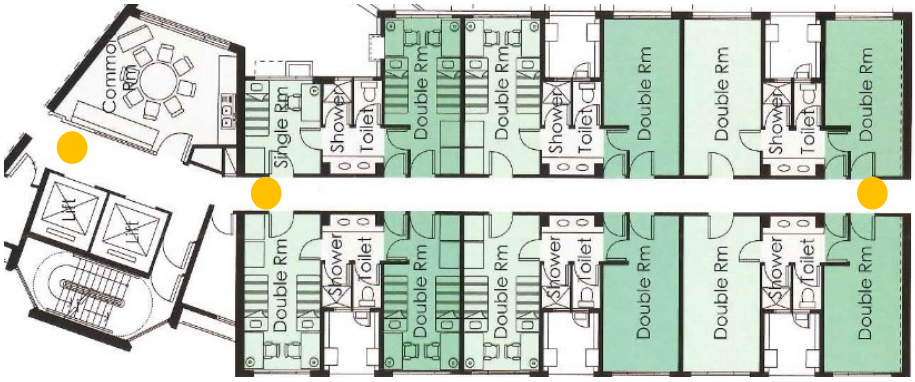
Q& A

CCTV on Student floors

1. **Q: Where are the CCTV cameras installed on student floors, including RM floor?**

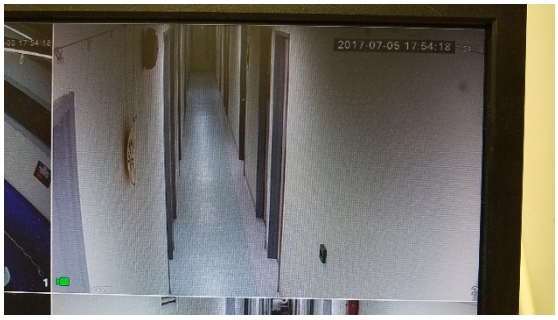
   A: At corridor on student floor, as sample shown below, with clear display of CCTV warning stickers posted at site.



: CCTV

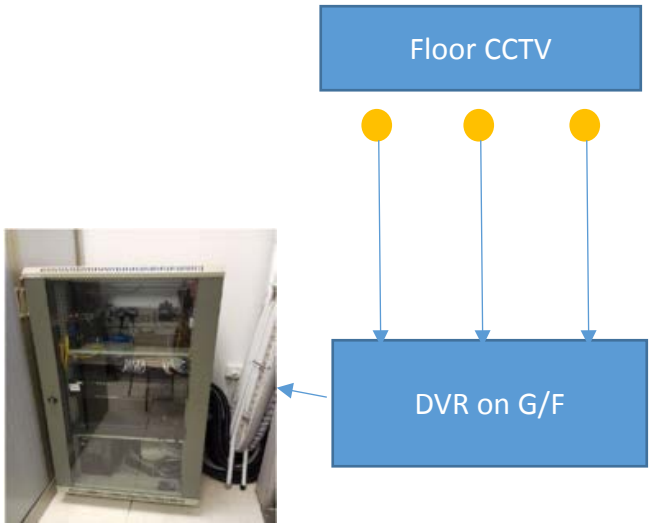
2. **Q: Will the inside of student rooms be viewed from CCTV?**

   A: Absolutely not! The cameras are strategically located to cover the corridor only, as shown in the sample views below, without infringing into any student privacy inside the room:



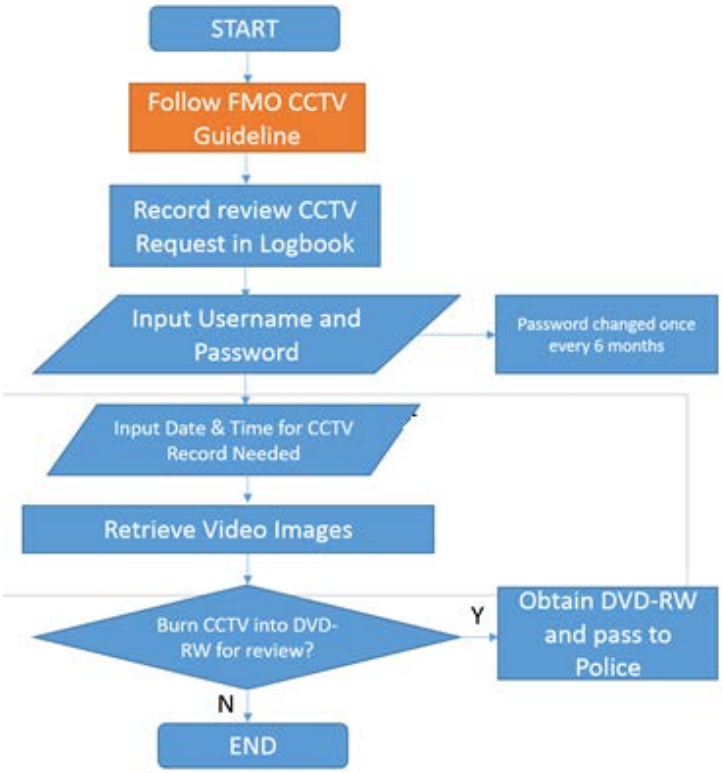
3. **Q: Will CCTV make me feel being monitored?**

   A: Absolutely no worry! Video images captured by CCTV are directly transmitted to and locked in DVR hard-disc without human intervention at all. The schematic below illustrates capture and store process:



4. Q: How is installation, recording, storage and retrieving of CCTV captures accessed?

A: Access to CCTV footage is under STRIGENT control as below:



5. Q: Under what circumstances will CCTV captures on student floor be retrieved and viewed?

A: In line with FMO CCTV Handling Guideline (V.4) and according to the requirements of Personal data (Privacy) Ordinance (Cap. 486) and to cope with the university environment*[refer to PCPD Media Statement dated 20 Sep 2017 overleaf], there are 3 reasons for reviewing the "image file(s)" and making copies:

i. Comply with the exemptions of law enforcement agents and investigators in Chapter 486, Section 58 of the Laws of Hong Kong;
ii. Comply with the authorization under the common laws, such as saving lives without delay, preventing suicide, elevator accident, etc.;
iii. Involve with legal liability and disciplinary investigations that CityU may undertake, such as sexual harassment, any violation incident, traffic accident, accidental injuries, property damage, etc.

The rule of thumb is charted as follows for easy reference:

Circumstances	Authorized Persons
Facilitating law enforcement *e.g. police investigation*	Director (SRO) & Resident Master
Authorization under common laws *e.g. saving lives, preventing suicide, elevator accident*	Director (SRO) & Resident Master
Legal liability & disciplinary investigations *e.g. sexual harassment, any violation incident, accident/ injuries, property damage*	Director (SRO) & Resident Master

6. Q: How can CCTV make me feel secured?

A: i) The purpose of CCTV on student/RM floors is to ensure University's duty of care and safety of hall residents;

ii) There is a logbook in Security Control to record each and every retrieval and viewing of CCTV images, which RM has the authority to examine it on regular basis;

iii) In residential year 2017/18, there is NOT a single case/circumstance making retrieving/viewing of CCTV captures on student floors in Hall 2 necessary.

Last updated on 9 March 2019

**** Source:*** **https://www.pcpd.org.hk/english/news_events/media_statements/press_20170920.html**

Date: 20 September 2017

PCPD Media Statement: Privacy is not a shield for those infringing legitimate interests; Education University is still required by law to ensure personal data security

(20 September 2017) The Office of the Privacy Commissioner for Personal Data ("PCPD") has completed a compliance check on the data leakage incident regarding the screenshots of CCTV footage of the Education University of Hong Kong ("EdUHK") and has requested the EdUHK to take appropriate remedial measures to prevent recurrence of such a data leakage incident. Having considered the concern and expectation of the public and the relevant parties, the PCPD would provide a response as follows.

EdUHK's purpose of circulating the screenshots

The compliance check revealed that, after the EdUHK had learnt that a certain banner had appeared on the campus Democracy Wall on 7 September 2017, it received enquiries from various parties, including the media. The EdUHK observed that if it was EdUHK's students who had posted the banner, the students concerned might experience great pressure and not know how to react. The EdUHK believed that it was necessary to ascertain the identity of the persons involved, so as to provide counselling for the relevant students. On the other hand, as the act of posting such a banner appeared to violate the General Code of Student Conduct[1], and affected EdUHK's reputation, the EdUHK needed to identify the persons involved in order to conduct further investigation, and to consider disciplinary action.

The security centre of EdUHK ascertained from campus CCTV footage that the banner had been posted by two males. Two screenshots were made on a security officer's mobile phone and sent to a WhatsApp group ("the Group") that consisted of senior management of the EdUHK, for the purpose of timely identification of the persons involved. Some members of the Group also sought assistance, for the same purposes, of 13 other staff members and one student by forwarding the two screenshots to them.

Circulation of the screenshots was exempt under the Ordinance, but the EdUHK had not made risk assessment carefully or given warning to the recipients

Though the purpose of circulating the two screenshots through WhatsApp for disciplinary investigation was different from the original purpose of the installing of the CCTV, which was for security[2], as per section 58[3] of the Personal Data (Privacy) Ordinance, the personal data used for investigation and punishment of seriously improper conduct (not limited to crimes) was exempt from the provisions of Data Protection Principle ("DPP") 3. Hence, the PCPD takes the view that the EdUHK's viewing of CCTV footage, and the circulation of the two screenshots through WhatsApp for identification and disciplinary investigation, were for the purpose of protecting legitimate interests and there was no contravention of DPP[3].

(a) However, the PCPD considers that even though it was necessary for the EdUHK to circulate the two screenshots within the Group in a timely manner, it should have reminded the members of the Group that the screenshots were confidential information and they should not be forwarded to others, and the screenshots must be deleted immediately after use. Moreover, the EdUHK had not confirmed the identity of the suspects. It is obvious that the EdUHK had not been sufficiently vigilant at this instance, and hence members of the Group were not aware of the required protection of the screenshots.

Subsequently, the Group sent the screenshots to staff members outside the Group for their assistance in identifying the two males. The PCPD is of the view that the EdUHK should have carefully considered if it was necessary to send the screenshots to others, and whether those persons intended to receive the screenshots were trustworthy and would not leak the screenshots. Furthermore, the EdUHK should have reminded or warned those persons to keep the screenshots confidential, and of the liabilities of data leakage. The EdUHK paid no due attention to these matters and also let members of the Group distribute the screenshots to other persons of their own accord, substantially increasing the risk of data leakage. It should be noted that in these circumstances, once

the screenshots had been sent to persons outside the Group, the EdUHK could not effectively stop further distribution of the screenshots. The screenshots might have been widely distributed to hundreds of people within a few minutes.

In all the circumstances, EdUHK failed to take all reasonably practicable steps to safeguard the two persons' personal data, thereby contravening DPP 4 of the Ordinance.

Remedial actions taken by the EdUHK

The EdUHK took the PCPD's advice and has taken the following actions to enhance the protection of the CCTV images:
(i) set out in the Group that members are required to maintain confidentiality; before sending out messages or photos involving personal data, to carefully consider if it is necessary to send the messages or photos and if the recipients are trustworthy that they will not leak the messages or photos; give reminders or warnings to the recipients as to the liabilities of data leakage; obtain the permission of the President or other authorised staff members before forwarding the messages or photos; and make it clear to the recipients that they must also maintain confidentiality;
(ii) devise CCTV monitoring policies and procedures to ensure that matters such as the kinds of personal data held and the main purposes for which the data collected is to be used, as well as the retention policies are clearly set out and communicated internally, as well as to the data subjects (persons under the CCTV surveillance); and ensure compliance of the policies and procedures by relevant internal staff; and
(iii) devise detailed guidelines for the CCTV operating staff as to how the recorded CCTV images should be used, and for the relevant security measures.

Privacy is not an absolute right

Although this incident has triggered debate in society that includes issues of moral judgment and freedom of speech, this compliance check focused only on the protection of personal data, as PCPD's powers are limited as dictated by the Ordinance. The use of CCTV for monitoring is often controversial. It is, however, indisputable that in many circumstances, and in particular when there is a security need and for the purposes of the prevention and detection of crime, the use of CCTV is not only effective but is also necessary. In this regard, the PCPD has published the "Guidance on CCTV Surveillance and Use of Drones" to offer advice as to how to use CCTV responsibly from the perspective of personal data privacy protection.

The Privacy Commissioner for Personal Data, Hong Kong, Mr Stephen Kai-yi WONG stressed, "Everyone's **privacy is protected by the law as fundamental human right, but it is not an absolute right**. **A person offending the law or certain established regulation cannot take privacy as a "refuge" or "sanctuary" of his wrongdoings.** The degree of protection of personal data privacy under the Ordinance, varies from different people in different circumstances. For examples, in order **to promptly and effectively detect a crime, a seriously improper conduct, a dishonesty or a malpractice, and to timely apprehend, prosecute or detain an offender, the personal data privacy right of the offender will not override the interests of society at large**. **Part 8 of the Ordinance therefore has provided for exemptions for the use of personal data in the prevention and detection of such acts, so that offenders and persons who committed seriously improper conduct, dishonesty or malpractice cannot use the Ordinance as a "shield" to fence off investigation and punishment.**

This compliance check has, pursuant to the provisions of the Ordinance, shown the need for striking of a balance between the rights of the individual and the interests of society at large. On one hand, PCPD has taken into account protection of personal data privacy of individuals and, on the other, considered the relevant exemptions of the Ordinance and the interests of society. This is to ensure that the use of CCTV for the collection of evidence, or the prevention or punishment of seriously improper conduct will not be unduly compromised.

\- END -

[1] Section 1 of the Code stipulates that "Students are expected to uphold the image and the reputation of the University by behaving themselves in a disciplined and responsible manner".

[2] According to DPP3, the EdUHK must obtain the prescribed consent of the two persons before it can use their images for a "new purpose".

[3] Section 58(2) of the Ordinance stipulates that personal data is exempt from the provisions of DPP3 in any case in which: (a) the use of the data is for any of the purposes referred to in section 58(1) (e.g. the prevention and detection of crime; the prevention, preclusion or remedying (including punishment) of seriously improper or dishonesty or malpractice; the apprehension, prosecution or detention of offenders, etc.); and (b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in section 58(1).