Personal Data System of Hong Kong College of Technology
Inspection Report

Published under Section 48(1) of the Personal Data (Privacy) Ordinance,
Chapter 486 of the Laws of Hong Kong

Background

On 21 February 2024, the Hong Kong College of Technology (HKCT) submitted a data breach notification to the Office of the Privacy Commissioner for Personal Data (the PCPD), reporting that one of its servers containing personal data had been attacked by ransomware and maliciously encrypted (the Data Breach Incident), affecting the personal data of approximately 8,146 individuals, including students, course applicants and ex-employees. The affected personal data included names, identity card numbers, mobile phone numbers, home phone numbers, dates of birth, email addresses, genders, photos, certificate examination results and proof of academic results, staff positions, corresponding departments, names of supervisors and their comments, addresses, bank account numbers and partial bank transaction records. Upon receiving the data breach notification, the PCPD commenced an investigation into the Data Breach Incident in accordance with established procedures, and issued a warning letter to HKCT upon the completion of the investigation.

Against this background and given that an upward trend in data breach incidents involving educational institutions was observed in recent years, the Privacy Commissioner for Personal Data (the Privacy Commissioner), Ms Ada CHUNG Lai-ling, considered that it was in the public interest to carry out an inspection (the Inspection) of the personal data system used by HKCT under section 36(a) of the Personal Data (Privacy) Ordinance (the PDPO), to assess the effectiveness of the remedial measures taken by HKCT following the Data Breach Incident and to further examine the data security of its systems containing personal data.

HKCT, as a data user under the PDPO, is obliged to comply with the requirements under the PDPO, which include the six data protection principles in Schedule 1 to the PDPO with respect to the collection, holding, processing and use of personal data. The Inspection focused on the measures implemented by HKCT regarding the security of personal data.

PCPD's officers conducted on-site inspections this year to inspect the personal data system of HKCT and assess the compliance with HKCT's security policies and practices by its employees. Through two rounds of written enquiries (including those following on-site inspections), the PCPD obtained and examined HKCT's policies, procedures, guidelines, training materials and other documents related to HKCT's personal data system.

Results of the Inspection

Areas of Good Practice

The Privacy Commissioner noted HKCT's good practices in the following areas:-

(i) Following the Data Breach Incident, HKCT has implemented settings on its email system to prevent suspicious emails, and provided staff with training on personal data protection, including the cybersecurity trainings "Phishing Prevention Awareness Drill" and "Constructing a Collective Firewall", which aimed at enhancing staff awareness on cybersecurity and safeguarding against suspicious emails;

(ii) HKCT has also enhanced the security and detection measures of its information system following the Data Breach Incident, including deploying antivirus software, endpoint detection and response solutions, situational awareness monitoring system, and dual firewalls to conduct real-time detection and analysis, and the firewall log records are reviewed by members of the information technology department on a daily basis. HKCT also plans to establish a dedicated task force on information security to monitor its network environment and information systems, thereby strengthening its capabilities to address potential cyberthreats;

(iii) HKCT has established a personal data privacy management programme and appointed a dedicated data protection officer. HKCT has also stipulated policies and guidelines in relation to data protection, which would be overseen and enforced by the data protection officer and responsible department heads;

(iv) HKCT's human resources department briefs all new employees on the contents of the employee handbook, including policies and guidelines related to data protection;

(v) HKCT has also developed a data breach incident response plan, which includes specific procedures needed to be executed and the review mechanism after a data breach incident occurs;

(vi) HKCT has provided information related to information security and network security on its intranet, and further disseminated relevant links to staff members via emails to enable them to access additional information;

(vii) HKCT adopts the "least privilege" principle and "role-based" access control mechanism, under which department heads grant employees the minimum access right necessary to perform their duties based on their roles and job responsibilities, and instruct the information technology department to configure corresponding access permissions for each employee; and

(viii) HKCT has engaged third-party cybersecurity experts to conduct vulnerability scans and penetration tests annually to identify the vulnerabilities within the systems, and implement corresponding remedial measures to reduce the risks of cyberattacks.

Areas for Further Improvement

Notwithstanding the good practices described above, the Privacy Commissioner noted the following areas for improvement in the measures implemented by HKCT in safeguarding personal data:-

(i) The "Departmental Operational Guideline" of HKCT's information technology department is principal-based and does not include detailed implementation procedures for technical and operational security measures, including operational requirements for the use and update of security devices and software, as well as the implementation of patching management etc., which may lead to security risks due to staff misinterpretation or inconsistent implementation;

(ii) HKCT has devised guidelines for data retention and deletion for different departments. However, the level of detail in these guidelines varies across different departments. Moreover, HKCT has not reviewed whether the personal data of former students stored in the admissions and management system should be deleted in accordance with these guidelines;

(iii) HKCT has not regularly monitored or audited staff records of access to and retrieval of personal data in the admissions and management system. As a result, it is unable to identify whether there is excessive access to or retrieval of personal data stored in the system;

(iv) The academic affairs office of HKCT provides the personal data of students to various departments upon request. However, HKCT has not established a clear mechanism to assess whether such requests are reasonable, or to ensure that the departments delete the data from their records after use; and

(v) HKCT has not conducted any security audits on its information systems, and therefore has not been able to evaluate the effectiveness of its existing security measures from a holistic perspective.

Conclusion

After the data breach incident that happened in 2024, HKCT has implemented various technical measures to enhance the security and detection capabilities of its information systems, established a personal data privacy management programme and appointed a dedicated data protection officer, and provided staff members with training and information on the protection of personal data to enhance staff awareness on cybersecurity and to safeguard them against suspicious emails. HKCT has adopted the "least privilege" principle and "role-based" access control mechanism, under which department heads grant the minimum necessary access rights to staff members based on their roles and job responsibilities. HKCT has also established a data breach incident response plan.

Overall, the Privacy Commissioner considers that HKCT has complied with the requirements of Data Protection Principle 4 of Schedule 1 to the PDPO concerning the security of personal data in the handling of the personal data of students and staff.

Despite HKCT's good practices, the Privacy Commissioner considers there are areas which can be improved in safeguarding personal data. These include developing more comprehensive and specific policies on information security and data retention, enhancing the review of records for information systems containing personal data, and conducting regular security audits to further strengthen the protection of the personal data it holds.

Recommendations

Through the Inspection, the Privacy Commissioner wishes to make the following recommendations to HKCT to implement appropriate organisational and technical measures to safeguard the information systems containing personal data and enhance data security:-

(i) Formulate detailed and comprehensive information security policies and procedures that transform the existing principles into operational procedures and technical control measures, providing staff members with a concrete cybersecurity framework to follow. Additionally, HKCT should

establish monitoring mechanisms to ensure staff compliance with all the requirements relating to data security, thereby reducing risks and security vulnerabilities caused by inconsistent implementation;

(ii) Develop a data retention policy applicable to all departments of HKCT. Within the operational guidelines tailored to individual departments, clearly specify the types of personal data held by each department, the retention period for such data, and the procedures for data deletion (including methods for deleting both physical and electronic records);

(iii) Regularly review the personal data of former students stored in the admissions and management system, and delete any data that has reached the end of its retention period in accordance with applicable data retention policies or guidelines;

(iv) Establish a comprehensive monitoring mechanism to regularly review log records of all information systems containing personal data, and develop alert protocols for abnormal activities and mechanisms for notifying relevant personnel, enabling early detection of irregular data access and export;

(v) The academic affairs office should assess whether departmental requests for personal data are reasonable and establish mechanisms for departments to delete data accordingly; and

(vi) Conduct regular security audits of information systems to evaluate whether HKCT's information security policies, procedures and measures are being properly implemented, and identify areas that require rectification or enhancement.

Through the above inspection results, the Privacy Commissioner would also like to make the following recommendations to educational institutions that handle vast amounts of personal data of students and staff members to ensure data security, including:-

- Establish a Personal Data Privacy Management Programme and appoint designated officer(s) as Data Protection Officer(s);
- Establish clear internal policies and procedures on data governance and data security, and ensure thorough implementation of the same;
- Provide staff with training on data protection and information security upon onboarding and at regular intervals;
- Adopt the "least privilege" principle and "role-based" access control mechanisms;
- Implement effective measures to prevent, detect, and respond to cyberattacks;
- Conduct comprehensive security risk assessments and audits for information systems regularly;
- Exercise due diligence in appointing and managing data processors; and
- Formulate response plans for data breach incidents and incidents involving artificial intelligence.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
13 November 2025