a):

Where staff personal data that is used within a unit is found to be inaccurate a note must be attached to the data that contains the information indicating that the data is inaccurate together with a statement that the data must not be used pending clarification or correction of the inaccuracy.

Illustration of DPP2 Guideline 2:

KLM Unit has implemented a practice whereby it retains personal data relating to former employees for two years after their employment terminates. The unit has adopted a procedure whereby the following statement is affixed to the personnel files of staff whose employment has terminated: "The content of this file must not be used or disclosed in any way unless the information contained herein is able to be verified as being up to date."

In the event of staff only releasing staff personal data after the accuracy of its contents have been verified, the requirement of Guideline 2 will have been fully complied with.

Guideline 3 **Third party disclosures.**

Where it is apparent that inaccurate staff personal data has been disclosed to a third party, (i.e. a person outside the CPCE), the third party concerned must be informed of such inaccuracy and provided with the necessary information to enable it to correct the data.[22]

Guideline 3 Compliance Requirement (a):

It is important that a unit complies with the Guideline concerning third party disclosure requirements as any failure to do so may give rise to an offence. For example, if a unit makes a correction to staff personal data as a result of a data correction request and the data has been disclosed to a third party within the previous 12 months, the unit is

[21] Data Protection Principle 2(1)(b)

[22] Data Protection Principle 2(1)(c)

required to supply the third party with a copy of the corrected data and a notice stating the reasons for the correction within 40 days of receiving the request *unless* there is reason to believe that the third party has ceased to use the data for the purpose, or a directly related purpose, for which the data was disclosed.

Illustration of DPP2 Guideline 3:

After releasing personal data relating to Julian Tai to the Inland Revenue Department, VUW Unit discovered that there were a number of inaccuracies in the data disclosed. In order to comply with the Guideline it is necessary for the unit to inform the IRD of such inaccuracies.

Guideline 4 Collection of Identity Card numbers and other personal identifiers.

Identity card numbers may only be collected within each unit in either one of the following ways:

- by means of physical production of the identity card in person by the individual holder
- by accepting the number as shown on a copy of the identity card which the individual holder chooses to provide rather than present his identity card in person
- first accepting the number as furnished and later, but before using it for any purpose, checking its accuracy and authenticity by means of the physical production of the identity card in person by the holder, or if that is not reasonably practicable, by means of a copy of the identity card provided by the individual holder[23]

The same requirements also apply to the collection of other personal identifiers, (e.g. a passport number), for a staff management purpose.[24]

Guideline 4 Compliance Requirement (a):

Collection of copies of identity cards. A copy of an identity card of a job applicant must not be collected unless and until the applicant has accepted an offer of employment by the relevant unit.[25]

[23] para: 2.4 of the Code of Practice on Personal Identifiers

[24] para: 4.4 of the Code of Practice on Personal Identifiers

[25] para: 2.2.4 of the Code of Practice on Human Resource Management

Guideline 4 Compliance Requirement (b):

Whenever a copy of an identity card of an individual who has accepted an offer of employment is collected by a unit, it is necessary to check the copy against the identity card as produced by the individual concerned.[26]

Illustration of DPP2 Guideline 4:

MNO Unit insists that job applicants must provided copies of their Hong Kong identity cards with their job applications. While the unit is entitled to inspect job applicants' identity cards at a secondary stage, it has no right to insist on obtaining copies of applicants' identity cards at the initial recruitment stage.

By reason that such a requirement is not consistent with Guideline 4, the unit risks facing a complaint being made to the PCO.

Guideline 5 Duration of retention of HR Personal Data.

Staff personal data must not be retained for any longer than is necessary to carry out the staff management purpose, or a directly related purpose, for which the data was collected.[27]

By way of exception, staff personal data is not required to be erased where:

- erasure of such staff personal data is prohibited by law, (e.g. under the Employment Ordinance an employer is required to retain certain employment for the previous six months)
- it is in the public interest (including historical interest) for the data not to be erased.[28]

Guideline 5 Compliance Requirement (a):

Staff personal data collected for the purpose of recruitment of an individual who is not accepted for employment by a unit should not be retained for longer than two years following the rejection of such applicant's application.[29]

---

[26] para: 3.5 of the Code of Practice on Personal Identifiers

[27] Data Protection Principle 2(2) and s 26(1)

[28] s. 26(1)

[29] paras: 1.3.3.1 & 2.10.1 of the Code of Practice on Human Resource Management

Guideline 5 Compliance Requirement (b):

Staff personal data relating to a former employee must not be retained for longer than seven years from the date the employee ceases to be employed by a unit.[30]

Guideline 5 Compliance Requirement (c):

Staff personal data retained after termination of employment may be retained for longer than the above periods if the individual concerned has given express and voluntary consent for this or there is a continuing reason that obliges the unit to retain the data for a longer period.[31]

Illustration of DPP2 Guideline 5:

The employment of Jasmine Sze was terminated in 1993 by reason of her misconduct. Because litigation commenced by Sze against the unit is still on-going, it is permissible for the unit to retain her personal data longer than seven years. (It is suggested to delete as the requirement has been explained above and the guideline referring here is not clear.)

Guideline 6 Retention guidelines.

Unit personal data officers must compile unit guidelines specifying the retention periods that apply to staff personal data held by a unit. The retention periods may be determined by individual unit personal data officers on the basis of their experience in handling the type of data concerned and having regard to the requisite period of retention required to fulfil the purpose for which the data is to be used.

Guideline 6 Compliance Requirement (a):

The retention period applying to staff personal data should be set by reference to the completion of a particular process, such as a recruitment or promotion exercise, or by reference to a particular period of time, or a combination of the two.

[30] paras: 1.3.3.2 & 4.2.3 of the Code of Practice on Human Resource Management

[31] paras: 1.3.3.3 & 1.3.3.4 of the Code of Practice on Human Resource Management

Guideline 6 Compliance Requirement (b):

Once the retention period guidelines are devised, it is the responsibility of unit personal data officers to ensure that such guidelines are observed throughout the unit, though there may be exceptions based on individual circumstances, i.e. a need to retain staff personal data for longer than the guideline retention period because in the particular circumstances of the case or by reason that the particular purpose or purposes for which the data is being used has not been fulfilled.

Illustration of DPP2 Guideline 6:

TUR Unit has compiled guidelines laying down various rules governing the retention of staff personal data. The unit has strictly enforced compliance of these guidelines amongst administrative staff, but has not in any way attempted to ensure that teaching staff follow the guidelines.

By the reason that the Privacy Ordinance applies to all staff personal data held within the unit, it is necessary for the rules to be equally applied to both administrative and teaching staff alike.

In this example, the unit leaves itself open to a serious complaint being made to the PCO in the event of teaching staff not observing the Guideline.

Chapter 5

Data Protection Principle 3 (DPP3): Use of staff personal data

Guideline 1 **Use of data.**

Staff personal data collected for a staff management purpose, must not be used for any other purpose (or a directly related purpose), unless the individual who is the subject of the data gives consent which is:

- Consent that is expressly given by the staff concerned
- Consent that is voluntarily given
- Consent that has not been withdrawn in writing[32]

Guideline 1 Compliance Requirement (a):

While it is permissible for a unit to use staff personal data for any purpose that is a "directly related purpose" to a staff management purpose, whether or not such a use may be regarded as a directly related purpose will often entail a question of judgment. For example, using staff personal data for the purpose of defending court proceedings is likely to be regarded as a directly related purpose, using staff personal data to promote discounted commercial products to CPCE staff is not likely to be regarded as a directly related purpose.

Guideline 1 Compliance Requirement (b):

The prior consent of an individual must be obtained in the event of a unit wishing to use staff personal data for a purpose which is neither a staff management purpose nor a directly related purpose. It should be noted that staff cannot be compelled to provide consent. As a result, a serious breach of the Privacy Ordinance will occur in the event of staff personal data being used, without the consent of individuals concerned, for a purpose which is neither a staff management purpose nor a directly related purpose.

Guideline 1 Compliance Requirement (c):

[32] Data Protection Principle 3 & s. 2(3)

Even where an individual has consented to a unit using staff personal data for a purpose which is neither a staff management purpose, nor a directly related purpose, such consent may be withdrawn at any time in writing by the individual concerned.

Illustration of DPP3 Guideline 1:

HIJ Unit has been invited to make a bid to provide distance learning courses in China in conjunction with established mainland tertiary institutions. The information provided as part of the bid included the provision of personal data relating to staff working within the unit.

After the unit carelessly disclosed the personal data concerning its staff to a mainland marketing agency, it has subsequently discovered that staff have been deluged with marketing material.

While it is likely that using the personal data of staff to provide courses in the mainland would be regarded as a directly related purpose for which the data was collected from staff (i.e. for employment and teaching purposes), the unit would have difficultly in arguing that using such data for marketing purposes was a directly related purpose.

In this example, the unit would be liable to have a serious complaint made against it to the PCO for releasing personal data to the marketing agency.

Guideline 2 Use of data indirectly collected.

Where staff personal data has been collected for a staff management purpose from a third party source or compiled within a unit, it is important that the responsible staff of each unit who collects or compiles such data should be aware of the staff management purpose or purposes for which such data is to be used. The reason why this so is that the Privacy Ordinance requires that the consent of the individual who is the subject of the personal data must be obtained in the event of staff personal data being used for a purpose that is different from the purpose for which the data was collected.

Guideline 2 Compliance Requirement (a):

Where staff personal data is collected from a third party source or compiled within a unit, there is no requirement for the individual who is the subject of the personal data to be notified of the purpose or purposes for which such data was collected.

The fact that an individual does not need to be informed of the purpose for which personal data is being collected does not mean that the personal data that has been collected may be used for any purpose. For example, where a job reference is obtained from a third party and it is clear that the purpose for which it is used is to assess the suitability of an individual for a particular job, it is important that such data is not used for any other purpose, (or a directly related purpose), without first obtaining the applicant's express consent in writing. The individual whose consent is being sought must be given a choice to consent or not to consent. Even where an individual consents to personal data being used for a purpose that differs from the purpose for which the data was first collected, such consent may be withdrawn at any time.

Illustration of DPP3 Guideline 2:

Course leaders engaged by TUV Unit are required to compile reports on part-time staff teaching on the unit's evening classes.

Recently the unit has learnt that a course leader has improperly used the data of a part-time staff member for personal reasons.

In this example, the unit will be liable for a breach of the Guideline by reason that a personal reason is not a purpose for which the data was collected.

Guideline 3 Disclosure of staff personal data to a third party without the subject's consent.

Staff personal data may only be disclosed to a third party without the consent of the individual concerned if the purpose for which the data is disclosed is the same purpose as, or a directly related purpose to the purpose for which the data was collected.

Guideline 3 Compliance Requirement (a):

Where staff personal data is collected from a third party source or compiled within a unit, there is no requirement for the individual who is the subject of the personal data to be notified in the event of such data being transferred to one or more third parties.

The fact that units do not need to informed staff of the third parties to whom staff personal may be transferred does not mean that such data may be transferred to any third party. Such data may only be transferred to a third party for the same purpose (or directly related purpose) for which the data was collected.

Illustration of DPP3 Guideline 3:

FGH Unit has compiled various staff appraisal reports concerning staff. Because the information used to compile the reports was not collected directly from staff the unit is under no obligation to inform staff of the purposes for which the reports were being compiled. Neither was the unit under any duty to inform staff to which third parties such reports might be transferred.

Soon after applying for a post at Metropolitan College, James So discovered that one of his staff appraisals had been disclosed to the college without his knowledge or consent.

By reason that James' appraisals had been compiled for the purpose of his employment within the unit, any disclosure to a third party without the consent of James would be regarded as a disclosure for a purpose other than a purpose for which the data was collected.

In this example, the unit ought first to have obtained the consent of James prior to disclosing his appraisals to the college. Even if James gave his consent he would have been entitled to withdraw that consent at any time.

Guideline 4 **Unsolicited personal data of a job-seeker.**

Where unsolicited personal data of a job-seeker is received by a unit, whether directly from the individual concerned or from a third party, such data must not be used for any purpose other than for assessing that individual's suitability for employment or a directly related purpose.[33]

Guideline 4 Compliance Requirement (a):

It is important to understand that each and every item of personal data that is collected by a unit must not be used for any purpose other than the purpose for which the data was collected. Where such a purpose has not been explicitly stated (as it must be where personal data is collected directly from staff) then such a purpose will need to be implied.

Illustration of DPP3 Guideline 4:

TUV Unit received an unsolicited job application from Benson Li. Benson recently discovered that personal data (including his photograph) relating to him had been used in brochures advertising staff vacancies within the unit.

[33] para: 2.4.2.2 of the Code of Practice on Human Resource Management

By reason that the implied purpose for which Benson's personal data had been collected was for the purposes of employment selection, the unit will be regarded as having used his personal data for an improper purpose in using his personal data for promotional purposes.

In this example, the unit will be regarded as having contravened the Guideline 4.

Guideline 5 Use of personal data of job applicants in future recruitment exercises.

Where units have in place a practice of retaining personal data collected from unsuccessful job applicants for reference in future recruitment exercises, as a matter of good practice, the applicants concerned must be informed of such a practice and given the opportunity to request that such personal data be not used for the purposes future recruitment exercises. So long as applicants are informed of such purpose there is no requirement to obtain the consent of applicants.[34]

Guideline 5 Compliance Requirement (a):

Where a unit has adopted a practice of retaining personal data for future recruitment exercises, a statement to this effect must be included in either the job advertisement or the application form.[35]

Illustration of DPP3 Guideline 5:

The recruitment advertisements and application forms used by OPQ Unit contain the following statement: "Any personal information that you provide may be used for other recruitment exercises undertaken either in this unit or elsewhere within the CPCE."

By reason that this statement will satisfy the information requirements of the Privacy Ordinance it is not legally possible for a job applicant to complain in the event of personal data being used for more than one recruitment exercise conducted by the unit or CPCE.

Guideline 6 Giving personal references.

Before any member of a unit gives a personal reference concerning a current or past employee of the CPCE, it is necessary to ensure that the individual who is the

[34] See note to para: 2.5.1 of the Code of Practice on Human Resource Management

[35] See Attachment G for a sample of such a statement

subject of the reference gives his or her express consent voluntarily (i.e. not under compulsion) to either the staff giving the reference or the employer requesting the reference.[36]

Guideline 6 Compliance Requirement (a):

It is common practice for employers to request a reference from previous employers without first obtaining the consent of the applicant in question. Units should first obtain the written consent of either the former employee directly or request that a copy of such consent be provided by the prospective employer who is requesting to be provided with such a reference. Units should make sure that they retain a copy of the consent that is provided by the former employee. It should be noted that just because a former member of staff gives his or her consent for a reference to be given, there is no legal requirement that compels a previous employer to provide any such reference.

Illustration of DPP3 Guideline 6:

RST Unit received a reference check request from BCD Co concerning a former employee. Annie Poon who is the unit's executive officer completed the reference check request form without enquiring whether the consent of the former employee had been given to either the unit or the prospective employer.

By reason that Annie has acted contrary to the Guideline her actions would be liable to be investigated in the event of a complaint being made to the PCO.

Guideline 7 Express consent required to be given to give references.

Before a unit seeks to obtain a personal reference of a job applicant, steps must be put in place to ensure that the applicant concerned has given express consent, on a voluntarily basis, for such a reference to be obtained.[37]

Guideline 7 Compliance Requirement (a):

In the event of a unit seeking to obtain a reference concerning a job applicant, steps should be taken to ensure that the applicant consents in writing to such information

[36] para: 3.7.1 of the Code of Practice on Human Resource Management

[37] para: 2.8.1 of the Code of Practice on Human Resource Management

being provided. Steps should also be taken to ensure that the applicant also authorises, in writing, for such reference to be provided by the former employer.

In the event of consent being obtained it should be retained on the successful applicant's file.

Illustration of DPP3 Guideline 7:

UVW Unit uses the following statement for the purposes of collecting references:

"I [here insert name] authorise UVW Unit to contact [here inset name of referee] for the purposes of providing an oral or written confidential reference. I further authorise [here inset name of referee] to provide such a reference to UVW Unit for the purposes of evaluating my job application."

By reason that the consent authorises one party to collect and one party to provide a reference, the terms of the authorisation satisfy the Guideline.

Guideline 8 Public disclosure of data prohibited without consent.

A unit must not publicly disclose any personal data of a successful candidate for employment unless:

- such a candidate has given consent to
- such a disclosure or such public disclosure is required by law or a statutory authority.[38]

Guideline 8 Compliance Requirement (a):

It is common for units to make public announcements concerning staff. For example, frequently staff newsletters will contain announcements or photographs of staff. Such announcements entail the disclosure of staff personal data. Units should ensure that the consent of staff is first obtained prior to making such announcements.

Illustration of DPP3 Guideline 8:

[38] para: 2.9.4 of the Code of Practice on Human Resource Management

LMN Unit recently issued a number of press releases concerning the appointment of a new head of unit. The unit issued the media releases without notifying or obtaining the consent of the individual concerned.

While it is unlikely that the head of the unit would complain of such publicity, the unit's action could always be the subject of an investigation (in the event of a complaint being lodged to the PCO) by reason that the unit has not complied with the Guideline.

Guideline 9 **Public announcements concerning former staff must not be excessive.**

If there is a need to make a public announcement that a former employee is no longer employed by a unit, (e.g. in a public announcement), no more than the minimum information necessary to identify the former employee concerned should be included in the notice. In particular, the former employee's identity card number must not be included in the notice.[39]

Guideline 9 Compliance Requirement (a):

While it is unlikely that a unit will take out newspaper advertisements to announce the departure of staff, in the event of such action being taken it is necessary to make sure that any personal data that is disclosed to any third party concerning a departing employee is kept to a minimum.

Illustration of DPP3 Guideline 9:

After the employment of Alison Mok was terminated, EFG Unit posted details of her departure on its website. The details not only included her name but also her Hong Kong identity card number and the fact that she was divorced.

While it is permissible for the unit to announce Alison's departure on its website by referring to her name, it is not permissible for the unit to post details concerning her marital status or identity card for the simple reason that such details are both excessive and unnecessary.

In this example, the unit will be regarded as being in serious breach of the Guideline.

[39] para: 4.6.1 of the Code of Practice on Human Resource Management

Chapter 6

Data Protection Principle 4 (DPP4): Security of staff personal data

Guideline 1 **Requirement to handle data in a manner that is secure.**

Each unit must take all reasonably practicable steps to ensure that staff personal data is protected against unauthorized or accidental access, processing, erasure or other wrongful use.[40]

Guideline 1 Compliance Requirement (a):

Each unit is required to undertake "all reasonably practicable steps" to keep staff personal data secure. The standard of the steps to be taken is essentially a relative one. Where personnel files are stored in securely locked cabinets, in a locked room, with restricted access, then it is likely that the standard will be met. If, by contrast, personnel files are kept in unlocked cabinets with unrestricted access, then clearly the standard will not be met.

Illustration of DPP4 Guideline 1:

HIJ Unit has adopted a practice whereby course leaders are responsible for recruiting part-time teaching staff and research assistants directly.

Recently a local newspaper ran a story in which hundreds of rejected applications for teaching and research assistant positions to the unit had been found on a Tuen Mun dump. The newspaper published photographs of a number of applications which disclosed the identity card numbers and photographs of the unsuccessful applicants.

In this example, the unit will be regarded as being in very serious breach of the Guideline. The fact that the unit has delegated its responsibilities to teaching staff will not operate as a defence. The CPCE and the unit would be liable for the actions of its staff.

Guideline 2 **Varying standards of security.**

[40] Data Protection Principle 4

In protecting the security of staff personal data, particular regard must be paid to:

- the kind of data and the harm that could result if security is breached;
- the physical location of the data;
- security measures (if any) incorporated into any equipment in which the data is stored;
- measures for ensuring the integrity, prudence and competence of persons having access to the data; and
- measures to ensure the secure transmission of the data.[41]

Guideline 2 Compliance Requirement (a):

Each unit must ensure that access to staff personal data is adequately monitored by the adoption of appropriate security controls. The degree of security required will obviously depend on the contents of the staff personal data involved. For example, the minutes of routine course committee meeting that contain personal data such as the name and unit of the members will require virtual no security, whereas the minutes of a disciplinary committee would generally require a much higher level of security to guard against accidental or unauthorised disclosure of personal data relating to the staff member who was the subject of the disciplinary proceedings.

Illustration of DPP4 Guideline 2:

UVW Unit has adopted a practice whereby biographical details of staff are included on the unit's website. While such a practice will not, by itself, contravene the Guideline, it will be necessary for the unit to carefully consider the consequences of posting specific information. For example, if the biographical details included the private telephones and residential addresses of staff, then the unit would in all likelihood be regarded as failing to comply with the Guideline by reason that such a disclosure (unless staff had given their express consent for such details to be included) would arguably amount to an unauthorised disclosure of staff personal data.

Guideline 3 Staff personal data held in a computer system.

[41] Data Protection Principle 4

Where staff personal data is held in a computer system within a unit, the security controls should include different account privileges based on a "need to know" and "need to use" basis. Only those staff with a need to have access to or use a particular category of personal data should be provided with the means to gain access to staff personal data, account names and passwords. An audit trail and auto detection of unsuccessful attempts to access the system should also be put in place.

The integrity of staff personal data in computer systems must be protected by up to date anti-virus software. Networked computer systems containing staff personal data must be protected against unauthorised access by secure firewall software.

Guideline 3 Compliance Requirement (a):

Each unit has a responsibility to ensure that there is proper security in place to protect staff personal data from being accidentally or wrongfully accessed. Even if the security of computers and computer systems is provided by another unit, the host unit remains primarily responsibility for taking adequate steps to make sure that computer based staff personal data remains secure.

Illustration of DPP4 Guideline 3:

Prior to his employment in WXY Unit terminating Joseph Lai had been employed as a senior computer technician. His position enabled him to gain access to personnel files stored on the unit's server.

After his employment terminated, Joseph was able to access the unit's computer system for the simple reason that his pass code had not been changed. As a result of him gaining access, Joseph was able to misuse data relating to the head and the dean.

The unit will be regarded as being in serious breach of the Guideline by reason that the unit had taken no action to prevent Joseph from gaining access to data after his employment had been terminated.

Guideline 4 Staff personal data in hard copy form.

Where staff personal data is held in hard copy form within a unit, access to such data must also be controlled on the basis of a "need to know" and "need to use" basis by the use of lockable cabinets, safes and secure areas and strict control exercised over the distribution of keys and entry codes.

Guideline 4 Compliance Requirement (a):

The fact that a unit has in place security measures will be of limited assistance in the event that such measures are not properly implemented. Even if security measures are implemented they must be implemented in such a way as to prevent accidental or wrongful disclosure. For example, if staff personal data, such as personnel files, that are kept inside a safe located inside a locked room can be accessed by any staff of the unit, such unrestricted access would not be regarded as sufficient security.

Illustration of DPP4 Guideline 4:

Using the same facts in the illustration immediately above, had Joseph been permitted to have limited access to personnel data of staff during his employment, such limited access might have also contravened the Guidelines in the event of Joseph being able to gain unlimited (and unauthorised) access by virtue of his technical knowledge. This is by reason that the unit ought to have in place adequate security measures that would either prevent or detect Joseph obtaining unlimited access to such personnel files.

Guideline 5 Copying of documents containing staff personal data.

Documents containing staff personal data must not be copied unless it is necessary for carrying out the staff management purpose for which the data is used. When that purpose is fulfilled, the copies must be destroyed. For example, if it is necessary to copy promotion board papers for each member of the board, once the promotion exercise is completed, a system should be in place to ensure that the copies are returned to the secretary of the board for destruction.

Guideline 5 Compliance Requirement (a):

The requirements limiting copying and requiring the destruction of copies of staff personal data apply equally to soft copies as to hard copies.

Staff within a unit should be encouraged not to make copies, whether hard or soft copies, of staff personal data simply for their own convenience in carrying out their duties. The practice of copious copying not only compromises the security of the data but it also compromises compliance with the requirements of the Privacy Ordinance which requires the destruction of personal data whenever the purpose for which such data was to be used has been fulfilled.

Illustration of DPP4 Guideline 5:

As a result of undertaking a wide range of course validations the staff of CDE Unit have accumulated multiple copies of validation documents and e-mails

containing staff personal data relating to hundreds of staff and former staff both within and outside the unit.

In order to properly comply with the Guideline it is necessary for the unit to put in place a system that results in surplus documents and e-mails held by all staff being purged as soon as the purpose for which such information was collected has been fulfilled.

Guideline 6 **Display of identity cards not permitted.**

Units must **not** publicly display details of any Hong Kong identity card number together with the name of the identity card holder.

Units are permitted to authorise persons who need to carry out recognised activities to require production of both the name of the holder and details of such a holder's Hong Kong identity card number.[42]

Guideline 6 Compliance Requirement (a):

The restrictions that apply to the public display of staff names and Hong Kong identity cards and Hong Kong identity card numbers together do not apply to the display of staff names and staff numbers that are not in any way based on Hong Kong identity card numbers.

While it is permissible to authorise staff (e.g. security staff) to require staff to produce their names and a Hong Kong identity card number, it is not permissible for such details to be accessed by unauthorised persons.

Illustration of DPP4 Guideline 6:

LMN Unit allows staff to obtain after hours access only on condition that they provide written details of their names and Hong Kong identity card. Details of staff are openly displayed at the guard station at the entrance to the unit.

While the unit is permitted to collect both the names of staff and their Hong Kong identity cards if such data is not publicly displayed, the unit may only publicly display either a name or a Hong Kong identity card.

The Guideline prohibits the unit from publicly displaying both items of staff personal data together.

---

[42] para: 2.7 of the Code of Practice on Personal Identifiers

In this illustration, the practice of the unit contravenes the Guideline.

Guideline 7 **Staff identity cards must not display Hong Kong identity card number.**

Units must **not** issue any staff card to an individual for a staff management purpose that displays such individual's Hong Kong identity card number.[43]

Guideline 7 Compliance Requirement (a):

While it is not permissible to issue staff cards that display an individual's Hong Kong identity card number in a legible form, there is nothing to prevent a unit to include a Hong Kong identity card number in a non-legible (e.g. digitalised) form on staff cards.

Illustration of DPP4 Guideline 7:

TUV Unit has issued staff identity cards that incorporate their Hong Kong identity card numbers in the form of a digitalised bar code.

By reason that the identity cards are not displayed in a legible form the requirements of the Guideline will be fully complied with.

Guideline 8 **Copies of Hong Kong identity cards must be marked with a "copy" chop.**

Where units collect copies of Hong Kong identity cards for staff management purposes, such copies must be clearly and permanently marked over the image of the identity card with the word "copy" (or other similar words) in the presence of the individual holder where the copy is made in that individual's presence.[44]

Guideline 8 Compliance Requirement (a):

[43] para: 2.8 of the Code of Practice on Personal Identifiers

[44] para: 3.9 of the Code of Practice on Personal Identifiers

The marking of an individual's Hong Kong identity card number may be undertaken in English or Chinese and any form of words may be used to indicate that the card has been copied. The marking on the copy may be by means of a stamp or handwriting.

Illustration of DPP4 Guideline 8:

As a matter of practice throughout the OPQ Unit, all copies of identity cards that are collected within the unit are chopped with the word "copy" immediately upon such cards being copied.

This practice satisfies the requirements of the Guideline.

<u>Guideline 9</u> Hong Kong identity cards must be treated as confidential.

Within each unit, copies of Hong Kong identity cards must be treated as confidential documents and kept under secure conditions with access being only permitted to staff members who need to carry out activities related to the permitted uses of such copies.[45]

<u>Guideline 9 Compliance Requirement (a):</u>

It is important that units take adequate steps to ensure that copies of Hong Kong identity cards are kept secured regardless of where such copies are stored. By reason that the practice of using copies of Hong Kong identity cards for the provision of services is so widespread in Hong Kong, there is much opportunity for the misuse of unsecured copies of Hong Kong identity cards belonging to staff.

Illustration of DPP4 Guideline 9:

Theresa Lai recently discovered that a copy of her Hong Kong identity card that she had provided to the GHI Unit had been use without her authority to collect a prize of three Gucci travel bags that she had won in a competition. She learned that the bags had been handed over to an unknown person using her identity card and purporting to be acting on Theresa's behalf.

On the assumption that Theresa could prove that the unit had not taken proper care of the copy of her identity card, it would always be open for her to look to the unit for compensation by reason of its failure to comply with the Guideline.

---

[45] para: 3.11 of the Code of Practice on Personal Identifiers

Guideline10 Liability for breaches of Privacy Ordinance by third parties.

The CPCE is liable for any breach of the Privacy Ordinance by a third party engaged by it to undertake activities on its behalf that involve the handling of staff personal data. It is a defence for the CPCE to argue that all reasonably practicable steps have been taken by the CPCE to prevent the breach. Examples of third parties that may be engaged by the CPCE to carry out data handling activities on its behalf include employment agencies, data processing contractors and document storage companies.[46]

Guideline 10 Compliance Requirement (a):

Before a unit engages any third party to carry out any activity involving the handling of staff personal data, steps should be taken to ensure that there is sufficient awareness, facilities (including security facilities) and capability to enable staff to comply with the Privacy Ordinance. Any failure on the part of a unit to do so may entail the individual concerned and the CPCE being in serious breach of the Privacy Ordinance.

Guideline 10 Compliance Requirement (b):

Where staff personal data is handled by an employment agency on behalf of a unit details of the agency's own personal data privacy policies and practices should be requested to verify whether the agency has adopted appropriate standards.

Guideline 10 Compliance Requirement (c):

Where staff personal data is handled by data processing contractors or document storage companies, each unit's primary concern should be whether such third parties have the proper facilities to ensure that the staff personal data concerned is securely stored, processed or transmitted in a way that does not contravene the Privacy Ordinance.

Guideline 10 Compliance Requirement (d):

Where staff personal data is handled by any third party to carry out any activity involving the handling of staff personal data on behalf of a unit, any agreement that is

[46] s. 65

entered for the purposes of such handling ought to contain a term in a form similar to that of **Appendix H**.

Illustration of DPP4 Guideline 10:

The STU Unit entered a storage facility agreement with CDE Company. The agreement provided that: "In providing storage facilities, the storage company hereby agrees to fully comply with all relevant provisions of the Personal Data (Privacy) Ordinance."

The unit entered the storage agreement on the basis of that compliance term. Recently, the unit has discovered that highly sensitive staff personal data has been wrongfully disclosed to third parties by staff employed by the storage company.

The storage company is now relying on an exemption clause in the storage contract to avoid any liability "for any loss or injury (however caused)" resulting from the wrongful disclosure by it staff.

By reason that the unit has failed to comply with the Guideline in not taking adequate steps to ensure that staff personal data was properly secured, both the unit and the storage company would be liable for any loss or harm resulting from the wrongful misuse of the data concerned.

In this example, the exemption clause would not operate to allow the storage company to distant itself for the wrongful actions of its staff.

Chapter 7

Data Protection Principle 5 (DPP5): Openness about staff personal data policies and practices

Guideline 1 **Data policies and practices must be made available.**

Each unit must take all reasonably practicable steps to ensure that anyone can:

- ascertain a unit's policies and practices in relation to staff personal data
- be informed of the kind of staff personal data held by the unit
- be informed of the main purposes for which staff personal data is held by the unit is to be used[47]

Guideline 1 Compliance Requirement (a):

The requirement of openness in respect of data policies and practices rests primarily on the CPCE. Each unit is of course responsible for communicating such policies and practices both internally and to the world at large. For example, the College of Professional and Continuing Education Personal Data Statement in **Appendix I** should be prominently displayed both within each unit and also in the event of a unit undertaking external promotion of its functions and activities. Where appropriate, a suitable reference to such policies ought to be made as a matter of practice on communications entailing an exchange if information.

Illustration of DPP5 Guideline 1:

The reception area of LMN Unit has a prominently displayed a copy of the CPCE's Personal Data Statement. E-mails used by the unit contain the following statement:

Notice: Personal data that is included in this e-mail or attachment must only be used strictly in accordance with the provisions of the Personal Data (Privacy) Ordinance. For details concerning our personal data policies and practices see our Personal Data Statement which is available on http://www.polyu.edu.hk/.

[47] Data Protection Principle 5

The provisions of the Guideline will be sufficiently complied with in the event of the unit directly and indirectly providing information concerning its personal data polices and practices.

Chapter 8.

Data Protection Principle 6 (DPP6): Compliance with requests for access and correction of staff personal data

<u>Guideline 1</u> Rights of individuals to be provided with copies of data being held.

Where a unit receives a data access request from an individual (or person authorised to make such a request on behalf of such an individual) to either:

- be informed whether the unit holds any personal data of which the individual is the subject; or
- be provided with a copy of such data,

the unit concerned must comply with the request within 40 days of the receipt of such a request.[48]

<u>Guideline 2</u> Requirements to be followed in the event of a data access being received.

In the event of a unit receiving a data access request there are:

- various requirements that must be strictly adhere in granting access ("mandatory requirement")
- there are other requirements that may be insisted on as a condition for granting access ("permissible requirement")

<u>Guideline 2 Compliance Requirement (a):</u>

Where a unit receives a data access request it is necessary to clearly differentiate between the mandatory requirements and the permissible requirements that apply in granting access. The reason why such a distinction is important is by reason that the CPCE and the individuals handling the request will be in serious breach of the Privacy Ordinance even if the request is unintentionally mistaken as a mandatory requirement rather than as a permissible requirement.

[48] Data Protection Principle 6 & ss. 18(1) and 19(2)

Illustration of DPP6 Guideline 2:

In the event of XYZ Unit receiving a data access request, such a request must be refused by the unit if the identity of the person making the request is not able to be ascertained.

Such a request must also be refused where granting access would result in the disclosure of personnel data of one or more other individuals other than the person making the data access request.

By reason that such refusals are mandatory it is not permissible for the unit to grant access simply in order to keep the person making the data access request happy. XYZ Unit would be in very serious breach of the Guideline if it wrongfully granted one individual access to personal data belonging to another person.

Similarly, the unit would also be in serious breach of the Guideline in the event of granting data access to one individual and by doing so disclosing the personal data of one or more other individuals without their knowledge or consent.

Guideline 3 **Refusal of data access request.**

It is mandatory for a unit to refuse to comply with a data access request if the identity of the person making the access request cannot be properly established.

Guideline 3 Compliance Requirement (a):

It is a mandatory requirement that a unit must refuse a data access request if the identity of the individual making a data access request is not certain.

The responsibility for placed on a unit to properly ascertain that the person making the request is entitled to obtain access to the personal data requested is a particular heavy one.

For example, if the handling officer inadvertently gave copies of personal data relating to a member of staff to a third party posing to be that staff member, the CPCE and handling officer would be in very serious breach of the Privacy Ordinance especially where adequate steps to ascertain the true identity of the individual making the request had not been taken.

Guideline 3 Compliance Requirement (b):

Copies of personal data provided by a unit as a result of a data access request should only be released after the handling officer has physically sighted the Hong Kong identity card of the person making the data access request.

Failure to properly ascertain the identity of the person seeking access will leave the CPCE and handling officer liable for failing to comply with the mandatory requirement of properly identifying the identity of the individual making a data access request.

Illustration of DPP6 Guideline 3:

JKL Unit received a data access request from an individual purporting to be Y K Wan. After copies of the contents of Y K Wan's personnel files were released to the person making the request it was subsequently discovered that the request had in fact been made by Y K Wan's former wife.

The unit will be regarded as having been in serious breach of the Guideline unless the unit can show that it took all reasonable care not to grant wrongful access to the data that was disclosed.

The fact that the disclosure was made to the wrong person would imply that the unit and the handling officer had not taken sufficient care to satisfy itself as to the true identity of the person making the data access request.

Guideline 4 Further grounds for refusing data access request.

It is mandatory for a unit to refuse to comply with a data access request if by granting access to such data the personal data of another individual would be disclosed without the consent of that individual.

Guideline 4 Compliance Requirement (a):

It is a mandatory requirement that a unit to refuse a data access request by an individual if the personal data of some other individual would also be disclosed as a result on granting access to the personal data requested.

It is permissible to disclose personal data that results in the disclosure of one or more individuals in the event of such individual having either given their consent or were previously informed of such a possibility at the time of collection.

Illustration of DPP6 Guideline 4:

A group of job applicants was simultaneously recorded on a video tape by CDE Unit. In the event of one of the job applicants making a data access request to

be provided with a copy of such a video tape, it is not permissible for the unit to grant access to the video tape unless all the other job applicants agree to the tape being released to the person making the request.

The unit may, however, release a copy of the video tape to the individual making the request if the other individuals had been informed of that fact no later than the time when the video was filmed.

Guideline 5 **Circumstances where data access must not be refused.**

A data access request **must not** be refused on the grounds that such disclosure would entail the disclosure of personal data relating to some other individual if the personal data of that other individual is capable of being processed in such a way as not to result in disclosure.

Guideline 5 Compliance Requirement (a):

A unit must not refuse a data access request if the identity of one or more individuals can be processed in such a way as to avoid disclosure. For example, access to minutes of meetings that identified various individuals must be granted to an individual making the request in the event that it is possible for the other individuals' personal data to be deleted by black marking pen.

Illustration of DPP6 Guideline 5:

An individual has requested access to the minutes of a committee meeting which rejected that individual's research application. Prior to granting the individual access to the minutes, it would be necessary to delete the names of all other research applicants (and any other minutes that might identify each of those applicants) as well as the names of committee members (and any other minutes that might identify each committee member) before access to the committee meeting minutes was granted to the individual making the data access request.

Guideline 6 **Identifying source of data not a reason for refusing a data access request.**

The fact that an individual is indirectly identified or identifiable as the source of the personal data which is the subject of the data access request does not provide grounds for refusing a data access request.

Guideline 6 Compliance Requirement (a):

It is a mandatory requirement that a unit must not refuse a data access request if the identity of one or more individuals can be processed in such a way as to avoid explicit disclosure even though one or more individuals may be identified indirectly as the source of the personal data.

Illustration of DPP6 Guideline 6:

A staff member of TUV Unit knows that his annual appraisal had been compiled by his head of unit. The fact that the staff member concerned was aware that the head of unit had made the appraisal could not be relied on as a ground for refusing to provide the staff member with a copy of the appraisal.

So long as the head of unit's name or other explicit identifying features (e.g. reference to title or post of appraiser) was deleted, the staff member making the request must be given a copy of his annual appraisal.

Guideline 7 **Data access request may be refused where not made on prescribed form.**

A unit **may** refuse to comply with a data access request if it is not made using the form prescribed by the PCO for this purpose[49]

Guideline 7 Compliance Requirement (a):

It is a permissible requirement that a data access request may be refused by a unit in the event of a data access request not being made on the official form that has been prescribed by the PCO. (See **Appendix J**).

Where a data access request is made in any other manner than a prescribed form it is permissible for a unit to refuse the request.

Of course in the event of such a request being refused, it is always open for the requestor to make a further request on a prescribed form.

Illustration of DPP6 Guideline 7:

WXY Unit received a data access request from Tim Lo. The request requested access to "all information relating to me and my immediate family" that was held by the unit.

[49] s. 20(3)(e)

While it is permissible for the unit to grant access to Tim, it is legally preferable for the unit to insist on Tim using the official data access request form.

The reason for doing so is simply because the form encourages persons making data access requests to be far more specific concerning the requests that they make.

Guideline 8 **Data access request may be refused where relates to staff planning exercise.**

A unit **may** refuse to comply with a data access request that has been made in relation to staff personal data if:

- the data consists of information relevant to any staff planning proposal to fill any series of positions of employment; or
- the data could cease any group of individuals' employment[50]

Guideline 8 Compliance Requirement (a):

It is a permissible requirement whether or not a unit gives access to staff personal data that involves multiple planned positions or proposed redundancies.

Once the staff planning proposals have been put in place or the redundancies given effect it will not be possible to resist granting a data access requested on such grounds.

Illustration of DPP6 Guideline 8:

Gillian Tang has heard persistent rumours that her section of five staff is to be made redundant.

Gillian recently made a data access request to HIJ Unit seeking confirmation concerning such rumours.

By reason that proposed redundancies relate to more than one post, it is permissible for the unit to deny Gillian access to personal data relating to the proposal until such time as the redundancies have been implemented.

[50] s. 53

Guideline 9 **Data access request may be refused where data held for certain employment purposes.**

A unit may refuse to comply with a data access request that has been made in relation to staff personal data if the data concerned is the subject of a process for either:

- recruitment, appointment or promotion
- determining whether an individual should be removed from employment or office
- deciding on the award, continuation or cancellation of a contract; or
- deciding whether disciplinary action should be taken against an individual

The refusal to comply applies only for the duration of the process and if the outcome of such a process is subject to an appeal.[51]

Guideline 9 Compliance Requirement (a):

It is a permissible requirement that a data access request may be refused by a unit in the event of a data access request being made in respect of an uncompleted process which is subject to an appeal.

Illustration of DPP6 Guideline 9:

The employment of J S Chan was terminated by KLM Unit by reason of his serious misconduct.

Because the grounds for terminating the employment of J S's were not subject to a right of appeal, it would not be permissible for the unit to refuse to grant access to any personal data relating to the termination by reason of the Guideline.

Guideline 10 **Data access request may be refused where it relates to certain types of personal reference.**

A unit may refuse to comply with a data access request that has been made in respect of a personal reference concerning an individual's suitability for employment or appointment to an office.

---

[51] s. 55

A reference is treated as a personal reference only when it is given by an individual on a voluntary basis and not given in the course of the referee's employment.

A refusal to provide a copy of such a reference may only be made for so long as the employment position or office remains unfilled.

Once the position is filled it will be necessary to grant access to a copy of a personal reference.[52]

Guideline 10 Compliance Requirement (a):

It is a permissible requirement that a data access request may be refused by a unit in the event of a data access request being made to access a personal reference prior to a particular post being filled.

Illustration of DPP6 Guideline 10:

An unsuccessful job applicant who applied to be employed by GHI Unit made a data access request to be provided with a copy of a personal reference provided by the applicant's referee. By reason that the position remains unfilled it is permissible for the unit to refuse to provide the unsuccessful applicant access to that reference until such time as the post is filled.

Guideline 11

There are other exemptions from the requirement to comply with data access requests that are aimed at protecting the public interest in such matters as the prevention, detection and remedying of wrongdoing and unlawful conduct.[53]

Guideline 11 Compliance Requirement (a):

The Privacy Ordinance recognises a number of instances in which a data access request may be refused by a unit on specified grounds.

These exceptions are not discussed in these Guidelines. The HRO is able to discuss with handling officers whether an exception applies to allow the unit to refuse granting a data access by reason of such exceptions.

---

[52] s. 56

[53] s. 58

Illustration of DPP6 Guideline 11:

PQR Unit was provided with anonymous information alleging that M K Lo was undertaking concurrent employment at two tertiary institutions.

In the event of the unit receiving a data access request from M K it would be permissible for the unit to refuse to disclose any information relating to the anonymous letter by reason that such disclosure might alert him to the fact that the unit was currently investigating whether the contents of the letter were true.

Even if the contents of the letter were mistaken, the unit is still entitled to refuse to disclose the contents of the letter to M K by reason that disclosure of the letter might directly or indirectly identify the person who was the source of the information.

Guideline 12 Steps to be followed where data access request refused.

Requirements in the event of refusing data access request. In the event of a unit refusing to comply with a data access request the following steps must be taken:

- the person who made the request must be informed of the refusal and the reasons for the refusal within 40 days of receipt of the request.[54]

- the reasons for the refusal must be entered in a log book kept for this purpose.[55]

Guideline 12 Compliance Requirement (a):

Every unit must ensure that the following rules are observed in the event of a data access request being refused.

It is particularly important that the reasons for refusing access are valid and consistent reasons are given for the refusal within the statutory time-frame and that proper log book entries are made.

As a matter of practice, it is not at all an easy task to make a refusal in such a way that completely complies with the requirements of the Privacy Ordinance.

---

[54] s. 21

[55] s. 27

As a result, any failure to comply with these refusal requirements will result in a serious breach of the Privacy Ordinance being incurred that may well result in an investigation by the PCO.

Illustration of DPP6 Guideline 12:

PQR Unit received a data access request from Queenie Cheung. The data access request was made in respect of "all personal data held within the unit, included data held by all other staff members concerning me".

Simon Chan, the administrative assistant, refused to grant Queenie access to such data on the grounds that "our unit neither has the resources nor the authority to undertake a search throughout the unit in order to provide you access to the information that you seek."

While most administrators would be sympathetic with the stand taken by Simon, lack of resources or authority is not a recognised excuse for refusing access.

In this example, Simon would be liable to a serious reprimand from the PCO in the event of not taking all reasonably practicable steps to locate personal data held throughout the unit.

Guideline 13 Data correction request.

An individual (or person authorised to act on behalf of such individual) who has been provided with a copy of any staff personal data held by a unit as a result of a data access request is entitled to make a data correction request in the event that such personal data is found to be inaccurate.

A data correction request must be complied with by the relevant unit within 40 days of its receipt.[56]

Guideline 13 Compliance Requirement (a):

In the event of a unit receiving a data access request it is important that such inaccuracies are rectified within the permitted time.

Failure to rectify any inaccuracies with the permitted time will result in a serious contravention of the Privacy Ordinance being committed.

[56] Data Protection Principle 6 & s. 22(1)

Illustration of DPP6 Guideline 13:

As a result of making a data access request to BCD Unit, Angela Ng discovered that her personnel file stated that she had been legally separated since 1987.

In fact she was happily married. Angela now demands a written apology and for her personnel file to be corrected within seven days.

While the Privacy Ordinance makes no requirement for apologies to be given and allows a correction to be made within 40 days, it would be advisable for the unit in this example to bend over backwards to apologise and meet the seven days' correction demand by reason that Angela would have good grounds for complaining to the PCO in the event of any disclosure of incorrect data having been previously made by the unit.

Guideline 14 Refusal of data correction request.

A data correction request may be refused if a unit is not satisfied that the data is inaccurate.[57]

Guideline 14 Compliance Requirement (a):

In practice most factual statements are able to be proven to be accurate or inaccurate without much difficulty.

Illustration of DPP6 Guideline 14:

The statement "Jules is consistently the last person to come to work" may be easily verified by examining the attendance records of Jules and his colleagues. Such records would easily establish whether or not Jules is in fact consistently the last person to arrive at work.

On the assumption that the statement was factually accurate, in the event that Jules challenged the accuracy of such a statement, his employer would entitled to refuse to make any changes to such a statement in the event of Jules making a correction request.

Guideline 15 Corrections of expressions of opinions.

[57] s. 24(3)

If the data correction request relates to personal data that consists of an expression of opinion, it is necessary to annex a note to the data stating the matters the requestor considers to be inaccurate.[58]

Guideline 15 Compliance Requirement (a):

Personal data may take the form of expressions of opinion. An expression of opinion is defined to include any assertion of fact which is unverifiable or having regard to all the circumstances of the case, is not practicable to verify.

Special rules apply where staff personal data in the form of expressions of opinions are involved.

Illustration of DPP6 Guideline 15:

The statement "Gina does not appear to have a co-operative attitude", comprises an opinion of the individual making the statement rather than a verifiable fact.

In the event of Gina making a correction request which challenges the accuracy of that statement, the person who controls the use of the statement may refuse to change the statement by:

1. *Compiling a note summarising Gina's grounds for challenging the accuracy of the statement.*

2. *Attaching the note to the opinion in such a way that the opinion cannot be used without the note being brought to the attention of any person reading the opinion.*

3. *Providing a copy of the note to Gina.*

In summary, where the accuracy of an opinion is disputed, there is no requirement in law for such an opinion to be changed or modified in any way.

Guideline 16 Requirements to be followed in the event of refusing data correction request.

If a data correction request is refused, the following steps must be undertaken:

---

[58] s. 25(2)

- the person who made the data correction request must be informed of the refusal and the reasons for the refusal within 40 days of receipt of the request[59]

- the reasons for the refusal must be entered into a log book kept especially for such a purpose[60]

Guideline 16 Compliance Requirement (a):

A unit should ensure that it follows all rules that must be followed in the event of a data correction request being refused.

It is particular important that the reasons for refusing access are valid and consistent reasons, that the refusal is given within the statutory time-frame and that proper log book entries are made.

As a matter of practice, it is not at all an easy task to make a refusal in such a way that completely complies with the requirements of the Privacy Ordinance.

As a result, any failure to comply with these refusal requirements will result in a serious breach of the Privacy Ordinance being incurred.

Illustration of DPP6 Guideline 16:

TUV Unit has received a data correction request from Cindy Lai stating that her birth date has been wrongly entered in her personnel file and that the appraisal for the last year was factually biased.

While the unit has a legal duty to correct references to Cindy's birthday within a specified time, there is no legal requirement for the unit to change the content of the appraisal in the event that the unit forms the view that the accuracy of the appraisal is in fact verifiable.

In such circumstances, the unit will be entitled to refuse to change the appraisal and in the event of doing so must inform Cindy of those reasons for the refusal and record those reasons in a log book.

---

[59] s. 25(1)

[60] s. 27

Appendix A

Data Protection Principles

1. Principle 1 - purpose and manner of collection of personal data

(1) Personal data shall not be collected unless—

(a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;

(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and

(c) the data are adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are-

(a) lawful; and

(b) fair in the circumstances of the case.

(3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that—

(a) he is explicitly or implicitly informed, on or before collecting the data, of—

(i) whether it is obligatory or voluntary for him to supply the data; and

(ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and

(b) he is explicitly informed-

(i) on or before collecting the data, of—

(A) the purpose (in general or specific terms) for which the data are to be used; and

(B) the classes of persons to whom the data may be transferred; and

(ii) on or before first use of the data for the purpose for which they were collected, of—

(A) his rights to request access to and to request the correction of the data; and

(B) the name and address of the individual to whom any such request may be made,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6.

2. Principle 2 - accuracy and duration of retention of personal data

(1) All practicable steps shall be taken to ensure that—

(a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;

(b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used—

(i) the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data are erased;

(c) where it is practicable in all the circumstances of the case to know that—

(i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and

(ii) that data were inaccurate at the time of such disclosure, that the third party—

(A) is informed that the data are inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) Personal data shall not be kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data are or are to be used.

3. Principle 3 - use of personal data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than—

(a) the purpose for which the data were to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a)

4. Principle 4 - security of personal data

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.

5. Principle 5 - information to be generally available

All practicable steps shall be taken to ensure that a person can—

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user are or are to be used.

6. Principle 6 - access to personal data

A data subject shall be entitled to—

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data—

(i) within a reasonable time;

(ii) at a fee, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).

Appendix B

Collection of staff personal data

Staff are reminded that all staff (including both teaching staff and support staff) who collect or use personal data relating to their colleagues or other persons employed by the CPCE are required to use such data strictly in accordance with this Guidelines on Handling Staff Personal Data a copy of which is available [here insert details as to where a copy of the Guidelines can be found].

Disciplinary action may be taken against any member of staff who handles personal data in a manner which contravenes these Guidelines.

[name]

Unit Personal Data Officer

Appendix C

Personal Information Collection Statement

The information you provide in this form and subsequently in the event of this form being either processed or given further effect will be used for the purpose(s) of [state purpose or purposes].

The completion of all the fields of the form is obligatory. Failure to complete one or more of the fields may result in [state consequence].

The information you provide in this form may be disclosed to the following party or parties [state the party or parties concerned] as well as other units within the CPCE for one or more of the purposes specified above or a purpose that is directly related to any such purpose or purposes.

You have the right to request a copy of your personal data held by the CPCE and to request the correction of any inaccuracy in the copy of personal data that is provided to you in accordance with the Personal Data (Privacy) Ordinance and subject to the data privacy policy and administrative requirements of the CPCE.

Any such enquiry should be made to:

Unit Personal Data Officer,
[Name of unit]
College of Professional and Continuing Education
c/o The Hong Kong Polytechnic University
Hung Hom, Kowloon.

Appendix D

Reference to Personal Information Collection Statement

The information that is provided by you in this form will be used for the purposes as stated in the personal information collection statement that is available from [here state where a printed personal information collection statement may be obtained]. You should take time to read that statement as it also includes other important information concerning your rights and protections under the Personal Data (Privacy) Ordinance.

Appendix E

Personal Information Collection Statement for Staff Management Process

The information contained in this form may be used for any one or more of the following purposes, including staff appraisal, promotion, performance evaluation and other matters relating to your employment. Personal data that is subsequently collected from you that relate to the matters in this form may also be used for any one or more of the stated purposes.

Appendix F

Statement for Advertisement

Personal data provided by job applicants will be used strictly in accordance with the CPCE's personal information collection statement, a copy of which will be provided immediately upon request.

Appendix G

Statement for retaining personal data for future recruitment exercise

Personal data provided by job applicants may be retained for the purposes of future recruitment exercises.

Appendix H

Contract term for third party carrying out activities involving the handling of staff personal data

The [third party] hereby represents and warrants that in carrying out the contract it will comply with the requirements of the Personal Data (Privacy) Ordinance, Cap. 486 ("the Ordinance"), and acknowledges that any failure by it to do so will amount to a repudiatory breach of contract entitling the CPCE to terminate the contract forthwith.

Once the contract is fully performed or on its earlier termination the [third party] represents and warrants that it will destroy or cause to be destroyed, or deliver up or cause to be delivered up to the CPCE all personal data (as that term is defined in the Ordinance) in its possession, power or control as a result of carrying out the contract.

The [third party] shall indemnify and keep indemnified the CPCE against all liabilities, claims, costs, damages and expenses, including without limitation legal fees on an indemnity basis, incurred by reason of any breach of the above representations and warranties.

Appendix I

College of Professional and Continuing Education
Personal Data Statement

Kinds of Personal Data held by the CPCE

There are three general categories of personal data held by the CPCE. Those categories comprise personal data contained in:

Student information, which include records containing information supplied by data subjects and data users and collected in connection with student applications, students, former students, contacts and marketing activities undertaken by or on behalf of the CPCE.

Personnel information, which include personal particulars, job descriptions, details of compensation and benefits, performance appraisals, references and disciplinary matters relating to job applicants, employees and former employees of the CPCE.

Other records, which include administration and other files, containing personal data provided to the CPCE by individuals for purposes other than those connected with students, contacts, marketing or employment.

Main Purposes of the CPCE for keeping Personal Data

The main purposes for which personal data is held by CPCE are as follows:

Student records are kept for purposes that include corresponding with, responding to and taking follow-up action in respect of students, contacts and promotional activities.

Personnel records of employees are kept for human resource management purposes, relating to such matters as statutory requirements, employees' terms of employment, performance appraisal, providing references, discipline and termination.

Other records are kept to enable the CPCE to carry out various functions and activities which vary according to the nature of the purpose for which such records are to be used, including administration of the CPCE's functions and activities, seeking advice on operational matters, undertaking promotional and training activities organized by, or on behalf of, the CPCE, including the acquisition of services and handling of enquiries from members of the public.

College of Professional and Continuing Education Personal Data Policies and Practices

College of Professional and Continuing Education's personal data policies and practices are those that comply with the Personal Data (Privacy) Ordinance that are contained in this Statement and any other notices relating to personal data, being policies and practices as are in force and as amended from time to time.

Data subjects are entitled to request the CPCE to grant access and correction of personal data in accordance with the provisions of the Personal Data (Privacy) Ordinance for which the CPCE may impose a fee to access.

PERSONAL DATA (PRIVACY) ORDINANCE
DATA ACCESS REQUEST FORM

Important Notice

1. Please read this Form and the footnotes carefully before completing this Form.

2. This Form is specified by the Privacy Commissioner for Personal Data ("the Commissioner") under section 67(1) of the Personal Data (Privacy) Ordinance ("the Ordinance") with effect from 1 April 2008. According to section 20(3)(e) of the Ordinance, a data access request may be refused if it is not made in this Form.

3. Please complete this Form in the Chinese or English language. A data user may refuse to comply with a data access request under section 20(3)(a) of the Ordinance if the request is not in writing in the Chinese or English language. **The completed Form should be sent directly to the data user to whom this data access request is made,** and not to the Commissioner.

4. Section 18(1) of the Ordinance confers a right on the data subject to access his personal data held by a data user.

5. The requestor shall specify in sufficient details and clarity the personal data requested in order to facilitate location of the requested data by the data user. Failure to supply such information which the data user may reasonably require to locate the requested data may result in the data user refusing to comply with the data access request under section 20(3)(b) of the Ordinance.

6. A data user shall comply with the data access request in accordance with section 19(1) of the Ordinance **within 40 days** after receiving the request. The duty of the data user to comply with a data access request extends only to supplying a copy of the personal data of the data subject, and not to supply a copy of the document in which the data is contained.

7. If the data user is unable to comply or has valid ground to refuse to comply with the request pursuant to section 20 of the Ordinance, it shall in accordance with section 19(2) or 21(1) of the Ordinance give the requestor written notification of such matter and the reasons **within the same 40 days** period.

8. Failure of the data user to comply with the data access request in accordance with the requirements of the Ordinance may constitute an **offence** and an offender is liable on conviction to a fine at level 3 under section 64(10) of the Ordinance.

9. Where this Form contains a summary of the relevant requirements of the Ordinance, the summary is provided for reference purpose only. For the complete and definitive statement of the law, please refer to the Ordinance itself.

Part I: Data User
Particulars of the data user to whom this data access request is made

Name[1] *(full name in block letters)*: _____

(for the attention of [2] _____)

Address : _____

_____

Part II: Data Subject
Particulars of the data subject making this data access request

Name in English *(full name in block letters, surname first)*: _____

Name in Chinese: _____

Hong Kong Identity Card Number [3]: _____

Personal identifier (e.g. student number, staff number, medical card number, account number, or other reference number) previously assigned by the Data User for identification purpose (if any): _____

_____

Correspondence address: _____

_____

Day time contact phone number: _____

Part III: The Requestor
Name, correspondence details and capacity of the Requestor

[This part should only be completed if the Data Subject is not the Requestor]

Name in English *(full name in block letters, surname first)*: _____

Name in Chinese: _____

Correspondence address: _____

_____

Day time contact phone number: _____

This data access request is made in my capacity as a relevant person[4] on behalf of the Data Subject, in proof of which I enclose the following[5]:- _____

_____

[1] Please fill in the full name of the Data User to whom the data access request is addressed.

[2] If you have previously been informed by the Data User of the name or title of the person to whom such a data access request may be made, please fill in here the name and/or title of such person.

[3] For data subjects who are Hong Kong Identity Card holders. The identity card number needs not be provided in this Form if you have reasonable grounds to believe that this will not be necessary for the unique identification of the data subject by the data user in the circumstances.

[4] Under section 2(1) of the Ordinance, a "relevant person", in relation to an individual, means:
(a) where the individual is a minor, a person who has parental responsibility over the minor;
(b) where the individual is incapable of managing his own affairs, a person appointed by the court to manage those affairs; or
(c) in any other case, a person authorized in writing by the individual to make the data access request.

[5] Please fill in here details of any documentary proof of "relevant person" status, e.g. copy birth certificate, copy court order, written authorization, etc., which you will provide with the Data Access Request Form. Please see also paragraph (b) of Part VIII of the Form.

Part IV: The Requested Data

This data access request is made under section 18(1) of the Ordinance for the following personal data of the Data Subject, except those specifically excluded under Part V of this Form:-

Description of the Requested Data[6]: _____

_____

_____

_____

Date around which or period within which the Requested Data were collected (if known):

_____

The name of the branch or staff member of the Data User that collected the Requested Data (if known):

_____

Part V: Exclusions

For the avoidance of doubt, the Requested Data access to which is sought **do not include** any personal data[7]:

☐ contained in documents previously provided to the Data User by the Data Subject (e.g. letters to the Data User from the Data Subject)

☐ contained in documents already provided to the Data Subject by the Data User (e.g. letters to the Data Subject from the Data User or documents provided pursuant to a previous request)

☐ in the public domain (e.g. newspaper clippings or entries in public registers concerning the Data Subject)

☐ (other excluded personal data): _____

(Please tick and complete where appropriate)

Part VI: The Request

I hereby request you:-

☐ (a) pursuant to section 18(1)(a) of the Ordinance, to inform me whether you hold the Requested Data[8]

☐ (b) pursuant to section 18(1)(b) of the Ordinance, if you hold any of the Requested Data, to supply me with a copy of such Data that you hold[9]

☐ both (a) and (b)

(Please tick where appropriate)

---

[6] Please specify clearly and in details the personal data requested (e.g. personal data contained in appraisal reports, medical records, credit reports) including further information, if any, such as the particular incident in association with it, the circumstances under which the personal data were collected and held, etc. to facilitate location of the Requested Data. Too general a description of the Requested Data, such as "all of my personal data", may render the request being refused by the data user pursuant to section 20(3)(b) of the Ordinance in that the data user is not supplied with such information as it may reasonably require to locate the personal data in which the request relates.

[7] Please tick to exclude, as far as possible, any personal data that you do not wish to include within the scope of the Requested Data. This may help to avoid any unnecessary delay or charge in complying with the data access request.

[8] By ticking this box, the Requestor has indicated that he or she is requesting only for a confirmation of "Yes" or "No" as to whether the Data User holds the Requested Data and is not requesting for a copy of the Requested Data.

[9] By ticking this box, the Requestor has indicated that he or she is requesting only for a copy of the Requested Data. Where the Data User does not hold the Requested Data, the Data User is not obliged to notify the Requestor. It is therefore advisable to tick the box "both (a) and (b)" if the Requestor wishes to receive notification from the Data User.

Part VII: Preferred Manner of Compliance

In your complying with this data access request, I would prefer that you[10]:

☐ give me an indication, before processing my data access request, of any fee that may be charged for compliance with my request[11]

☐ notify me when a copy of the Requested Data is ready for collection

☐ send by registered mail a copy of the Requested Data to me at my address given in this Form

☐ send by ordinary mail a copy of the Requested Data to me at my address given in this Form

☐ supply to me a copy of the Requested Data in the_____language

☐ supply to me a copy of the Requested Data in the form of _____ (e.g. computer disk, microfilm, etc.)

(Please tick and complete where appropriate)

Part VIII: Further Information and Payment

I understand that before complying with my request, you may require me to provide[12]:

(a) proof of my identity;

(b) where I am making this request as a relevant person, proof of the identity of the Data Subject and further proof (if any) of my status as a relevant person;

(c) such further information as may be reasonably required for you to locate the Requested Data;

(d) payment of a fee charged under section 28 of the Ordinance.

Part IX: Use of Personal Data

Except with the prescribed consent of the individual concerned, the personal data provided in this Form will be used for the purpose of processing this data access request and for directly related purposes only.

_____ _____

Date Signature of the Data Subject/ Requestor*

(* Delete where appropriate)

[10] Please tick and fill in according to preference. However, compliance with the data access request may not be in the preferred manner where this is not reasonably practicable.

[11] Sections 28(2) and (3) of the Ordinance provide that a fee may be charged for compliance with a data access request under section 18(1)(a) or (b), which fee shall not be excessive. According to section 28(5) of the Ordinance, compliance with a data access request may be refused unless and until any such fee has been paid.

[12] Failure to provide the additional information as required may result in the data access request being refused, or not being complied with to the desired extent.