創興銀行有限公司
Chong Hing Bank Limited

Privacy Policy Statement

December 2022

越秀集團成員 A Member of Yuexiu Group

Table of Contents

1. Interpretation

In this Policy Statement, unless the context otherwise requires:-

"Bank" refers to "Chong Hing Bank Limited"

"DPO" refers to the Bank's "Data Protection Officer"

"Group" refers to "Chong Hing Bank Limited and its subsidiaries"

"HKAB" refers to "Hong Kong Association of Banks"

"HKMA" refers to "Hong Kong Monetary Authority"

"HKSAR" refers to "Hong Kong Special Administrative Region of the People's Republic of China"

"Ordinance" refers to the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong)

"Other Relevant Rules and Guidelines" include those stipulated by Office of the Privacy Commissioner for Personal Data, the HKMA, the HKAB, and / or regulators / industrial organisations to which the Bank is subject to from time to time

"PCPD" refers to "Privacy Commissioner for Personal Data"

"PICS" refers to the Bank's "Personal Information Collection Statement" as may be varied or updated from time to time, which is available at the Bank's branches and website

"Staff" refers to all the employees of the Bank

2. Introduction

2.1 This Policy Statement provides information on the policies of the Bank under the Ordinance and Other Relevant Rules and Guidelines. The Bank applies, where practicable, those principles and processes set out herein to its operations. This Policy Statement will be taken into consideration by the Bank when formulating all data protection measures and initiatives. For the avoidance of doubt, this Policy Statement only sets out the Bank's policy on personal data privacy in relation to the operation of its Hong Kong branches and subsidiaries.

3. Company Corporate Policy in relation to Data Protection Strategy

3.1 The Bank respects personal data, and strives for protection of personal data privacy, confidentiality and security, and compliance with the provisions of the Ordinance and Other Relevant Rules and Guidelines.

3.2 Proper and adequate control measures are in place to protect the personal data of individuals and other persons, and its staff members are timely reminded of the importance of protecting personal data. The data security policies are persistently communicated to the Staff and promoted within the Bank on an on-going basis.

3.3 The Bank employs good practice in all business processes and operational procedures to protect personal data privacy of individuals and other persons by minimising data protection risk. The Bank endeavours to meet the reasonable expectations of integrity, security and fairness in the collection and use of personal information.

3.4 The Bank's management takes the lead to inculcate the Staff through effective communication and due reinforcement with the importance of personal data privacy and shares work norms which emphasise compliance with requirements under the Ordinance and Other Relevant Rules and Guidelines.

3.5 Where the individual legitimately requests access to or correction of his or her personal data held by the Bank, the Bank provides or corrects that data in accordance with the time and manner in compliance with the requirements under the Ordinance.

3.6 The Bank will not provide personal data of individuals and other persons to unrelated third parties for direct marketing or other unrelated purposes for monetary gains without consent of individuals and other persons or otherwise in breach of the Ordinance.

4. Appointment of Data Protection Officer

4.1 The Bank appoints DPO to oversee the compliance with the Ordinance, Other Relevant Rules and Guidelines and personal data protection policies of the Bank.

4.2 For making enquiries about the Bank's privacy policies and practices, please address to our DPO:-

Address : G. P. O. Box 2535, Hong Kong
Telephone : (852) 3768 6888
Facsimile : (852) 3768 1688
Email : dpo@chbank.com

5. Kinds of Personal Data Held by the Bank

5.1 There are mainly two broad categories of personal data held in the Bank. They are personal data related to customers and employment of the Bank.

5.2 Personal data held by the Bank regarding customers, which are necessary for customers to supply to the Bank from time to time for the purposes stated in Section 7 of this Policy Statement, may include but not limited to the following:-

(a) name and address, occupation, contact details, date of birth and nationality of customers, and their identity card and / or passport numbers and place and date of issue thereof;

(b) current employer, position and personal income of customers;

(c) details of all assets and wealth held by customers;

(d) information obtained by the Bank in the ordinary course of the continuation of the business relationship;

(e) information as to credit standing provided by a referee, credit reference agency(-ies), or debt collection agency in connection with a request to collect a debt due from any customer to the Bank; and

(f) personal information in the public domain.

5.3 Personal data relating to employment held by the Bank may include but not limited to the following:-

(a) name, address, contact details, date of birth, nationality, resumes, qualifications, working experience, identity card and / or passport numbers and place and date of issue of the Staff and potential employees;

(b) name, contact details, date of birth, identity card and / or passport numbers and place and date of issue of the family members and / or connected parties of the Staff;

(c) additional information compiled about potential employees to assess their suitability for a job in the course of the recruitment selection process which may include references obtained from their current or former employers or other sources;

(d) additional information compiled about Staff which may include records of remuneration and benefits paid to Staff, records of job positions, job particulars, transfer and training, records of medical checks, sick leave and other medical claims, group medical insurance records, mandatory provident schemes participation, disciplinary matters and performance appraisal reports of Staff;

(e) relevant personal data pertaining to former employees for the Bank to fulfill its obligations to the former employees and its legal obligations under certain ordinances; and

(f) personal information in the public domain.

5.4 The Bank may hold other kinds of personal data which it needs in the light of the specific nature of its business.

6. Collection of Personal Data

6.1 The Bank only collects necessary, adequate but not excessive personal data, and collection of personal data is in a lawful and fair manner. Individuals and other persons shall supply data in connection with the opening or continuation of operation of accounts, and / or the establishment or continuation of provision of banking facilities and / or the provision of banking, financial services (which is defined as including but not limited to credit card, fiduciary, securities and / or investment services) and / or insurance services or compliance with any laws, guidelines or requests issued by regulatory or other authorities, or otherwise carry out transactions as part of the Bank's services. If individuals and other persons do not supply data, the Bank may not be able to provide / continue providing services to them.

6.2 The Bank will also collect data relating to an individual or other person from third parties, including third party service providers with whom the individual or other person interacts in connection with the marketing of the Bank's products and services and in connection with the individual's or other person's application for the Bank's products and services (including receiving personal data from credit reference agencies approved for participation in the Multiple Credit Reference Agencies Model (hereinafter referred to as "credit reference agencies")).

6.3 In the course of collecting personal data, the Bank provides the individual concerned with PICS informing him or her of the purposes of collection, consequences of failure to supply his / her personal data, classes of persons to whom the data may be transferred, his or her right to access and correct the data, direct marketing policy and a response channel, contact person for requesting access or correction and other relevant information.

6.4 Save for the purposes for the opening or continuation of accounts, or provision of banking services, the Bank will not collect personal data from minors (particularly those who are incapable of making an informed decision) without prior consent from a person with parental responsibility or guardianship for the minors.

6.5 Prior to collecting and obtaining any personal data from public domain, the Bank will observe the original purposes of making the personal data available in the public domain and the restrictions (if any and if they have reasonably come to the Bank's notice) imposed by the original data users on further users.

6.6 In relation to the collection of personal data online, the following practices are adopted:-

(a) The Bank follows adequate standards of security and confidentiality to protect any information provided to the Bank online by customers. Encryption technology is employed for sensitive data transmission on the Internet to protect personal data privacy.

(b) The Bank uses cookies on the Bank's website in order to enable the Bank to evaluate and improve its website by tracking how users navigate through the website. A cookie is a small file that can be placed on users' computer hard disk. Users are not obliged to turn on "Cookies" of their browser for the website, and users can disable "Cookies" by changing the setting of web browser but may find that certain features on the Bank's website will not function properly. When users visit the Bank's website, the Bank's server will record their data such as IP address together with the date, time and duration of visit. The Bank uses the information obtained to compile statistical data on the use of the Bank's website but such information is used on an anonymous and aggregated basis, and users cannot be identified from the compiled data. The cookies will expire once the session is closed.

(c) The Bank may work with third parties (for example, digital analytic solution providers) to track website usage and activities by using cookies at its website on the Bank's behalf. The information collected will be kept for an appropriate period of time based on the actual needs to fulfil the original or directly related purpose for which it was collected and to satisfy any applicable statutory or contractual requirements. No personally identifiable information will be collected or shared with other third parties.

(d) The Bank collects customer's personal data through the Bank's website for processing transactions and executing instructions for the purposes stipulated in the Bank's PICS. The Bank endeavours to maintain and keep customer's personal data confidential.

6.7 In relation to personal data relating to employment, the Bank only collects personal data for purposes stated in Section 7 of this Policy Statement.

6.8 Closed Circuit Television ("CCTV") cameras are positioned in the vicinity of ATM machines and inside the area of branches of the Bank for security and safety purposes with CCTV recording system in operation. Conspicuous notices are posted inside these areas to notify persons the purposes of personal data collection.

6.9 The Bank endeavours to ensure that its Staff abide by "Code of Conduct for Employees" all the times in the use and confidentiality of information during their employment or after their cessation of employment.

7. Purposes of Using Personal Data

7.1 The Bank intends to use the personal data collected from a customer and / or an individual for the purposes including:-

(a) in considering, assessing and processing any applications from customers and / or individuals concerning the provision of banking, financial and / or insurance services;
(b) in the daily operation of the banking, financial and / or insurance services and facilities provided to customers;

(c) in conducting credit checks at the time of application for credit and / or at the time of regular or special reviews which may take place on one or more occasions every year;
(d) in creating and maintaining the Bank's credit scoring and other risk models;
(e) in assisting other credit providers in Hong Kong approved for participation in the Multiple Credit Reference Agencies Model to conduct credit checks and collect debts;
(f) in ensuring ongoing credit worthiness of customers and / or individuals;
(g) in designing banking, financial and / or insurance services and products for customers' use;
(h) in marketing services, products and other programmes (please refer to paragraph 8 of the Bank's PICS which is available at its website www.chbank.com);
(i) in determining amounts owed to or by customers or individuals;
(j) in enforcing the Bank's rights, including but not limited to the collection of amounts outstanding from customers and in providing security or guarantee for customers' obligations;
(k) in compliance with any requirements existing currently and in the future for disclosure and use of data that are applicable to or is expected to be complied with by the Bank, any of its holding company, subsidiary of any such holding company, controller of the Bank (as such terms are defined in the Banking Ordinance (Chapter 155 of the Laws of Hong Kong)), its subsidiary companies and / or any of the Bank's branches and offices from time to time within and / or outside the jurisdiction of the HKSAR according to:-
    (i) any law binding or applying to it (e.g. the Inland Revenue Ordinance and its provisions including those concerning automatic exchange of financial account information);
    (ii) any Order / Judgment made by a competent Court or Tribunal;
    (iii) any guidelines or guidance of any local or foreign legal, regulatory, tax, governmental, law enforcement or other authorities, or self-regulatory or industrial bodies or associations of financial services providers (e.g. guidelines or guidance given or issued by the Inland Revenue Department including those concerning automatic exchange of financial account information); and
    (iv) any present or future contractual or other commitment with legal, regulatory, tax, governmental, law enforcement or other authorities, or self-regulatory or industrial bodies or associations of financial services providers;
(l) in compliance with any obligations, requirements, policies, procedures, measures or arrangements for disclosing or using data and information concerning the sanction, prevention, detection, investigation and / or prosecution of money laundering, terrorist financing or other unlawful activities within or outside the jurisdiction of the HKSAR;
(m) in enabling an actual or proposed assignee of the Bank or participant or sub-participant of the Bank's rights in respect of the customer and / or individual to evaluate the transaction intended to be the subject of the assignment, participation or sub-participation; and
(n) any purposes relating thereto.

7.2 All the information and personal data sent to the Bank via the Bank's website shall remain and be deemed the property of the Bank and shall be free to use by the Bank for any lawful purpose subject to the compliance with the Ordinance.

7.3 The purposes for which personal data relating to Staff and potential employees may be used by the Bank are as follows:-

(a) Human resources management
(1) processing employment applications;
(2) determining the terms and conditions of staff employment;
(3) considering eligibility for and administration of staff loans and benefits / entitlements;
(4) providing and maintaining the payroll, compensation and benefits for the Staff and their family members;
(5) maintaining a database of the Staff's personal data;
(6) conducting performance management process, promotion, transfer, job rotation, training, demotion, secondment, relocation and termination of employment, wherever applicable;
(7) considering reorganisation of the Bank, when necessary;
(8) providing reference letters to staff;
(9) facilitating communication between the Staff and the Bank; and
(10) maintaining daily operation of the Bank and any other lawful purposes which are related to the Staff employment with the Bank such as providing employee references and compiling tax returns.

(b) Compliance with internal rules, statutory and / or legal requirements
(1) registering Staff members as intermediaries or licences with statutory authorities / institutions;
(2) conducting credit checks on staff creditworthiness;
(3) conducting checking as part of the Bank's anti-money laundering and counter terrorist financing controls;
(4) monitoring connected lending activities;
(5) detecting or conducting investigation regarding any suspicious fraud cases, misconduct or criminal activities;
(6) conducting surveys and generating data for analysis, statistics and audits; and
(7) meeting the regulatory requirements applicable to the Bank.

(c) Any other purposes relating or incidental to any of the above.

8. Disclosure of Personal Data

8.1 Personal data held by the Bank relating to individuals and other persons will be kept confidential but the Bank may provide or transfer such information to the following major classes of persons within or outside the HKSAR for any purposes set out in Section 7 above or for other purposes specified in the Bank's PICS:-

(a) the Bank's officers, Staff and / or agents;
(b) the Bank's agents, contractors or third party service providers;

(c) credit reference agencies (including the operator of any centralised database used by credit reference agencies) and debt collection agencies;
(d) local or foreign legal, regulatory, tax, governmental, law enforcement or other authorities; and
(e) any holding company, subsidiary of any such holding company and controller of the Bank.

For details, please refer to the Bank's PICS which is available at its website www.chbank.com.

8.2 CCTV is installed and used in the vicinity of ATM machines and inside the area of the branches of the Bank for general security and to monitor any possible wrongful, illegal and / or unlawful activity. CCTV may capture images of individuals and other persons or information relating to such individuals and other persons. Personal data may be collected from the CCTV and may prospectively be used and transferred as per the relevant sub-paragraphs under paragraphs 4 and 5 of the PICS for security, investigation, prevention of and / or enforcement of the Bank's rights in any criminal, unlawful, or other wrongful activities. Personal data collected from the CCTV in the form of recorded images will not be used by the Bank for any direct marketing nor will it be provided to any entity for direct marketing purposes.

8.3 For Staff and potential employees, the Bank may disclose and transfer their personal data as specified in Section 5.3 within as well as outside the HKSAR, to the individuals and parties including but not limited to the Bank's subsidiaries and associate companies; any other branches, offices or centres of the Bank; the Bank's insurers and bankers; medical practices providing medical cover for the Staff; administrators or managers of the Bank's retirement schemes; any relevant provident fund managers; any agents, contractors, or third party service providers who provide administrative, telecommunications, computer or other services to the Bank in connection with the operation of the Bank's business; persons seeking employee references in respect of Staff with the prescribed consent of the Staff concerned; any actual or proposed purchaser of all or part of the business of the Bank or, in case of any merger, acquisition or other public offering, the purchaser or subscriber for shares in the Bank; third parties in the form of directories of names and office telephone numbers of key officers of the Bank for promotional and administrative purposes; government and other legal or statutory / regulatory bodies; and other companies engaged in contractual activities on the Bank's behalf; for the purposes set out in Section 7.3 of this Policy Statement.

8.4 The Bank may, in accordance with the customer's instructions to the Bank or third party service providers engaged by the customer, transfer customer's data to third party service providers using the Bank's API for the purposes notified to the customer by the Bank or third party service providers and / or as consented to by the customer in accordance with the Ordinance.

9. Intra-group Sharing of Personal Data

9.1 Unless prescribed consent is obtained, any sharing of the data within the Group could be restricted to the purposes of collection or directly related purposes including the purpose of providing the services to the customers and on a "need-to-know" and "need-to-use" basis. The Bank will not share customer's personal information with unrelated third parties without obtaining prescribed consent from the customer. Where it is necessary to share customer's personal data within the Group for providing services sought by the customer or directly related matters, the members of the Group should have already informed the customer of such intended information sharing through their respective PICS and / or Account Terms of varying products and facilities.

10. Accuracy of Personal Data

10.1 The Bank takes practical steps to ensure that personal data it collects, uses or discloses are accurate, complete and up to date, having regard to the purposes (including any directly related purposes) for which the personal data are or are to be used.

10.2 The Bank mails all correspondence to a customer's latest address in the Bank's record. Customers shall, as soon as practicable, notify the Bank of any change of personal particulars provided to the Bank which may affect the provision of the banking services to them by completing the Bank's standard forms or by other duly signed written instruction.

10.3 In relation to personal data relating to employment, Staff who wish to update their personal data can do so by completing the "Employee Information Update Form" or by accessing to the relevant system in the Bank's intranet.

11. Retention of Personal Data

11.1 The Bank takes practicable steps to ensure that personal data will not be kept longer than necessary for the fulfillment of the purposes (including any directly related purpose) for which the data are or are to be used and the compliance of all applicable statutory and regulatory requirements and contractual obligations. Different retention periods apply to the various kinds of personal data collected and held by the Bank in accordance with its internal customer document retention and destruction policy subject to the legal and regulatory requirements.

11.2 Recorded images captured by CCTV described in Section 8.2 above are retained for 90 days and are safely deleted as soon as practicable once the purpose of collection is fulfilled unless (i) notice in writing is received from authority requiring to keep the records for a longer period which are related to an ongoing criminal or other investigation, or to any other purposes as specified in the notice; or (ii) it is necessary or justified for the Bank to keep the record images for a longer period for purposes set out in Section 8.2 above.

11.3 The Bank retains the personal data of unsuccessful job applicants for future recruitment purposes for a period of not longer than 2 years from the date of rejecting the applicant, unless there is subsisting and adequate reason that obliges the Bank to retain the data for a longer period or that applicant has given prescribed consent for the data to be retained beyond 2 years.

11.4 For personal data of successful job applicant, the Bank retains their personal data during their employment and after they cease to be employed by the Bank, but such data will be retained for not longer than 7 years from the date of their cessation of employment, unless there is subsisting and adequate reason that obliges the Bank to retain the data for a longer period or that former employee has given prescribed consent for the data to be retained beyond 7 years.

12. Security of Personal Data

12.1 The Bank ensures an appropriate level of protection for personal data in order to prevent unauthorised or accidental access, processing, erasure, loss or other use of that data.

12.2 The Bank restricts physical access to data by providing secure storage facilities, and incorporates security measures into equipment in which data are held with a view to achieving appropriate levels of security protection.

12.3 Computer data are stored on computer systems and storage media to which access is controlled.

12.4 Where the Bank holds, uses and transmits personal data, steps will be taken to protect them from accidental or unauthorised disclosure, change or destruction.

12.5 Recorded images captured by CCTV are kept in safe custody. Hard disks and any devices storing the recorded images are securely protected from unauthorised access and only viewed, retrieved or handled upon proper authorisation for the intended purposes.

12.6 Other security measures of the Bank include:-
(a) educating Staff as to their obligations with regard to personal information;
(b) encrypting data transmitted from customer's computer to its systems;
(c) employing firewalls, intrusion detection systems and virus scanning tools to protect against unauthorised persons and viruses from entering its systems; and
(d) ensuring security controls in place to protect against unauthorised access to buildings by any person.

13. Data Breach Handling

13.1 The Bank will ensure any material breaches of personal data protection requirements or loss or leakage of customer data are properly handled in a timely manner according to relevant guidelines and reported to the relevant authorities where appropriate.

14. Handling of Personal Data in Debt Collection

14.1 The Bank may use an individual's personal data for recovery of any debts due and owing from the customer who is in default of payment, including transfer of the data of the customer and security providers concerned to debt collectors for debt collection purposes. Such use is directly related to the original purpose of data collection.

14.2 Unless there is a real need to do so, the Bank will not disclose sensitive data including information showing the financial problems of a customer to any third parties.

14.3 The Bank will act according to "Code of Practice on Consumer Credit Data": by contractual means requiring its debt collection agent to follow such conduct as stipulated by the "Code of Banking Practice" in relation to debt collection activities; restricting the kinds of debtor's data that may be disclosed to the agent to identification and location data, the nature of the credit and the amount to be recovered and goods to be repossessed; checking the accuracy of the data before providing it to the agent.

15. Outsourcing Personal Data Processing

15.1 When the Bank engages a data processor, whether within or outside the HKSAR, to process personal data on the Bank's behalf, the Bank adopts contractual or other means with a view to (i) preventing any personal data transferred to the data processor from being kept longer than is necessary for processing of the data; (ii) preventing unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing. Personal data may include specified account information and personal particulars of the customers and individuals depending on the nature of the process.

15.2 The Bank may incorporate additional contractual clauses in the service contract or enter into a separate contract with the data processors. The types of obligations to be imposed on data processors by contract may include the following:-

(a) security measures required to be taken by the data processor to protect the personal data entrusted to it and obligating the data processor to protect the personal data by complying with the data protection principles;

(b) timely return, destruction or deletion of the personal data when it is no longer required for the purpose for which it is entrusted by the Bank to the data processor;

(c) prohibition against any use or disclosure of the personal data by the data processor for a purpose other than the purpose for which the personal data is entrusted to it by the Bank;

(d) absolute prohibition or qualified prohibition on the data processor against sub-contracting the service that it is engaged to provide;

(e) where sub-contracting is allowed by the Bank, the data processor's agreement with the sub-contractor should impose the same obligations in relation to processing on the sub-contractor as are imposed on the data processor by the Bank; where the sub-contractor fails to fulfill its obligations, the data processor shall remain fully liable to the Bank for the fulfilment of its obligations;

(f) immediate reporting of any sign of abnormalities or security breaches by the data processor;

(g) measures required to be taken by the data processor to ensure that its relevant staff members will carry out the security measures and comply with the obligations under the contract regarding the handling of personal data;

(h) the Bank's right to audit and inspect how the data processor handles and stores personal data; and

(i) consequences for violation of the contract.

15.3 The Bank may engage non-contractual monitoring and auditing mechanisms to monitor its data processors' compliance with data protection requirements, such as through the adoption of the following measures:-

(a) The Bank will endeavour to select reputable data processors offering sufficient guarantees in respect of the technical competence and organisational measures governing the processing to be carried out, and with a good track record on data protection.

(b) The Bank shall endeavour to be satisfied that the data processors have robust policies and procedures in place, including adequate training for their staff and effective security measures, to ensure that the personal data in their care are properly safeguarded at all times and are not kept for longer than necessary.

(c) The Bank shall have the right to audit and inspect how the data processors handle and store personal data, and exercise the right to audit and inspect when warranted.

16. Access and Correction of Personal Data

16.1 Under the terms of the Ordinance, individuals have the right to:-

(a) ascertain whether the Bank holds any personal data relating to them and, if so, obtain copies of such data by means of a data access request;

(b) require the Bank to correct personal data in its possession which is inaccurate for the purpose for which it is being used by means of a data correction request; and

(c) ascertain the Bank's policy and practices in relation to personal data, which are those policies set out in their entirety therein.

16.2 The Bank will impose a fee for complying with a data access request in accordance with the Ordinance. The cost of compliance may vary with the scope and complexity of the data access request in question. Individuals can make reference to the Bank's latest "Bank Service Charges" accessible at its website www.chbank.com for the fee in relation to a data access request. The Bank is entitled to refuse to comply with a data access request unless and until the fee imposed has been paid.

16.3 Individuals may exercise their right of access by:-

(a) completing the "Data Access Request Form" (Form OPS003 specified by the PCPD) in Chinese or English; and

(b) sending the completed form, along with appropriate proof of identity (a copy of the applicant's Hong Kong Identity Card or Passport), and the applicable fee to the DPO of the Bank or any of the Bank's branches.

16.4 The Bank will, upon satisfying itself of the authenticity and validity of the access request, comply with a data access request within 40 calendar days after receiving the request.

16.5 The Bank may withhold personal data under exemption provisions of the Ordinance.

16.6 Staff who wish to access and correct their personal data can complete "Data Access Request Form" or "Employee Information Update Form" and forward it to Human Resources Division or amend the data through the relevant system in the Bank's intranet.

17. Direct Marketing and Opt-out Requests

17.1 The Bank will use the personal data of an individual or other person in direct marketing but will not do so unless it has received the consent of an individual or other person (which includes an indication of no objection) to the intended use.

17.2 On the first occasion when the Bank uses an individual's or other person's personal data for direct marketing by telephone, mail or any means, it will inform the individual or other person that he / she may, on a no charge basis, request the Bank to cease to use his / her personal data in direct marketing. This arrangement is generally described as "direct marketing opt-out".

17.3 An individual or other person may also, on a no charge basis, require the Bank to cease using his / her personal data for direct marketing at any time by filling in the "Instruction on Direct Marketing" available at the Bank's website at www.chbank.com or by contacting any branch of the Bank or Customer Services Hotline at 3768 6888. To make an enquiry about their direct marketing opt-out records, customers may visit any branch of the Bank or contact the said Customer Services Hotline.

17.4 The Bank accepts an unsubscribe request made from individuals and other persons during person-to-person marketing calls, and will not make person-to-person marketing calls to the individuals and other persons on the unsubscribe list.

17.5 The Bank does not retrieve personal data from public registers for direct marketing.

17.6 In relation to the use of personal data by the Bank in direct marketing, please refer to paragraph 8 of the Bank's PICS which is available at its website www.chbank.com.

18. Off-site Marketing Campaign

18.1 The Bank during off-site marketing activities will take practicable steps to ensure the safe storage and secure transmission of the personal data so collected:-

(a) the personal data is not seen by or accessible to irrelevant parties during and after the collection process;
(b) forms and documents collected ("application documents") will be properly logged;
(c) the application documents are securely stored in a locked container under the custody of a designated officer;
(d) adequate security protection is provided by encryption of any such personal data stored in portable storage devices;
(e) specific precautionary measures are implemented to ensure secure transmission of the application documents to the Bank;
(f) the Staff are prohibited from bringing home any of the application documents; and
(g) a designated officer is appointed to oversee security of the application documents.

19. Revision of Privacy Policy Statement

19.1 This Policy Statement is subject to review and change from time to time. Please approach the Bank or visit the Bank's website at www.chbank.com regularly for the latest Policy Statement.

(In case of any inconsistencies between the English and Chinese versions of this Policy Statement, the English version shall prevail.)