Published under Section 48(1) of the

Personal Data (Privacy) Ordinance (Cap. 486)

Inspection Report :

Personal Data System of the Student Financial Assistance Agency

Report Number: R14-3771

Date issued: 23 January 2014

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

This page is intentionally left blank to facilitate double-side printing

Report on the Inspection of the Personal Data System of the Student Financial Assistance Agency

This report of an inspection carried out by the Privacy Commissioner for Personal Data (the "**Commissioner**") pursuant to section 36 of the Personal Data (Privacy) Ordinance, Cap. 486 (the "**Ordinance**") in relation to the personal data system used by the Student Financial Assistance Agency ("**SFAA**") is published pursuant to section 48 of the Ordinance.

Section 36 of the Ordinance provides:-

"*Without prejudice to the generality of section 38, the Commissioner may carry out an inspection of-*

(a) any personal data system used by a data user; or

(b) any personal data system used by a data user belonging to a class of data users,

for the purposes of ascertaining information to assist the Commissioner in making recommendations-

(i) to-

(A) where paragraph (a) is applicable, the relevant data user;

(B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and

(ii) relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be."

The term "**personal data system**" is defined in **section 2(1)** of the Ordinance to mean "*any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system.*"

The relevant parts in **section 48** of the Ordinance provide:-

"*(1) Subject to subsection (3), the Commissioner may, after completing an inspection where section 36(b) is applicable, publish a report-*

(a) setting out any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(b) in such manner as he thinks fit.

……

(3) Subject to subsection (4), a report published under subsection (1)… shall be so framed as to prevent the identity of any individual being ascertained from it.

(4) Subsection (3) shall not apply to any individual who is-

(a) the Commissioner or a prescribed officer;

(b) the relevant data user."

Allan CHIANG
Privacy Commissioner for Personal Data

Table of Contents

Executive Summary

Introduction

1. The Student Financial Assistance Agency ("**SFAA**") is the executive agency of the HKSAR Government's policy on student finance. On average, SFAA receives over 956,000 applications per year for various student financial assistance schemes and over 8,000 applications per year for various scholarships, merit award and loan fund schemes. SFAA collects, holds, processes and uses a wide range of personal data including the name, Hong Kong Identity Card ("**HKID Card**") Number, date of birth ("**DOB**"), contact information, employment details, annual income, bank account details and education information of applicants and their family members.

2. Given the vast number of data subjects, the sensitive personal and financial data involved, as well as the continual role of SFAA in the administration of student financial assistance schemes, the Commissioner considers that it is in the public interest to carry out an inspection of the personal data system used by SFAA (the "**Inspection**") pursuant to section 36 of the Personal Data (Privacy) Ordinance (the "**Ordinance**") for the purpose of making recommendations to SFAA to promote compliance with the Ordinance. Other public bodies that collect personal data from members of the public for the purpose of providing financial assistance in a way similar to SFAA are encouraged to take reference from this report.

3. Instead of examining the personal data systems of all the schemes administered by SFAA, the Commissioner decided to focus efforts on the personal data system of four financial assistance schemes for primary and secondary students (the "**Identified Schemes**"), in view of the vast number of applications processed in the Identified Schemes (which represent nearly 75% of the total applications received by SFAA), the representativeness of the computer system used among the whole range of systems used by SFAA and the sensitivity of the personal and financial data involved.

The Inspection

4. The personal data system of SFAA in relation to the Identified Schemes was inspected. Specifically, the collection, retention, use and security of personal data were reviewed against the requirements under Data Protection Principles ("**DPPs**") 1 to 4 in Schedule 1 to the Ordinance.

5. The Inspection comprised a review of SFAA's relevant policies and procedures, making enquiries, site inspection, attending demonstrations by SFAA of data handling procedure and interviews with the relevant staff of SFAA in the period from 30 April 2013 to 5 August 2013.

Findings and Recommendations

6. The Commissioner is reasonably satisfied with the data protection measures in the personal data system of the Identified Schemes taking into consideration the large scale of operation and that no serious or major deficiencies were found during the Inspection. At the same time, the Commissioner has identified 15 issues to be addressed and his recommendations are summarised below:-

Collection of personal data

(1) For the purpose of processing financial assistance applications, SFAA collects a wide range of personal data from applicants and their family members, including the name, HKID Card Number, DOB, contact information, employment details, etc. Among the personal data collected, DOB of the applicants and their family members are used among other data to facilitate the checking of their particulars in the database of Education Bureau and Social Welfare Department. As HKID Card Number is already a reliable and unique data for identifying a person, the Commissioner questions the need to additionally collect DOB. He recommends SFAA not to collect DOB of the applicants and their family members if they can provide HKID Card Number. He accepts that year of birth may be collected for application vetting and statistical purposes.

(2) The application form does not specify the types of personal data that are mandatory for the applicants to supply and the consequences of not supplying such data. The Commissioner recommends specifying such details on the form.

Data retention

(3) There is no regular checking to ensure electronic data saved in individual staff's computers and network drive has been erased according to SFAA's data retention policy. The Commissioner recommends setting up a monitoring mechanism to ensure erasure has been properly carried out.

(4) SFAA permanently retains 35 types of data including individually identifiable personal data such as the English name, HKID Card Number and DOB of all applicants and their family members. The Commissioner recommends a review of such practice and anonymisation of the data where appropriate.

Use of personal data – identity verification

(5) SFAA does not provide staff with written guidelines prescribing the types of personal data that can be disclosed to a phone enquirer who claimed himself to be the applicant. Also, a caller only needs to provide his full name and HKID Card Number for verifying his identity as an applicant. The Commissioner recommends promulgation of clear guidelines to staff as to the types of data that may or may not be disclosed to a caller over the phone and implementation of more stringent identity verification procedures, for example, by requesting additional information from the caller.

Use of personal data – disclosure

(6) Given the small area of the enquiry room at the SFAA office, the Commissioner recommends that the SFAA's current practice of handling walk-in enquiries from one applicant family at any one time should be strictly followed to avoid the discussion of one case being overheard by others.

(7) After successful completion of the family-based assessment of eligibility, which takes into account an applicant's gross annual household income and household size, SFAA will issue an Eligibility Certificate to the eligible student, who has to follow up by submitting the Eligibility Certificate to his school to certify his student status and school attendance. The student reference number, his partial HKID Card Number, his name and DOB are printed on the Eligibility Certificate. Removal of the HKID Card Number and DOB is recommended as the student reference number is itself a unique personal identifier.

(8) The Commissioner considers it unnecessary to show the student's partial HKID Card Number and DOB, together with his name, on the letter notifying the applicant of the assessment results, and recommends the removal of such data from the letter.

Data security

(9) Upon lapse of the academic year in which the assistance has been disbursed, records are considered inactive and the paper files would be kept in SFAA's office for one year before being transferred to Government Records Service for storage for another two years. However, there is no activity update of the computer record for the file transfer to Government Records Service. As such, there is no audit trail for tracking the

movement of individual files to Government Record Services. The Commissioner recommends SFAA to ensure updating of the computer record of file activity status and conduct verification to ensure all paper files are passed to Government Records Service according to SFAA's data retention policy.

(10) SFAA carries out home visits to authenticate selected successful applications. The Commissioner recommends reviewing and minimising to the extent practicable the number of documents containing personal data an SFAA staff member brings outside the SFAA office for conducting home visits.

(11) Backup tapes of all IT systems of SFAA are regularly transported from one SFAA office to another for safe-keeping. However, such tapes are not encrypted. The Commissioner recommends encryption of all backup tapes that need to be transported to offsite storage.

Training

(12) SFAA is recommended to require staff of designated ranks and posts to attend IT security awareness training on a mandatory instead of the current voluntary basis.

Outsourcing of data processing

(13) SFAA engages a contractor to transcribe data provided in the application forms onto CDs (the "**Data Prep Contractor**"). SFAA conducted two inspections on Data Prep Contractor's premises during the period from March 2010 to March 2013. However, the inspections were conducted without the involvement of IT technical support. Besides, the inspection results were not documented and no check was conducted on

whether the data on the application forms had been completely erased by the Data Prep Contractor after the transcription process. The Commissioner recommends SFAA to involve IT technical support in future inspections of the Data Prep Contractor to ensure the relevant IT security measures are in place; document the results of inspection; perform random check to ensure data is not retained longer than necessary by the Data Prep Contractor; and establish a policy on the frequency of inspections (e.g. once a year) and review of the inspection results by management staff of sufficient seniority.

(14) In addition to the Data Prep Contractor, SFAA also engages other data processors such as couriers to transport documents containing personal data between different offices and within offices. The contracts with all data processors have not specified the reporting procedure for signs of abnormalities or security breaches. Therefore, the Commissioner recommends reviewing and revising the contractual terms to ensure such reporting procedure is explicitly spelt out.

Review of personal data handling policies

(15) There is no record of regular review of the internal documents on the handling of personal data and IT security policies. The Commissioner recommends that regular reviews should be carried out and documented, and relevant documents and policies should be updated to take account of any new practices, or development in technology, etc.

Conclusion

7. Notwithstanding the findings identified in paragraph 6, the personal data system inspected is generally in compliance with the requirements of the Ordinance. The Commissioner is pleased to place on record his general

observations in the Inspection as follows:-

(a) Only necessary but not excessive data is collected;

(b) The collection means are lawful and fair;

(c) The Guidance Notes on the Application For Eligibility (the "**Guidance Notes**") provided by SFAA to the applicants contain adequate information on the purposes of the use of data, the classes of transferees, data access / correction right and persons to contact for exercising such right;

(d) Practical steps have been taken to ensure data accuracy;

(e) The three-year retention period of data stored in inactive records could be justified;

(f) Data is only used for the purposes set out in the Guidance Notes; and

(g) Practical steps, such as the emphasis of data protection in training and circulars, password controls for access to offices' restricted areas and computer systems, escort of couriers, etc., have been taken to avoid unauthorised or accidental access, processing, erasure, loss or use of data.

8. Of the 15 recommendations outlined above, the Commissioner considers that the following five areas call for SFAA's prompt attention:

(a) review the types of data to be retained permanently and anonymise the data where appropriate (paragraph 6(4) above);

(b) provide written guidance on the handling of phone enquirers who claim to be the applicant himself and introduce more stringent identity verification procedures (paragraph 6(5) above);

(c) encrypt data kept on backup tapes (paragraph 6(11) above);

(d) provide mandatory IT security awareness training to designated ranks and posts of SFAA staff (paragraph 6(12) above); and

(e) enhance control over the Data Prep Contractor (paragraph 6(13) above).

Chapter One

Introduction

SFAA

1.1 It is the HKSAR Government's education policy to ensure that no student is deprived of education because of lack of financial means[1]. SFAA is an executive agency of the HKSAR Government's policy on student finance. SFAA currently administers a total of 14 publicly funded student financial assistance schemes for students from pre-primary to tertiary levels and 21 scholarships, merit award and loan fund schemes[2].

1.2 On average, SFAA receives over 956,000 applications per year for various financial assistance schemes and over 8,000 applications per year for various scholarships and merit award schemes[3]. SFAA collects, holds, processes and uses a wide range of personal data of applicants and their family members. The kinds of personal data held by SFAA include the name, Hong Kong Identity Card ("**HKID Card**") Number, Date of Birth ("**DOB**"), contact information, employment details, annual income, bank account details, education information, etc. of the applicants and their family members.

1.3 Given the vast number of data subjects, the sensitive personal and financial data involved, as well as the continual role of SFAA in the administration of student financial assistance schemes, the Commissioner considers that it is in the public interest to carry out an inspection of the personal data system used by SFAA (the "**Inspection**") pursuant to section 36 of the Personal Data (Privacy) Ordinance (the "**Ordinance**").

[1] SFAA's official website at www.sfaa.gov.hk.
[2] Please refer to Annex 1 for the full list of schemes administered by SFAA at the time of the Inspection.
[3] Statistics on the average number of the applications received by SFAA for the three academic years of 2010 / 11, 2011 / 12 and 2012 / 13 provided by SFAA on 24 April 2013.

Financial Assistance Schemes

1.4 Instead of examining the personal data systems of all the schemes administered by SFAA, the Commissioner decided to focus efforts on the personal data system of four financial assistance schemes for primary and secondary students (the "**Identified Schemes**") administered by the Textbook Assistance / Student Travel Subsidy Section of SFAA for reasons set out in paragraph 1.7.

1.5 The Identified Schemes are briefly described below[4]:-

(a) School Textbook Assistance Scheme: It is applicable to needy primary 1 to senior secondary 3 / secondary 6 students who are studying in government, aided, per caput grant schools and local private schools under the Direct Subsidy Scheme for covering the costs of essential textbooks and miscellaneous school-related expenses.

(b) Student Travel Subsidy Scheme: It is applicable to needy students receiving formal primary, secondary education or attending a full-time day course up to first degree level in an acceptable institution, residing beyond 10 minutes walking distance from school and travelling to school by public transport.

(c) Subsidy Scheme for Internet Access Charges: It is applicable to needy families whose children are full-time students receiving education at primary or secondary level, or full-time students pursuing Yi Jin Diploma programmes or equivalent courses of the Vocational Training Council to meet the internet access charges for e-learning at home for their children. The subsidy is granted on a household basis.

[4] SFAA's official website at www.sfaa.gov.hk

(d) Examination Fee Remission Scheme: It is applicable to needy students attending public examinations administered by the Hong Kong Examinations and Assessment Authority.

1.6 An application for the Identified Schemes is processed in two phases, namely the "Application for Assessment of Eligibility" and the "Application for Financial Assistance Scheme(s)". The former is a family-based assessment to determine whether the applicant's family is eligible for financial assistance, whereas the latter is a student-based application which enables the applicant to choose the specific scheme(s) he[5] wishes to apply for his child / children.

Reasons for the Inspection of the Identified Schemes

1.7 The Commissioner considers the Inspection of the personal data system of the Identified Schemes would provide a solid basis for him to provide recommendations to SFAA for the reasons below:

(a) The average number of applications received for each of the three academic years of 2010 / 11 to 2012 / 13 for the Identified Schemes exceeds 713,000[6], which represents nearly 75% of the average number of all applications received by SFAA;

(b) The computer system concerned, namely, the Student Financial Assistance Management System ("**SFAMS**"), is used[7] to

[5] Words and expressions importing the masculine gender include the feminine gender in this report.
[6] Statistics provided by SFAA on 24 April 2013.
[7] SFAA maintains different computer systems to support the administration of different schemes. Of the 14 financial assistance schemes, SFAMS supports processing of eight of them, namely School Textbook Assistance Scheme, Student Travel Subsidy Scheme, Subsidy Scheme for Internet Access Charges, Examination Fee Remission Scheme, Tertiary Student Finance Scheme – Publicly-funded Programmes, Non-means-tested Loan Scheme for full-time tertiary students, Yi Jin Diploma Fee Reimbursement and Financial Assistance Scheme for Designated Evening Adult Education Courses. The Commissioner notes that SFAA plans to implement a new integrated function-based computer system called the Integrated Student Financial Assistance System to replace the various scheme-based computer systems in phases for the purpose of improving the efficiency and effectiveness in administering the student financial assistance schemes. A Privacy Impact Assessment has been conducted for the proposed system.

support more than 50% of the financial assistance schemes administered by SFAA (including the Identified Schemes);

(c) Personal data including contact information, employment details, annual income, bank account details and, education information of the applicants and their family members would be collected by SFAA;

(d) Data input and courier services are outsourced to contractors; and

(e) Records containing personal data are taken out of the SFAA premises for paying home visits as part of the authentication process.

1.8 It is intended that the recommendations contained in this report could be of use to SFAA in respect of both the Identified Schemes and other Schemes not covered by the Inspection. Other public bodies that collect personal data from members of the public for the purpose of providing financial assistance in a way similar to SFAA are encouraged to take reference from this report.

Chapter Two

The Inspection

Commencement of the Inspection

2.1 In accordance with section 41 of the Ordinance, on 30 April 2013 the Commissioner informed SFAA in writing of his intention to carry out an inspection of the personal data system of SFAA with a view to making recommendations to promote compliance with the Ordinance.

The Inspection Team

2.2 An inspection team (the "**Team**") consisting of six officers[8] from the Office of the Privacy Commissioner for Personal Data was formed to carry out the Inspection.

Pre-Inspection Meeting

2.3 The Team held a pre-inspection meeting with representatives of SFAA on 21 May 2013 to explain the nature, purpose, scope and methodology of the Inspection. The Team also answered SFAA's queries and addressed its concerns, and gained a better understanding of the operation and work flow of the personal data system of SFAA.

Scope of the Inspection

2.4 The personal data system was examined against the requirements under Data Protection Principles ("**DPPs**") 1 to 4 in Schedule 1 to the Ordinance in respect of the collection, retention, use and security of personal

[8] The Team consisted of one Chief Personal Data Officer, one Information Technology Advisor, one Senior Personal Data Officer, two Assistant Personal Data Officers and one Personal Data Assistant.

data. The four DPPs are reproduced in Annex 2. DPP5, concerning information to be generally available, and DPP6, concerning access to personal data, are not covered in this Inspection.

Methodology

2.5 The Team performed the following procedures during the Inspection under section 36 of the Ordinance:-

Policy review

2.6 A detailed and comprehensive policy on how to properly handle applicants' and their family members' personal data is essential for ensuring good and uniform practice. In the Inspection, the Team examined the relevant policies, procedural manuals, guidelines and training material which SFAA follows in the handling of personal data.

Enquiries

2.7 The Team made written and verbal enquiries with SFAA. The information obtained through enquiries assisted the Team in understanding the operation of the personal data system, reconciling the documentary evidence obtained in the Inspection and identifying any cause for concern. SFAA was also able to supplement the evidence in question to avoid misunderstanding or misinterpretation.

Site inspections

2.8 Between 26 June 2013 and 8 July 2013, the Team inspected the premises of SFAA located at Mong Kok, Cheung Sha Wan and Kwai Hing. The Team was able to personally inspect the place and equipment used for collecting, processing and storing the personal data, sample check file records, observe the transportation and storage procedures for the backup tapes and identify any issues that might not have been apparent from documents or representations.

Walkthrough demonstration

2.9 Representatives of SFAA walked through with the Team the work flow of collection and return of application forms and compact discs (the "**CDs**") by a contractor engaged by SFAA to transcribe data contained in the application forms onto CDs (the "**Data Prep Contractor**"). The Team also observed a demonstration of the data transfer and data matching process in SFAMS. In addition, the Team observed interactive queries performed by SFAA staff on the database supporting the Identified Schemes. These demonstrations enabled the Team to observe the process and equipment used in the handling of personal data and to gain a better understanding of the actual data flow involved.

Interviews

2.10 The Team interviewed 28 SFAA staff, from management and operational levels, of different teams under the Textbook Assistance / Student Travel Subsidy Section and the Information Technology Management Unit of SFAA to understand their handling of personal data, their familiarity with the policies, guidelines and procedures relating to their work, and the training they provided and received.

Chapter Three

Personal Data System and Data Flow of the Identified Schemes

The Personal Data System

3.1 The personal data system examined in the Inspection includes the automated system used for processing of personal data (which mainly is SFAMS for the Identified Schemes) and the procedures of the relevant departments as well as data processors in the collection, holding, processing or use of the personal data of the Identified Schemes.

3.2 The table below lists the major kinds of personal data of applicants and their family members involved in the Identified Schemes:-

Kinds of personal data	**Examples**
Name and other identifiers	• Name in Chinese and English • HKID Card Number • Student Reference Number • Family ID assigned by SFAA
Contact information	• Address • Home phone number, mobile phone number, office phone number
Employment details	• Name of employer • Position
Financial details	• Annual income • Unavoidable medical expenses • School grants for selected items of school related expenses under the Comprehensive Social Security Assistance Scheme • Bank name • Bank account number
School information	• School name • School address

Kinds of personal data	Examples
	• School type • Class attending
Scheme details	• Scheme(s) applied for • Level and amount of assistance granted by SFAA
Other	• DOB • Signature • Marital status • Hong Kong resident status

3.3 For the purpose of the Inspection, the operation of the personal data system is divided into four stages, namely:-

(a) Application collection and data preparation;

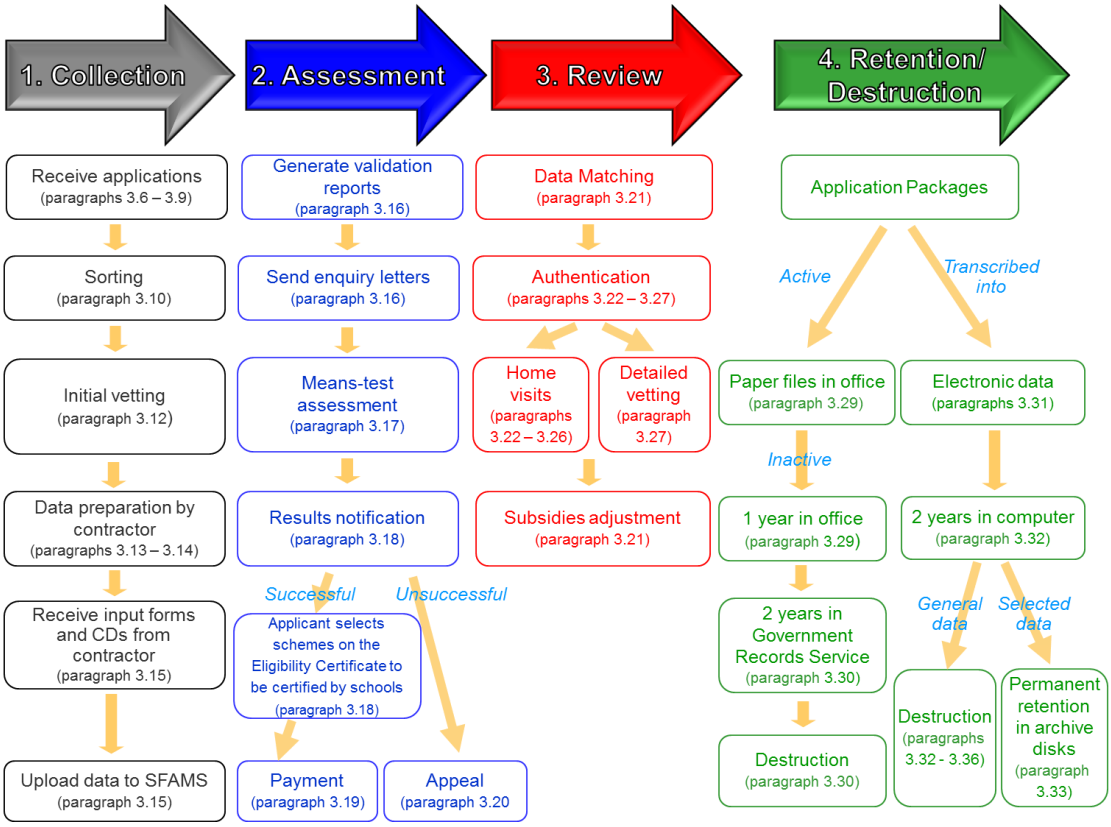
(b) Application assessment;

(c) Application review; and

(d) Retention and destruction of records.

Data Flow in the Four Stages of the Identified Schemes

3.4 The following flow chart illustrates the four stages of data flow describing how personal data is collected, processed, used and destroyed under the Identified Schemes.



First stage – Application collection and data preparation

3.5 As mentioned in paragraph 1.6, applications under the Identified Schemes are processed in two phases, namely the "Application for Assessment of Eligibility" and "Application for Financial Assistance Scheme(s)".

3.6 First time applicant[9] should complete and submit the "Application for Assessment of Eligibility / Financial Assistance For Primary and Secondary Students - Form A" ("**Form A**") to SFAA.

[9] The applicant must be the parent or guardian of the student.

3.7 An applicant who has received financial assistance or submitted an Eligibility Certificate[10] to SFAA in the current school year will receive from SFAA a pre-printed "Application for Assessment of Eligibility / Financial Assistance For Primary and Secondary Students - Form B" ("**Form B**") for the next school year, and an applicant who has received School Textbook Assistance for the current school year will also receive a pre-printed "Application for Financial Assistance Scheme(s) for Primary and Secondary Students - Form R" ("**Form R**") for the next school year. The applicant should confirm the data contained therein and complete the form(s).

3.8 Applicants are required to provide or confirm their personal data on Forms A, B and R as listed in Annex 4. An applicant should submit the completed form(s) together with the supporting documents by post to SFAA's Post Office Box using the addressed envelope provided by SFAA. SFAA also accepts applications submitted by hand to SFAA enquiry counter or placed into its locked drop-in box located at reception or outside SFAA's office.

Drop-in box outside SFAA's office.

SFAA's enquiry counter.

3.9 SFAA engages a contractor to pick up mailbags containing application packages from the Post Office. According to SFAA, the entire transportation process is escorted by an SFAA staff member.

[10] Please refer to paragraph 3.18 for the function of an Eligibility Certificate.

Mailbags collected from the Post Office.

3.10 Once the contract workers (who are provided by another contractor under a temporary manpower services contract) received the application packages from applicants, they would open the packages, date-stamp, sort, tally the quantity of applications, and place the packages into cartons for internal transfer to the SFAA Processing Team for initial vetting.

Opening and sorting application packages.

Application packages ready for transfer to the Processing Team for initial vetting.

3.11 SFAA issues acknowledgement to applicants by sending text messages (SMS) to applicants' mobile phones or in writing (if Hong Kong mobile phone number is not provided).

3.12 The Processing Team then checks the sufficiency of supporting documents such as copies of identification documents, documentary proof of unavoidable medical expenses, supporting documents for separation / divorce and documentary proof of total income during the specified period. The Processing Team also verifies the accuracy of the information provided on the

application form against the supporting documents. The Processing Team may contact the applicants by phone or in writing for clarifications or further details in respect of assessments. The Processing Team then segregates the application forms from the supporting documents. The forms, stored in sealed cartons, are placed in the designated area of each floor for pick-up by the Data Prep Contractor. An SFAA staff member counts the number of cartons and prepares a collection form for the Data Prep Contractor.

3.13 The Data Prep Contractor is engaged to provide the following services[11]:-

(a) Collection of the forms by batches;

(b) Data input of the application forms;

(c) Transcription of data onto CDs in text format; and

(d) Delivery by batches of the CDs together with the forms to SFAA by hand.

3.14 Twice a week, the Data Prep Contractor collects the cartons containing the forms from SFAA office. An SFAA staff member accompanies the Data Prep Contractor to collect the cartons from various floors and checks the number of cartons against the collection form to ensure the correct quantity of cartons is collected by the Data Prep Contractor.

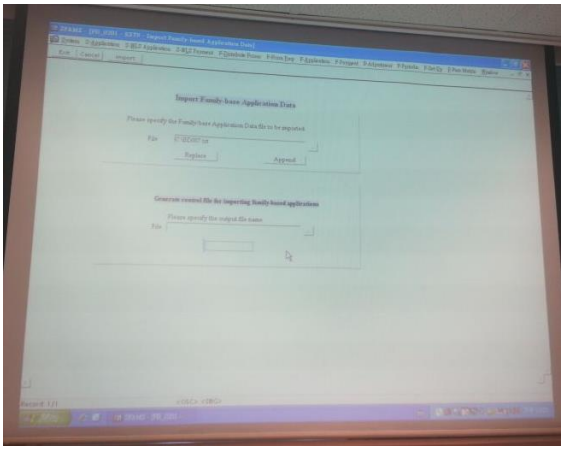
Sealed cartons are placed in the designated area for pick-up.

The Data Prep Contractor, accompanied by an SFAA staff member, is collecting the cartons.

[11] According to the "Specification for Provision of Data Preparation Services 2013 / 2014", which forms part of the contract with the Data Prep Contractor.

3.15 Upon completion of data input, the Data Prep Contractor delivers the CDs and cartons containing the forms to SFAA by hand. A designated staff of SFAA then uploads the data contained in the CDs to SFAMS for subsequent processing. The forms are returned to the Processing Team who will merge the forms with the relevant supporting documents and file them together.

Data Prep Contractor delivers CDs and boxes of forms after completion of each batch.



Uploading data from CDs into SFAMS.

Second stage – Application assessment

3.16 After uploading the data contained in CDs to SFAMS, validation reports for cases with insufficient or inaccurate information would be generated from SFAMS. A standard enquiry letter would then be issued to applicants to seek further clarifications or supporting documents.

3.17 Each application is assessed by means test using the "Adjusted Family Income" mechanism, whereby an applicant's gross annual household income and household size are taken into account in determining his eligibility for assistance[12].

[12] The applicable formula is "Gross annual income of the family / [no. of family members + (1)]". For single-parent families of 2 to 3 members, the '+(1)' factor in the divisor of the formula will be changed to '+(2)'.

3.18 For new applicants submitting Form A to apply for financial assistance and for continuing applicants[13] who are issued with Form B only, an Eligibility Certificate is issued to each eligible student whose family passed the means test. The applicant then selects the schemes he wishes to apply for each of his children on the Eligibility Certificates and submits the Eligibility Certificates to the children's schools, which are required to certify the students' status and attendance, and return the completed Eligibility Certificates to SFAA.

3.19 Upon receipt of the returned Eligibility Certificate, SFAA disburses School Textbook Assistance, Student Travel Subsidy and Subsidy for Internet Access Charges, where applicable, to the successful applicants by auto-pay. As for Examination Fee Remission Scheme, SFAA will arrange for payment of examination fees to the Hong Kong Examinations and Assessment Authority direct on behalf of the students after verification.

3.20 An applicant whose family failed in the means test will be notified by SFAA by post. An applicant may apply in writing to SFAA for reassessment if he is dissatisfied with the assessment result. Detailed justifications and documentary evidence would need to be provided to support his application for reassessment.

Third stage - Application review

Data matching

3.21 SFAA conducts data matching with the Education Bureau and Social Welfare Department to ensure prudent use of public money and that financial assistance is provided to students and families with genuine need without the payment of double subsidies. If it is found that subsidies have been wrongly disbursed, e.g. the student has moved to a school not eligible for School Textbook Assistance or quit studying, SFAA would take action to recover the financial assistance given.

[13] For continuing applicants who are issued with pre-printed Form B and Form R, and could pass the means test, SFAA will disburse textbook assistance to the applicant before the commencement of the new school year. A notification letter instead of the Eligibility Certificate will be sent to the applicant.

Home visits

3.22 Throughout the academic year, SFAA conducts authentication on successful applications by means of home visits and detailed vetting. Authentication process is handled by a designated team (the "**Authentication Team**") located in another office building separate from the Processing Team. The authentication process enables SFAA to verify the truthfulness and completeness of the information provided by the applicants. SFAA will adjust the level and the amount of assistance granted, and recover overpayment where necessary.

3.23 Home visits start in November and are completed by July the following year. SFAA adopts a risk-based approach in selecting cases for conducting home visits.

3.24 Selected case files will be sent to the Authentication Team by courier, escorted by SFAA staff.

3.25 The Authentication Team first contacts the applicant or his spouse by phone to schedule a home visit appointment. If the applicant or his spouse cannot be reached, a standard call-back letter would be issued. After confirming a home visit appointment, the staff member will input the appointment details, such as the case number, residential district, contact number, type of scheme into a file saved in the network drive that could be assessed by the Head of the Authentication Team.

3.26 An Authentication Team staff member will bring along with him a print-out from SFAMS and case file when conducting a home visit. He may take photographs using an SFAA provided digital camera for capturing images of supporting information if necessary, but the Team was informed that the taking of photographs is uncommon. Upon completion of a home visit, the staff member is required to submit a report (and recommendation if there is any overpayment or down-payment case identified) to his supervisor.

Detailed vetting

3.27 For applications that are randomly selected for detailed vetting, applicants are required to provide concrete income proof (e.g. bank statement

of all income earning family members) during the assessment period or explanation as to why he is unable to provide such proof.

Fourth stage – Retention and destruction of records

3.28 Records are considered active during the current school year in which the assistance is disbursed, and when currently in use by SFAA staff for purposes such as handling appeals.

Paper files

3.29 Active records contained in paper files (including application forms and supporting documents) are kept in SFAA's office during the current school year. Upon lapse of the school year in which the assistance has been disbursed, records are treated as inactive and would be kept in SFAA's office for another year before being passed to Government Records Service for retention.

Case files are stored in mobile racks at SFAA's office for one year.

3.30 Each year, SFAA informs Government Records Service of the types, quantity and scheduled disposal date of records to be delivered to Government Records Service. The prescribed retention period in Government Records Service is two years. Around one to two months before the end of the prescribed retention period, Government Records Service sends a

"Confirmation on Records Disposal" to SFAA. Government Records Service will destroy the inactive records on SFAA's behalf after receiving SFAA's endorsed "Confirmation on Records Disposal".

Electronic records

3.31 Majority of the data containing in the application form (except position, name of employer/ firm and office telephone number of the applicant and relevant family members, explanation of special family information, such as duration and name of family members in receipt of Comprehensive Social Security Assistance and the signatures of the applicant and his spouse) is transcribed into electronic data by the Data Prep Contractor and subsequently uploaded into SFAMS from which SFAA staff may download the data into their individual computers and network drive.

3.32 It is SFAA's practice that electronic records of application related data will not be kept for more than two years. Staff from SFAA's Information Technology Management Unit are responsible for erasing the data stored in SFAMS after each academic year whereas individual staff member is responsible for deleting the personal data stored in his individual computer (and network drive to which he has access). SFAA would normally send an email at the beginning of each academic year to remind its staff to erase the time-lapsed electronic data.

3.33 Despite erasure action described in paragraph 3.32, SFAA retains selected personal data permanently in CDs (see Annex 5 for the list of data selected) which are kept in a locked cabinet.

3.34 CDs storing the data input by the Data Prep Contractor will be shredded by a designated SFAA staff member around one month after the data has been uploaded to SFAMS.

3.35 The Data Prep Contractor erases the data stored in their server one month after transcribing such data onto CDs and providing such CDs to SFAA.

3.36 Staff of the Authentication Team use a digital camera to take photos during home visits. Upon completion of home visits, they upload the image files to their computers and print the photos for record. They are required to

delete the image files in the computers after printing and format the memory card inside the digital camera completely before leaving the office to conduct home visit(s) each day.

Summary

3.37 The table below summarises the retention periods of different types of records containing personal data.

Record Type	Retention Period
Paper record (inactive record)	1-year retention in SFAA office followed by 2-year retention in Government Records Service
Electronic record - General data - Selected data - CDs from Data Prep Contractor - Data kept by Data Prep Contractor	 - 2-year retention in individual staff's computer and network drive - Permanent retention in archive disks - About 1 month - About 1 month

Chapter Four

Findings and Recommendations

Preliminaries

4.1 Findings and recommendations made in this Report were based on the information provided by SFAA and the Team's on-site observations at the material time. They are not to be treated as exhaustive to cover every aspect of the operation of the personal data system of the Identified Schemes, and may be regarded only as verification of the compliance level of the matters in question at the time when the Inspection was carried out.

4.2 The findings are divided into two categories. The first category consists of "specific findings" regarding the level of compliance with the four DPPs of the Ordinance. The second category consists of "other findings" in relation to the general measures adopted by SFAA in personal data protection.

Specific Findings

DPP1 – Purpose and Manner of Collection of Personal Data

Requirements under the Ordinance

4.3 DPP1 regulates the collection of personal data in respect of (a) the purposes for which the personal data is collected and whether it is necessary to collect such personal data; (b) the proper means to be used in collecting the personal data; and (c) the duty of the data user to inform the data subject details of such collection (including the purpose of collection and classes of possible transferees of the data).

4.4 As SFAA collects HKID Card Number and HKID Card Copy of the applicants and their family members, analysis has been made in accordance

with the "Code of Practice on the Identity Card Number and other Personal Identifiers" (the "**Code**") issued by the Commissioner. Extracts of the relevant paragraphs of the Code are reproduced in Annex 3.

The Team's findings

4.5 An applicant would need to provide or confirm[14] in Forms A, B and / or R the personal data[15] of himself, his spouse, unmarried children residing with the family and dependent parents and provide the relevant supporting documents such as copies of HKID Card and income proof for application purpose.

4.6 The Team examined the above types of personal data collected by SFAA and understood that the data is required for identification, communication and / or assessment purposes but was concerned whether there was a genuine need to collect the DOB of the applicant and his family members, and the marital status (married, divorced, separated, widowed, single, etc.) of the applicant.

4.7 SFAA provided the following explanations for collecting DOB:

(a) DOB of a student is one of the data used, besides name and HKID Card Number, to match with data in Education Bureau's database to verify or update student records and confirm eligibility for various financial assistance schemes;

(b) DOB of all other persons may be used to cross check with Social Welfare Department on whether the person concerned received Comprehensive Social Security Assistance, especially

[14] As mentioned in paragraphs 3.6 – 3.7, new applicants are required to fill out Form A, whereas applicants who have received financial assistance or submitted an Eligibility Certificate to SFAA on or before 1 April of the current school year would confirm or update the pre-printed information on Form B. Those who have received textbook assistance in the current school year also need to confirm and fill out Form R.

[15] Personal data requested in Forms A, B and R is tabularised in Annex 4.

if that person does not possess a HKID Card;

(c) SFAA staff may raise questions in relation to the dependent parents named by applicants based on their ages; and

(d) DOB of the students would also be used for statistical purpose as members of Legislative Council may ask about the age profile of students.

4.8 SFAA explained that the marital status is required so as to determine the type of supporting document required and whether certain types of income, e.g. alimony, would be expected. The marital status also facilitates staff's understanding of an applicant's family background to avoid asking inappropriate questions.

4.9 The application forms themselves have not specified which items are obligatory or voluntary. The Team was advised that the application would still be processed even if some items, e.g. mobile phone number, are not supplied.

4.10 SFAA provides detailed Guidance Notes on the Application For Eligibility (the "**Guidance Notes**") for the Identified Schemes and applicants are advised to read the Guidance Notes before completing the application forms. The Guidance Notes contain a part on "Provision / Handling of Personal Data"[16] which, among other things, states the following:-

(a) "It is the responsibility of applicants to complete the application fully and truthfully and to provide all supporting documents."

(b) "Insufficient information / misrepresentation of facts / providing false and misleading information will render the application processing deferred, application disqualified for further processing or will even lead to criminal prosecution."

[16] Part 5 in the Guidance Notes for Form A and Part 6 in the Guidance Notes for Form B and Form R.

(c) *"The personal data…will be used by SFAA and* [Education Bureau] */ disclosed to the agents of SFAA /* [Education Bureau], *the schools / institutions concerned and relevant government bureaux / departments for the following purposes*[17] *…"*

(d) *"The applicant has the right to obtain access and make corrections to the data provided by him / her…Such request should be addressed to Assistant Controller (Administration), SFAA."*

Commissioner's comments and recommendations

4.11 The Commissioner acknowledges that the collection of the personal data specified in the application forms was necessary or directly related to those purposes set out in paragraph 4.10.

4.12 Regarding whether the data collected by SFAA is adequate but not excessive, the Commissioner examined the data collected and agreed that there is no excessive collection in relation to identification, communication and assessment purposes except for the collection of DOB of the applicants and their family members.

4.13 In particular, the Commissioner is concerned about the need to collect DOB from persons who can provide HKID Card Number for the purpose of checking with Education Bureau / Social Welfare Department database given that HKID Card Number is already a reliable and unique data for identifying a person. Should the age profile of the students and dependent parents be required, the collection of the year of birth should suffice. As regards the collection of marital status, the Commissioner found such collection justified after understanding the rationale set out in paragraph 4.8.

[17] Please refer to Annex 6 for all the seven purposes stated in the Guidance Notes.

4.14 The Commissioner also concludes that the collection of HKID Card Number and HKID Card Copy is justified under the Code given the following:

(a) Paragraph 2.3.1 of the Code allows the collection of HKID Card Number if a statutory provision confers on the data user the power to collect the HKID Card Number. Section 5 of the Registration of Persons Ordinance (Cap. 177) confers on a public officer[18] the power to require any registered person in all dealings with the Government to furnish his HKID Card Number. SFAA staff, being public officers, are therefore entitled to collect HKID Card Numbers in the handling of the financial assistance applications.

(b) Paragraph 3.2.1.2 of the Code allows the collection of HKID Card Copy where the use of HKID Card Copy is necessary for any of the purposes mentioned in section 58(1) of the Ordinance. Such purposes include the prevention, preclusion or remedying of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons. As mentioned in the Guidance Notes (see details in Annex 6), the personal data collected by SFAA will be used to prevent double subsidies and detect fraud. The Commissioner therefore considers that it is justifiable to collect HKID Card Copy.

4.15 Personal data is collected through application packages prepared by the applicant and there is no information suggesting that SFAA has used any unfair means (e.g. deception or coercion) in collecting personal data.

4.16 The Guidance Notes clearly state the consequences of not completing the application form fully, the purposes for which the data is to be used, the parties to whom the personal data collected would be transferred, and the

[18] Section 3 of the Interpretation and General Clauses Ordinance (Cap. 1) defines "public officer" to mean any person holding an office of emolument under the Government, whether such office be permanent or temporary.

person to whom a data access or correction request should be made. That said, as the Team was advised by SFAA that it is not obligatory for the applicant to supply all the data, such as mobile phone number, as required in the application form, the Commissioner therefore suggests that SFAA should spell out explicitly which items are obligatory.

Recommendations

(1) Consider not collecting the DOB of the applicant and his family members if their HKID Card Numbers are provided. Depending on its operational needs, SFAA can consider requesting the year of birth instead of DOB for dependent parents and students to facilitate application vetting and / or to meet statistical purpose.

(2) Specify in the application forms which kinds of personal data are to be mandatorily supplied for SFAA to review the application and the consequences of not supplying such data.

DPP2 – Accuracy and Retention of Personal Data

Requirements under the Ordinance

4.17 DPP2(1) requires data users to, among other things, take all reasonably practicable steps to ensure that the personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used.

4.18 DPP2(2) stipulates that 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 is or is to be used. Section 26(1) of the Ordinance similarly stipulates that once the personal data held is no longer required for the purpose (including any directly related purpose) for which the data was used, a

data user must take all practicable steps to erase the personal data unless any such erasure is prohibited under any law or it is in the public interest (including historical interest) for the data not to be erased.

The Team's findings on accuracy of personal data

4.19 The obligation to ensure accuracy of data provided by the applicant to SFAA rests on the applicant himself. The applicant is required to declare in the application form that *"The information…and the supporting documents provided by me / us are true, complete and accurate…Any misrepresentation, concealment of facts, provision of misleading or false information or intentional obstruction of SFAA staff in their course of authentication will lead to disqualification, restitution in full of the assistance granted and possible prosecution."*

4.20 SFAA verifies the accuracy of the data by vetting the data in the application form against the supporting documents provided, and conducting authentication of the successful applications (including home visit and detailed vetting) to verify whether the information provided therein is true, complete and accurate.

4.21 SFAA engages the Data Prep Contractor to transcribe the data contained in paper forms onto CDs. According to the contract with the Data Prep Contractor, each data requires double entry by two different data entry operators. Once the system detects any discrepancy between the first entry and second entry, a third operator who is different from the first and second entry operators should conduct the third data entry for the data field with discrepancy. Starting from August 2013, if the value input by the third entry does not match with the first or second entry, a fourth operator will be prompted to input the value again until the fourth entry is the same as the third entry.

4.22 SFAA maintains an error register which documents the number and types of errors made by the Data Prep Contractor on a monthly basis. Sample

email correspondence between SFAA and the Data Prep Contractor shows that SFAA has requested the Data Prep Contractor to investigate and enhance the accuracy whenever error was spotted.

The Team's findings on retention of personal data

4.23 Records are considered inactive upon the lapse of the academic year in which assistance has been disbursed.

4.24 It is SFAA's policy to retain inactive records in paper form for three years. SFAA advised that it is necessary to retrieve records for the following purposes:

(a) Appeal, review and audit trail purposes;
(b) Cross referencing with information provided in past years' application in vetting current year's application to gauge any major differences; and / or
(c) Investigating suspected deception cases, which may necessitate reference to past years' applications and taking recovery actions for long-outstanding overpayments.

4.25 In view of the purposes stated above, the retention periods for both successful and unsuccessful applications are the same. The retention period is reviewed every five years.

4.26 Inactive paper files are stored in SFAA's office for one year to serve all the purposes listed in paragraph 4.24. They are then transferred to Government Records Service for storage for another two years before destruction mainly for the purpose mentioned in paragraph 4.24(c).

4.27 Besides paper records, SFAA also retains data electronically in SFAMS, individuals' computers and/ or network drive for the current academic year when the applications are received for processing the application, and

another year for the reasons mentioned in paragraphs 4.24(a) and (b). Electronic data saved in SFAMS would be erased by SFAA's Information Technology Management Unit while that saved in individuals' computers or network drive will be erased by individual staff after two years' retention.

4.28 During the site inspection, the Team sample checked the paper files stored in the mobile racks and the electronic data stored in staff's computers and did not uncover any data that was kept longer than the retention period.

4.29 That said, the Team found a lack of monitoring over erasure of files stored in individuals' computers and network drive. SFAA staff would save working files (e.g. files consisting personal data exchanged with other government departments, e.g. Social Welfare Department, Education Bureau, etc.) in their computers or in some cases keep a copy in network drive for processing. Though SFAA would normally issue an email message at the beginning of each academic year to remind colleagues to delete files containing personal data, there is no follow-up check, regular or random, by supervisors to ensure the process was duly carried out. It is uncertain if staff followed the reminder email to conduct such deletion which may cause personal data to be kept longer than necessary.

4.30 Before the records are erased from SFAMS by SFAA's Information Technology Management Unit, SFAA archived a total of 35 types of data permanently including the English name, HKID Card Number, DOB of the applicant, spouse, unmarried children and dependent parents as well as the annual income of the applicant, spouse and unmarried children, etc.[19] in CDs. SFAA explained that such data has been kept since academic year 2005 / 2006 mainly for the purpose of responding to statistical questions raised by Legislative Council members such as the number of families receiving student financial assistance, age profile of the students, number of family members, assistance level, geographical distribution of the applicants, etc. SFAA also explained that such data may be required for complaint handling, recovery of

[19] Please refer to Annex 5 for the list of data retained permanently.

overpaid assistance and investigation of fraud cases.

Commissioner's comments and recommendations

4.31 The Commissioner is pleased to note the steps taken by SFAA to ensure accuracy of the personal data through use of the double entry system.

4.32 The Commissioner considers the retention period reasonable but notes the lack of regular or random checking on the erasure of electronic data by individual staff which casts doubt on whether the prevailing policy is in fact followed.

4.33 The Commissioner recognises that SFAA may wish to retain part of the data for statistical purposes. The Commissioner takes the view that so long as the personal data held is permanently anonymised to the extent that it is no longer practicable for the data user (or anyone else) to directly or indirectly identify the individuals concerned, the data is not considered to be personal data and is not subject to the provisions of the Ordinance. Personal data used for handling complaints, recovery of overpayment and investigation of fraud cases may warrant a retention period longer than three years. It is, however, questionable why the individually identifiable data (i.e. English name, HKID Card Number and DOB) of all the applicants and family members is retained permanently for the purposes mentioned in paragraph 4.30. This is an area that requires SFAA's review.

Recommendations

(3) Set up a monitoring mechanism to ensure that personal data held by all relevant SFAA staff in individual computers and network drive which is no longer required is erased.

(4) Review to restrict the types of data to be retained permanently, and to anonymise such data where appropriate.

DPP3 – Use of Personal Data

Requirements under the Ordinance

4.34 DPP3 requires data users not to use (which includes "transfer" or "disclose") personal data for a new purpose unless with the prescribed consent from the data subjects. New purpose is defined under the Ordinance to mean any purpose other than a purpose which is the same as or directly related to the collection purpose.

The Team's findings

4.35 As mentioned in paragraph 4.10(c) and detailed in Annex 6, the Guidance Notes list seven purposes for the use (including disclosure) of personal data collected. By signing the application form, the applicant declares that he has read the Guidance Notes and fully understood and agreed to the arrangements stated therein.

4.36 The Team considered that the activities in the data flow as described in Chapter 3 are covered by the purposes listed in the Guidance Notes. The Guidance Notes state that the data will be disclosed to the agents of SFAA for the purpose of processing applications and therefore cover the transfer of personal data to the Data Prep Contractor. Besides the activities mentioned in the data flow, the Guidance Notes also state that the data could be used for activities relating to the recovery of overpayments, as well as for statistical and research purposes.

4.37 The Team was informed that applicants and their family members may, from time to time, contact SFAA for enquiries. The types of personal data that may be disclosed depend on the identity of the caller. SFAA requires a caller to provide his full name and HKID Card Number to verify the caller's identity. Hence, a caller who can provide an applicant's name and HKID Card

Number will be assumed to be the applicant himself.

4.38 SFAA relied on internal training conducted each year to guide staff on what could be disclosed when handling a telephone enquiry. The training material specifies what could not be disclosed if a caller is not the applicant. For example, if the caller is a family member stated in the application form, SFAA staff can answer questions such as whether SFAA has received the application and whether SFAA has issued the notification result. If the caller is not the applicant nor a family member stated in the application form, no answer may be given to case related questions. However, as for the handling of enquiries from a caller representing himself as the applicant, there is no written guideline on the types of personal data that can be disclosed. SFAA explained that training was given to staff not to disclose any sensitive financial information such as income to the caller and the case may be referred to the specific case officer where required.

4.39 As regards the handling of walk-in enquiries, a notice is posted outside the SFAA's enquiry room that only one family would be entertained at a time for privacy reason. Although the enquiry room consists of two enquiry counters, the room is quite small so that the discussion of one case can be easily overheard by others. During the site inspection on 4 July 2013, the Team noticed that two officers were serving two enquirers simultaneously apparently relating to two distinct applications at adjacent enquiry counters.

4.40 As regards the Eligibility Certificate which is sent to each eligible student for the applicant to select the financial assistance schemes to be applied for, the Team also noted that both partial HKID Card Number and student reference number, together with the student's name and DOB, were pre-printed on the Eligibility Certificate. The Eligibility Certificate will be submitted via the student's school which will certify the student's status and attendance.

4.41 The Guidance Notes state that "*in order to protect personal data, only the prefix and the first 3 digits of HKID card No. are shown."* However, as full student reference number is also shown on the Eligibility Certificate and

student reference number is the same as the HKID Card Number if the student possesses a HKID Card[20], the presentation of the partial HKID Card Number and full student reference number together on one document could mean that in fact the full HKID Card Number is presented.

4.42 SFAA advised that partial HKID Card Number and student reference number would facilitate the school to check if the student indeed studies at that particular school. When asked why both pieces of information are needed, SFAA advised that Primary 1 students do not have student reference number and so only HKID Card Number would be shown on the Eligibility Certificate.

4.43 The Team also noted that DOB and partial HKID Card Number together with the student's name were pre-printed on the letter notifying the applicant of the assessment results. SFAA explained that DOB and partial HKID Card Number are provided to facilitate the applicant to identify which of his children has been assessed to be eligible for financial assistance.

Commissioner's comments and recommendations

4.44 The Commissioner is generally satisfied that SFAA uses the personal data obtained for the same or directly related purposes as set out in the Guidance Notes.

4.45 The Commissioner however noted the risk of unnecessary disclosure of data during telephone / walk-in enquiries or on the Eligibility Certificate / letter notifying the applicant of the assessment results. In particular, when receiving a telephone enquiry, SFAA only requires a caller to provide his name and HKID Card Number for identity verification purpose and there is no well-documented instructions or guidelines on the types of personal data in the respective application that can be disclosed to the caller representing himself as

[20] If a student was not born in Hong Kong and has not yet obtained HKID Card, Education Bureau will first assign an 8-digit student reference number to the student. After the student has received the HKID Card, Education Bureau will update the student reference number to be the same as his HKID Card Number.

the applicant. The Commissioner therefore considers SFAA's handling of telephone enquiries a high risk area for breach of privacy.

4.46 To address the need for the school to verify the identity of a student (except for Primary 1 students), the Commissioner considers that the provision of student reference number together with the student's name on the Eligibility Certificate should suffice.

4.47 The Commissioner also finds it hard to understand the reason for providing DOB and partial HKID Card Number of the student on the letter notifying the result of assistance granted given that the name of the student is already printed on in that letter. The Commissioner takes the view that excessive disclosure should be avoided as the name of the eligible person should already serve the purpose of enabling the applicant to identify which of his children has been granted the assistance.

Recommendations:

(5) Provide clear instructions to staff as to the types of data that may or may not be disclosed to a phone enquirer who himself claims to be the applicant (e.g. the annual income of the applicant and his family members should not be disclosed over the phone); and implement more stringent identity verification procedures to confirm the enquirer's identity (e.g. request additional information other than the name and HKID Card Number of the applicant, e.g. correspondence address and telephone number provided on the application form).

(6) Strictly enforce the practice of handling walk-in enquiries from one applicant family at the enquiry room at one time.

(7) HKID Card Number and DOB should be removed from the Eligibility Certificate if student reference number is already shown.

(8)	Review the need for stating the name, DOB and partial HKID Card Number on the letter notifying the applicant of the assessment results, and whether it is sufficient to show only the name of the student on the letter.

DPP4 – Security of Personal Data

Requirements under the Ordinance

4.48 Under DPP4, data users are required to take all reasonably practicable steps to ensure that the personal data they keep is protected against unauthorised or accidental access, processing, erasure, loss or use. In ascertaining the appropriate steps to take, the data users have to consider, among other things, the kind of data and the harm that could result if such irregularities should arise, and the security measures incorporated into any equipment in which the data is stored. The requirement is not to impose an obligation on data users to provide absolute security of personal data, but the steps taken to safeguard security should be proportionate to the sensitivity of the personal data involved.

The Team's findings on storage and transit of paper files

4.49 During the site inspection, the Team was shown how the application package was received, opened, sorted, and packed in sealed cartons by agency workers for internal delivery to SFAA's Processing Team for initial vetting.

4.50 A bar code is assigned to each application. The SFAA's Processing Team scans the bar code into SFAMS once the application package is passed to them, and takes over the files thereafter.

4.51 All applications are treated as restricted documents. Staff are required to enter a password to enter the office and all staff are required to wear a staff card. Different passwords are set for each of the premises of SFAA and

are changed every three months or as required.

4.52 Each sub-team of SFAA's Processing Team prepares its own packing list when transferring paper files to Government Records Service for storage. There is however no activity update of the computer record to record file transfer to Government Records Service. In effect, this means that there is no audit trail for tracking the movement of individual files when these are passed to Government Records Service and SFAA is unable to verify the number of files passed to Government Records Service against the computer record.

4.53 SFAA's Authentication Team would bring (a) a SFAMS print-out containing applicants' data and (b) the case file containing the application package for conducting home visits. It is however questionable whether the full set of SFAMS print-out is required as most of the information contained therein should be contained in the case file already.

4.54 SFAA confirmed that there was no loss of case files in the academic years of 2011 / 12 and 2012 / 13 by its Processing Team and Authentication Team.

The Team's findings on data stored and transmitted electronically

4.55 SFAA demonstrated to the Team how the data was uploaded from a CD prepared by the Data Prep Contractor to SFAMS, and retrieved data from SFAMS for transmission to other parties for data matching and verification purposes. SFAA also explained to the Team the approval procedures for transmitting the data to the bank for payments through auto-pay.

4.56 The text files saved in CDs are zipped and protected by passwords which follow a pattern made known to three staff members of SFAA only. Data stored in the CDs is first saved in the computer and then uploaded to SFAMS by a designated staff member of SFAA. All CDs not yet destroyed are stored in a locked cabinet.

4.57 Backup tapes of all IT systems are transported from one SFAA office to another for safe-keeping twice every week by a courier, escorted by an SFAA staff member. Tapes are sealed in a bag then placed into plastic boxes secured by plastic security seals with serial numbers. The data on such tapes, however, is not encrypted. SFAA's Information Technology Management Unit explained that the data is classified as "Restricted". According to its internal IT Security Policy and the Security Regulations, encryption is only required for restricted data for transmission over unsecured network but not at storage.

4.58 The Team is given to understand that all IT security awareness training is attended by SFAA staff on a voluntary basis. Although new staff are subject to mandatory induction training which contained IT security awareness elements, attendance of biennial IT security awareness training provided by a security assessment contractor is not compulsory.

4.59 The use of USB thumb drives on SFAA workstations is controlled by "end-point" security software, which limits the use of USB thumb drives only to SFAA-approved computers or users.

4.60 The Team sample checked the digital cameras of SFAA's Authentication Team and no photos were found stored in the memory cards.

Commissioner's comments and recommendations

4.61 Generally speaking, the Commissioner is satisfied with the security of data contained in paper files and saved in SFAMS.

4.62 The Commissioner however would like to see measure(s) in place to update computer record of file activity status and conduct verification on the number of paper files passed to Government Records Service against the computer record. It is also suggested that only necessary documents, rather than the full set of SFAMS print-out together with the case file, be taken out of the office for the purpose of conducting home visit.

4.63 Transporting the backup tapes to another office for storage is good practice and commonly used. However, given these tapes are transported outside of the secured server rooms, there is always a risk of loss, theft or access by unauthorised parties. The Commissioner considers backup tapes as a kind of portable storage devices which are subject to security risks when they are transported outside secured office areas, and therefore any personal data stored in them should be encrypted to safeguard against unauthorised access.

4.64 The Commissioner opines that voluntary attendance of IT security awareness training would mean that SFAA could not ensure appropriate SFAA staff are familiar with IT security. SFAA has not demonstrated a systematic way to assess and manage the IT security awareness level of its staff. This is another area that the Commissioner recommends prompt action on SFAA's part.

Recommendations:

(9) Update the computer records of file activity status and conduct verification to ensure that all inactive paper files for which the one year "reference" period has expired are passed to Government Records Service for retention.

(10) Review the necessity to bring full sets of both the SFAMS print-out and the case files for conducting home visits to minimise the number of documents containing personal data brought outside of the office to the extent practicable.

(11) Encrypt all backup tapes that are to be transported to offsite storage.

(12) Provide mandatory IT security awareness training to the SFAA staff of designated ranks and posts.

Other Findings

Control of data processors

4.65 As far as the Identified Schemes are concerned, SFAA engages a Data Prep Contractor for data input and other companies for providing courier services between different office buildings as well as between the Post Office and the office buildings (collective known as "**Data Processors**"). The contractual terms governing data protection vary for each Data Processor.

4.66 The most comprehensive terms are included in the contract with the Data Prep Contractor, which commits to take every precautionary measure to protect the personal data contained in the documents or storage media from accidental or intentional leakages to any unauthorised person / party. Failure to do so shall be treated as a breach of contract.

4.67 The Team was advised that SFAA visited the Data Prep Contractor's premises twice between March 2010 and March 2013. No written report which documents the visits however existed. No IT technical support was involved in the inspection of the contractor's security measures.

4.68 The Data Prep Contractor committed in writing to destroy all the data collected in due course upon completion of the service rendered. The Team however noted that SFAA has not checked whether this was the case.

4.69 SFAA's contract with the courier service company that transports backup tapes, files and documents containing personal data between different offices does not include specific terms requiring the handling staff of the courier service company to protect the personal data entrusted to it in accordance with the requirement under the Ordinance (except prohibition against disclosure of files / documents details).

4.70 SFAA's contract with the courier service company that provides delivery services to and from the Post Office specifies that the courier service

company must ensure the security of the transportation services and is liable to compensate for any loss or damage incurred during the trips. It also specifies that the courier service company shall take every precautionary measure to protect the personal data contained in the documents or storage media from accidental or intentional leakage to any unauthorised person / party.

4.71 All the above contracts are silent on the need for immediate reporting of any sign of abnormality or security breach by the Data Processor concerned.

Commissioner's comments and recommendations

4.72 According to section 65(2) of the Ordinance, any act done or practice engaged in by a person as agent for another person with the authority of that other person shall be treated for the purposes of this Ordinance as done or engaged in by that other person as well as by him. A data user is under statutory obligations to monitor their data processors' compliance with DPPs. The primary means by which a data user may protect personal data entrusted to its data processor is through a contract. The Commissioner is of the view that the contract may impose obligations on data processors governing matters such as, the security measures required, the timely return, destruction or deletion of the personal data, prohibition against any unauthorised use or disclosure of the personal data, immediate reporting of any sign of abnormality or security breach, the data user's right to audit and inspect how the data processor handles and stores personal data, etc.

4.73 The Commissioner acknowledges that the contract between SFAA and the Data Prep Contractor is comprehensive in its scope. The Commissioner, however, would like to see more stringent measures to be put in place given that the Data Prep Contractor has access to all the data in the application forms and Eligibility Certificates.

4.74 Besides, the reporting procedure in the event of a suspected data breach which is not presently included in the contractual terms with the Data

Processors should be explicitly spelt out in the contract to ensure this is well communicated.

Recommendations:

(13) Involve IT technical support in future inspections of the Data Prep Contractor to ensure that the relevant IT security measures are in place; document the results of inspection; perform random checks to ensure data is not retained longer than necessary; and establish a policy on the frequency of inspections (e.g. once a year) and review of the inspection results by management staff of sufficient seniority.

(14) Review and revise contractual terms governing Data Processors' obligations to include the reporting procedures for signs of abnormalities or security breaches.

The review mechanism for internal documents and IT policies on data protection

4.75 All new staff are required to read and sign off their understanding of a number of internal circulars on data protection including all the DPPs under the Ordinance. There is however no record of regular review of these internal circulars.

4.76 Besides, SFAA IT Security Policy says that the Policy itself should be reviewed at least once a year but there is no evidence that this is done formally. Evidence (e.g. from the amendment history of the IT Security Policy) showed that the reviews of the IT policies and guidelines were triggered by events such as (1) the SFAA biennial security assessment recommendations and (2) review by Office of the Government Chief Information Officer of the Baseline IT Security Policy. There was no formal record to show that time-based review was carried out on a regular basis and at least once a year.

Commissioner's comments and recommendations

4.77 Given the substantial amendments to the Ordinance in 2012, the Commissioner sees the needs for SFAA to update its policies and internal documents on data protection to reflect the new requirements.

Recommendation:

(15) Regular reviews of the internal documents on the handling of personal data and IT security policies should be carried out and documented, and relevant documents and policies should be updated to take account of any new practices, or development in technology, etc.

Chapter Five

Conclusion

5.1 Given that SFAA is established to provide financial assistance to students in need, it is necessary for SFAA to collect personal data of the applicants and their family members. To ensure SFAA's data protection policies are fully complied with, a team of privacy respectful staff and a privacy-designed personal data system are necessary.

5.2 The Commissioner is reasonably satisfied with the data protection measures in the personal data system of the Identified Schemes. Based on the findings of the Inspection, he makes 15 recommendations, including but not limited to a review of the permanent retention of selected data, enquiry handling procedures, IT security awareness training, data encryption in backup tapes and control measures over the Data Prep Contractor.

5.3 The Commissioner wishes to thank the co-operation of the staff of SFAA, which helped this Office understand the data flow in detail and appreciate the reasons for collecting, retaining and processing of personal data. The Commissioner appreciates their assistance, rendered over and above their normal duties and in the peak seasons of receiving and processing applications.

5.4 The Commissioner hopes that this report will be of value to SFAA in respect both of the Identified Schemes and other schemes they administer but not covered by the Inspection. Other public bodies which collect personal data from members of the public for assessment of eligibility to financial assistance and handle personal data in a way similar to that mentioned in the report are encouraged to take reference from this report.

Annex 1 – List of Financial Assistance Schemes and Scholarships, Merit Award and Loan Fund Schemes

The 14 financial assistance schemes administered by SFAA include:

(1) Tertiary Student Finance Scheme - Publicly-funded Programmes
(2) Financial Assistance Scheme for Post-secondary Students
(3) Yi Jin Diploma Fee Reimbursement
(4) Financial Assistance Scheme for Designated Evening Adult Education Courses
(5) School Textbook Assistance Scheme
(6) Examination Fee Remission Scheme
(7) Student Travel Subsidy Scheme
(8) Subsidy Scheme for Internet Access Charges
(9) Kindergarten and Child Care Centre Fee Remission Scheme
(10) Pre-primary Education Voucher Scheme
(11) Non-means-tested Loan Scheme for Full-time Tertiary Students
(12) Non-means-tested Loan Scheme for Post-secondary Students
(13) Extended Non-means-tested Loan Scheme
(14) Continuing Education Fund

The 21 major scholarships, merit award and loan fund schemes administered by SFAA include:

(1) Sir Edward Youde Memorial Fellowships for Overseas Studies
(2) Sir Edward Youde Memorial Scholarships for Overseas Studies
(3) Sir Edward Youde Memorial Overseas Fellowship/Scholarship for Disabled Students
(4) Sir Edward Youde Memorial Fellowships for Postgraduate Research Students
(5) Sir Edward Youde Memorial Scholarships for Undergraduate and Diploma Students
(6) Sir Edward Youde Memorial Fellowships/Scholarships for Disabled Students
(7) Sir Edward Youde Memorial Awards for Disabled Students
(8) Sir Edward Youde Memorial Medals

(9) Sir Edward Youde Memorial Prizes for Senior Secondary School Students
(10) Sir Edward Youde Memorial Outstanding Apprentice Awards
(11) Sir Edward Youde Memorial Awards for Self-improvement for Working Adults
(12) Hong Kong Rotary Club Students' Loan Fund and Sing Tao Foundation Students' Loan Fund
(13) Agricultural Products Scholarship Fund and Marine Fish Scholarship Fund
(14) Japanese Government (Monbukagakusho:MEXT) Scholarship (Undergraduate Student)
(15) Li Po Chun Charitable Trust Fund - Overseas Postgraduate Study and Professional Training Scholarship
(16) Singapore Scholarships
(17) Sir Robert Black Trust Fund - Scholarships
(18) The University of Birmingham Hong Kong Postgraduate Scholarships
(19) Education Scholarships Fund
(20) Scholarship for Prospective English Teachers
(21) Grantham Scholarships Fund

Annex 2 – 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 is 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 is 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 is or is 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 is 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 it was collected, of-

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

(B) the name or job title, and address, of the individual who is to handle any such request made to the data user,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data was collected and that purpose is

specified in Part VIII of this Ordinance as a purpose in relation to which personal data is 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 is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used;

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

(i) the data is 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 is 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 is materially inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used by the third party; and

(ii) that data was inaccurate at the time of such disclosure,

that the third party-

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

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

(2) All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used.

(3) Without limiting subsection (2), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

(4) In subsection (3)—

data processor (資料處理者) means a person who—

(a) processes personal data on behalf of another person; and

(b) does not process the data for any of the person's own purposes.

3. Principle 3 - use of personal data

(1) Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose.

(2) A relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using his or her personal data for a new purpose if—

(a) the data subject is—

(i) a minor;

(ii) incapable of managing his or her own affairs; or

(iii) mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap 136);

(b) the data subject is incapable of understanding the new purpose and deciding whether to give the prescribed consent; and

(c) the relevant person has reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject.

(3) A data user must not use the personal data of a data subject for a new purpose even if the prescribed consent for so using that data has been given under subsection (2) by a relevant person, unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the data subject.

(4) In this section—

new purpose (新目的), in relation to the use of personal data, means any purpose other than—

(a) the purpose for which the data was 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

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

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

(2) Without limiting subsection (1), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

(3) In subsection (2)—

data processor (資料處理者) has the same meaning given by subsection (4) of data protection principle 2.

Annex 3 - Code of Practice on the Identity Card Number and other Personal Identifiers

Extract of the paragraphs on the collection of HKID Card Number and HKID Card Copy

"2.3 A data user should not collect the identity card number of an individual except in the following situations:

2.3.1 pursuant to a statutory provision which confers on the data user the power or imposes on the data user the obligation to require the furnishing of or to collect the identity card number;

...

"3.2 A data user should not collect a copy of an identity card except:

3.2.1 where the use of the copy by the data user is necessary:

...

3.2.1.2 for any of the purposes mentioned in section 58(1) of the Ordinance (the prevention or detection of crime, the apprehension, prosecution or detention of offenders, the assessment or collection of any tax or duty, etc.);

..."

Annex 4 - Personal data collected in Forms A, B and R of the Identified Schemes

The below table summarises the personal data collected by SFAA through the forms.

Item	Description	Applicant	Spouse	Unmarried children residing with the family	Dependent parent (if applicable)
(1)	English name	√	√	√	√
(2)	Chinese name	√	√	√	√
(3)	Correspondence address	√			
(4)	HKID Card Number	√	√	√	√
(5)	DOB	√	√	√	√
(6)	Home telephone number	√			
(7)	Mobile telephone number	√			
(8)	Marital status	√			
(9)	Job position	√	√	√ (Note a)	
(10)	Name of employer/firm	√	√	√ (Note a)	
(11)	Office telephone number	√	√	√ (Note a)	
(12)	Total annual income	√	√	√ (Note a)	
(13)	Other contribution	√	√	√	√
(14)	Medical expenses	√	√	√	√
(15)	Signature	√	√		

Item	Description	Applicant	Spouse	Unmarried children residing with the family	Dependent parent (if applicable)
(16)	Status			under education / in employment / unemployed / other	Dependency status
(17)	Residential address			√ (Note b)	
(18)	Student reference number			√ (Note b)	
(19)	School name			√ (Note b)	
(20)	School code			√ (Note b)	
(21)	Class attending			√ (Note b)	
(22)	Bank account name and number	√			
(23)	Scheme(s) applied for			√ (Note b)	
(24)	Comprehensive Social Security Assistance	√	√	√	√

Note a: applicable for unmarried children residing with the family and are in employment

Note b: applicable for primary and secondary students applying for financial assistance

Annex 5 – Types of data retained permanently

Types of data kept in CDs after case records are purged from SFAMS:

(A) Family base

1. Family application number
2. Applicant's English name
3. Applicant's HKID Card Number
4. Spouse's English name
5. Spouse's HKID Card Number
6. Applicant's and spouse's DOB
7. Unmarried children's English name
8. Unmarried children's HKID Card Number
9. Dependent parents' English name
10. Dependent parents' HKID Card Number
11. Unmarried children & dependent parents' DOB
12. Processing team number
13. Effective date
14. Applicant's annual income
15. Spouse's annual income
16. 30% of unmarried children's annual income
17. Other contribution
18. Medical expenses
19. Total income (item 14 + item 15 + item 16 + item 17 – item 18)
20. Denominator (number of family members +1 / +2)
21. Adjusted family income value (item 19 divided by item 20)
22. Final assistance level
23. Remarks

(B) Student base

24. Family application number + student reference number
25. Student's English name
26. Student's HKID Card Number
27. Student's DOB
28. Assistance level
29. Scheme(s) applied
30. Amount of assistance paid and value date
31. Treasury planning unit of student residential address
32. Examination Fee Remission amount
33. School code
34. Class code
35. Effective date for individual scheme

Annex 6 - Use of Personal Data

The Guidance Notes on the Application For Eligibility:

Extract of the paragraph on the provision / handling of personal data

"*5.2 The personal data provided in the application and any supplementary information provided on the request of the SFAA will be used by the SFAA and* [Education Bureau] */ disclosed to the agents of the SFAA /* [Education Bureau], *the schools / institutions concerned and relevant government bureaux / departments for the following purposes:-*

(i) Activities relating to the processing of application and notification of application results. For notification of application result, the applicant consents that the SFAA may inform schools / institutions of the results of the application, including assistance level, subsidy amount and date of payment of assistance;

(ii) Activities relating to authentication of application against other database of the SFAA and the database of other relevant government bureaux / departments in association with the student financial assistance received by the applicant / applicant's family members to prevent double subsidies;

(iii) Activities relating to the recovery of overpayments, if any;

(iv) Activities relating to the matching of the personal data of the student-applicant with the database of [Education Bureau] *in association with processing of the applicant for student financial assistance schemems and the granting of other student financial assistance by the SFAA, so as to verify / update student records of the SFAA and confirm eligibility of individual scheme;*

(v) Activities relating to the matching of the personal data of the applicant and applicant's family members with other database of the SFAA and the database of [Social Welfare Department] *in association with processing of the application, the granting of other student financial assistance by the SFAA and* [Social Welfare Department] *to prevent double subsidies*

and detect fraudulence;

(vi) Statistics and research purposes; and

(vii) Processing of applications / selection of needy students for award of other student financial assistance administered by the SFAA, the [Education Bureau]*, the* [Hong Kong Examinations and Assessment Authority]*, other relevant government departments / organizations and the schools / institutions concerned.*

5.3 The personal data of the applicant and those of his / her family members provided by the applicant may be disclosed to government bureaux / departments / organizations and the schools / institutions concerned for the purposes stated in paragraph 5.2 above; or where applicant has given consent to such disclosure; or where such disclosure is authorized or required by law."