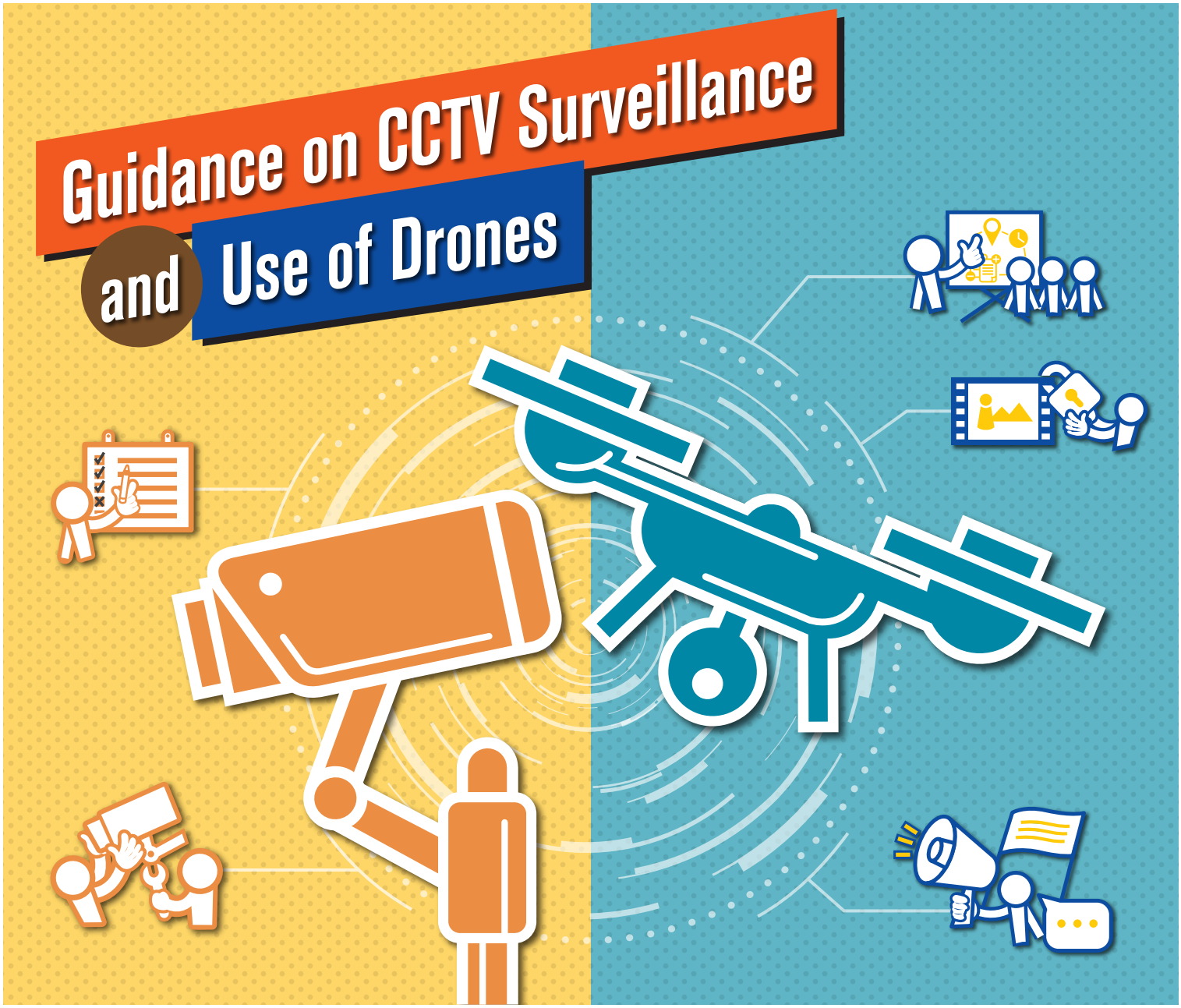
Guidance on CCTV Surveillance and Use of Drones



PCPD

HK

PCPD.org.hk

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

CCTV Surveillance

Before installing a CCTV system, a data user should take the following steps:

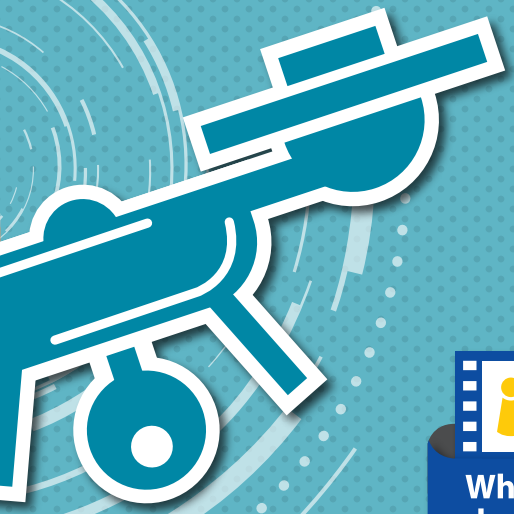
- Decide whether there is a pressing need to install a CCTV system;
- Find out whether there is any less privacy-intrusive alternative other than using a CCTV system;
- Establish the specific purpose of the use of the CCTV system;
- Find out the concerns of the people being affected and address them;
- Decide whether it is necessary to carry out CCTV surveillance covertly; and
- Determine the scope or extent of the surveillance.

When installing a CCTV system, a data user should ensure that …

- The cameras are not installed in places where people are expected to enjoy privacy, such as inside a changing room;
- The CCTV system is protected from vandalism or unlawful access;
- The people affected are explicitly informed that they are under CCTV surveillance, the purpose of surveillance and the means to raise an enquiry;
- The personal data collected by the CCTV system is deleted as soon as practicable when the purpose of the surveillance is completed; and
- The effectiveness of the safeguards and procedures for the CCTV system is regularly reviewed.

Use of Drones

Drones can perform as powerful surveillance tools when fitted with cameras. Users of drones, therefore, should be mindful of the need to respect others' personal data privacy. Be a responsible drone operator!



Before using a drone equipped with a camera, a data user should:

- Carefully plan the flight path to avoid flying close to other people or their properties;
- Pre-define what, where and when to conduct recording to avoid collection of unnecessary personal data; and
- Develop a data retention and destruction policy to erase irrelevant recording timely.

When using a drone equipped with a camera, a data user should:

- Encrypt the images transmitted wirelessly to avoid interception by unrelated parties;
- Implement access control to prevent the recording from falling into the wrong hands if the drone is lost;
- Inform affected people clearly of the operation of the drones by -
  - (i) Flashing lights to indicate that recording is taking place;
  - (ii) Making prior public announcement(s) to indicate the coverage of the upcoming the drone operations;
  - (iii) Putting corporate logo and contact details on the drone;
  - (iv) Having the crew members wear clothes with the same corporate identities; and
  - (v) Putting up big banners at "launch sites".

*For details, please refer to the content of *Guidance on CCTV Surveillance and Use of Drones*.

PCPD.org.hk

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **enquiry@pcpd.org.hk**

Disclaimer

The information and suggestions provided in this publication is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the "Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Commissioner under the Ordinance.

First published in July 2010
March 2015 (First Revision)
March 2017 (Second Revision)

Guidance on CCTV Surveillance and Use of Drones

Introduction

The use of CCTV[1] covering public places or common areas of buildings for security reasons or for monitoring illegal acts[2] (e.g. throwing objects from heights) has become increasingly widespread. Since CCTV may capture extensive images of individuals or information relating to individuals, its use should be properly controlled to avoid intrusion into the privacy of individuals.

This guidance note offers advice to data users (both organisational and individual data users) on determining whether CCTV should be used in given circumstances and how to use CCTV responsibly. Owing to the increased popularity of unmanned aircraft systems (more commonly known as "**Drones**") for use in photography, surveying and surveillance, the latter part of this guidance note also provides recommendations on the use of drones from the perspective of protecting personal data privacy.

Recommendations given in this guidance note are based on the key requirements under the Personal Data (Privacy) Ordinance (the "**Ordinance**") relating to the collection of personal data.

As regards the use of CCTV to monitor and record employees' activities at workplaces, more specific guidance can be found in *Privacy Guidelines: Monitoring and Personal Data Privacy at Work*[3] issued by the Privacy Commissioner for Personal Data, Hong Kong (the "**Commissioner**").

CCTV

Privacy Impact Assessment for CCTV Installation

Before using CCTV, data users should carry out a privacy impact assessment, taking into account at least the following factors:

- **Assessment** – Are the design and use of the CCTV system appropriate, necessary and proportionate for the given circumstances?
- **Alternatives** – Are there other less privacy-intrusive means than the use of CCTV to achieve the same objective?
- **Accountability** – Has the data user acted and been seen to have acted responsibly and transparently, in terms of its policy, controls, and compliance with the Ordinance, in the use of CCTV?

CCTV and the Ordinance

If a CCTV system does not have recording function (still pictures or video), its use will normally not involve collection of personal data as defined under the Ordinance, and is therefore not regulated under the Ordinance.

1 "Closed Circuit Television" – camera surveillance systems or other similar surveillance devices that are capable of capturing images of individuals.

2 Covert surveillance conducted by a law enforcement agency is regulated by the Interception of Communications and Surveillance Ordinance, Cap 589.

3 See www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf

On the other hand, whether the domestic or personal use of CCTV systems covering semi-public / public areas (such as surveillance cameras installed outside a residential unit or dash cams inside vehicles) is regulated by the Ordinance would depend on whether the purpose of the installation is to collect or compile information about identified persons.

If employers of domestic helpers use CCTV systems to monitor their helpers, they should read *Monitoring and Personal Data Privacy at Work: Points to Note for Employers of Domestic Helpers*[4] issued by the Commissioner.

Is It Necessary to Use CCTV?

Data Protection Principle ("DPP") 1(1) of the Ordinance requires that personal data shall only be collected where it is necessary for a lawful purpose directly related to the function or activity of the data user and that the data collected shall be adequate but not excessive.

In assessing whether it is necessary to use CCTV, the primary question to ask is –

"Is the use of CCTV in the circumstances of the case justified for the performance of the lawful function and activity of the data user and whether there are less privacy-intrusive alternatives?"

For example, the use of CCTV for deterring and detecting specific or repeated criminal activities like the throwing of corrosive liquid from heights would appear to be justifiable. In any case, for the purpose of crime prevention, due consideration should be given to the use of less privacy-intrusive arrangements or alternatives that could achieve the same purpose.

A data user should conduct an assessment objectively before installing CCTV to ensure that it is the right response to tackle the problem at hand (e.g. the throwing of objects from heights) and the degree of intrusion into privacy is proportionate to the severity of the problem. The following steps should be taken:

- Decide whether there is a pressing need to use CCTV (for example, if the use involves public interest or public safety);
- Find out whether there are other less privacy-intrusive options to better address the problem or that could be used together with CCTV to make it more effective or less privacy-intrusive;
- Establish the specific purpose of the use of CCTV and clearly identify the problem to be addressed. For example, a bank may want to use CCTV to deter thieves from robbing customers who use ATM machines to withdraw money, and the operator of a public open car park may want to use CCTV to monitor the safety of users and the security of vehicles parked;
- Collect relevant information to see whether CCTV will substantially solve the problem at hand. For example, if a property management company intends to use CCTV to tackle the problem of objects thrown from heights, records of similar incidents and the effectiveness of the use of CCTV to successfully prevent or detect the incident would be relevant;
- Assess whether there is genuine need for the use of high definition equipment to record detailed facial images of individuals. For example, detailed facial images are generally not required when CCTV is used for monitoring traffic flow or crowd movement;
- Any facial recognition system used in conjunction with CCTV must be supported by strong justification as the use of CCTV to enable automatic identification and tracking of individuals captured on CCTV footage is not normally expected by the public;
- Consult, where practicable, people who may be affected by the CCTV on what their concerns are, what steps may be taken to address these concerns and minimise the privacy intrusion;
- Covert CCTV surveillance should not be used without strong / overriding justification, and only as the last resort; and
- Clearly determine the scope or extent of monitoring. For example, it is not appropriate to use CCTV as a permanent measure when it was intended to address a temporary need.

[4] See www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/points_to_note_15102015_e.pdf

Positioning of CCTV Cameras and Notices

CCTV cameras should be positioned in a way that will not unnecessarily intrude into the privacy of individuals. No CCTV cameras should be installed in places where people have a reason to expect privacy (e.g. changing room). CCTV systems as a whole should be properly protected from vandalism or unlawful access.

People should be explicitly informed that they are subject to CCTV surveillance. An effective way is to put up conspicuous notices at the entrance to the monitored area and affix further notices inside the area as reinforcement. This is particularly important where the CCTV cameras themselves are very discreetly located, or located in places where people may not expect to be subject to surveillance (for example, in a taxi or a public light bus).

The notices should contain details of the data user operating the CCTV system, the specific purpose of surveillance and the person to whom matters relating to personal data privacy issues can be raised.

Proper Handling of the Recorded Images

DPP2(1) and **DPP2(2)** impose a duty on data users to ensure data accuracy and that there is no excessive retention of personal data.

The personal data collected should be deleted from the CCTV as soon as practicable once the purpose of collection is fulfilled. For instance, the recorded images captured by the CCTV installed for security purpose should be securely deleted regularly if no incident of security concern is discovered or reported.

If third party contractors are engaged in the provision and / or maintenance of CCTV, and have access to the CCTV images containing personal data, **DPP2(3)** requires that data users must adopt contractual or other means to ensure that personal data accessible by contractors is not kept longer than necessary. Depending on the particular situation, data users may need to work with their contractors to ensure that this principle is complied with. For example, contractors engaged to extract footage from the CCTV system to fulfil data access requests received by data users must be instructed not to keep the footage longer than necessary. Data users may refer to the Information Leaflet *Outsourcing the Processing of Personal Data to Data Processor*[5] published by the Commissioner for details.

DPP4(1) requires data users to take all reasonably practicable steps to ensure that the personal data held by them is protected against unauthorised or accidental access, processing, erasure, loss or use.

Security measures must be in place to prevent unauthorised access to the CCTV system including proper access control defining who can access the recorded images and under what circumstances.

Recorded images, whether stored locally in the CCTV or remotely in a computer, should be kept in safe custody. There must also be sufficient safeguards in place to protect the wireless transmission systems for images, if used, from interception. Access to places where the images recorded by the CCTV cameras are viewed, stored or handled should be secured and restricted to authorised persons only. Proper logs of which staff members in custody of the recorded images should be updated on time. Transfers and movements of the recorded images should also be clearly documented.

Once there is no valid reason to retain the recorded images, they should be securely deleted.

If a data user engages contractors that would have access to the recorded images, **DPP4(2)** requires that the data user must adopt contractual or other means to ensure that there is no diminution in protection for the personal data accessible by contractors[6].

Transfer of CCTV Records to Third Parties

On the use of personal data, **DPP3** stipulates that personal data shall only be used for the purposes for which it was collected or a directly related purpose. Unless the data subject gives prescribed consent (which means express consent given voluntarily) or if any applicable exemptions under the Ordinance apply, personal data should not be used for a new purpose.

5 See www.pcpd.org.hk/english/resources_centre/publications/files/dataprocessors_e.pdf

6 See footnote 5

When a data user (e.g. building management company) is asked to provide copies of CCTV records to a law enforcement agency (e.g. the police) for criminal investigation purpose, the exemption provided under section 58(2) of the Ordinance[7] may apply. The data user, however, is under no general obligation to supply the personal data as requested. Before the exemption is invoked, the data user must be reasonably satisfied that failure to supply the data would likely prejudice the investigation.

Transparency of Policy and Practice

DPP5 requires data users to make generally available their privacy policy and practice.

To meet this requirement, data users should devise CCTV monitoring policies and / or procedures to ensure that matters such as the kinds of personal data held, the main purposes for which the data collected is to be used and the retention policies are clearly set out and communicated internally and to the data subjects.

It is also important for data users to establish who has the responsibility to operate the CCTV system and control the zoom-in functions (if any), and to decide what is to be recorded, how the recorded images should be used, how the recording media is to be disposed of after use and to whom the recorded images may be disclosed.

The above policies or procedures should be communicated to and followed by the relevant staff members. Staff who operate the systems or use the images should be trained to comply with the policies and procedures. Adequate supervision should also be in place. Misuse or abuse of the CCTV system or the recorded images should be reported to a senior staff member so that appropriate follow up actions, including disciplinary actions, can be taken.

Regular Reviews

Compliance checks and audits have to be carried out regularly by the data users to review the effectiveness of the safeguards and procedures for the CCTV system.

The justifications for the continued use of CCTV systems should be reviewed regularly to ensure that they are serving the purpose for which they were first installed. If such reviews indicate that the use of the CCTV is no longer relevant or necessary, or if less privacy-intrusive alternatives can be used to achieve the same purpose, the data user should cease using the CCTV.

Drones

There is no universally accepted definition for drones but typically they cover aircrafts that are either controlled autonomously by computers or by remote pilots.

Drones can be used in many ways that bring about great social and economic benefits, such as land surveying, predicting weather patterns, fighting fires, as well as search and rescue operations. They are also increasingly used in commercial operations (such as shooting advertisement, TV and movie production); and for hobby or recreational purposes.

The use of certain types of drones may be subject to regulation (including the need for a permit) by the Civil Aviation Department[8] and, if the remote control equipment is modified to extend its control range, the Office of the Communications Authority[9] in Hong Kong.

Privacy intrusiveness of Drones

Drones can perform as powerful surveillance tools when fitted with cameras. The threats they pose to privacy are consistent with the use of CCTV. Hence the above guidelines for CCTV apply equally to the use of drones fitted with cameras.

Furthermore, drones can be far more privacy-intrusive than CCTV in view of their unique attributes:

- Being small, portable, mobile and cheap, they can track an individual's activities more persistently over time and in places that are not expected while covering a wider area;

7 A data user may rely on the exemption under section 58(2) of the Ordinance to exempt from the provisions of DPP3 the use of personal data for the prevention or detection of crime.

8 See www.cad.gov.hk/english/Unmanned_Aircraft_Systems.html

9 See www.ofca.gov.hk

- They are a relatively covert form of surveillance as they are mobile and in practical terms, it is difficult for the public to know who the operators are; and
- When equipped with a full range of advanced surveillance technologies such as telephoto lens and infrared sensors, they would acquire sophisticated abilities such as capturing data from distances and through objects, and with a fine level of detail.

To eliminate or reduce the harmful effects of these highly privacy-intrusive features, users of drones should be particularly mindful of the need to respect people's privacy. Public perception and the reasonable privacy expectations of affected individuals should be ascertained. The alternative use of less privacy-intrusive means of collection and use of personal data should be seriously considered. The intrusion on privacy can only be justified if it is proportional to the benefit to be derived, or else it could amount to unfair collection of personal data under **DPP1(2)**.

Suggestions on Responsible Use

Some tips on the responsible use of drones are as follows:-

Flight path – Flight paths should be carefully planned so as to avoid flying close to other people or their properties. For example, drones should be launched from a location as close as possible to the area they need to cover.

Recording and retention – If recording is intended, the recording criteria (what, where and when to record) should be pre-defined to avoid over-collection of information, some of which may be related to individuals. Drones may go off course by accident and record scenes unintentionally. A policy to erase irrelevant recording and a data retention policy should be developed.

Security – If images are transmitted through wireless means, encryption should be considered to avoid the adverse consequences of interception by unrelated parties. If the drone has a recording function, access control should be considered to prevent the recording from falling into the wrong hands in the event the drones are accidentally lost.

Notice – Being transparent about the operation of the drone is important to building trust with those affected by its operations. Informing them clearly of your purposes and operation details is the best first step to assure them that you have nothing to hide and are not covertly monitoring anyone. However, this often poses the greatest challenge and innovative approaches may be called for, such as:-

- flashing lights may be used to indicate that recording is taking place;
- pre-announcing drone operations in the affected area by social media;
- putting corporate logo and contact details on drones;
- having crew members wear clothes with the same corporate identities; and
- putting up big banners with privacy notices and contact details at "launch sites".

PCPD.org.hk

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **enquiry@pcpd.org.hk**

Disclaimer

The information and suggestions provided in this publication is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the "Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Commissioner under the Ordinance.

First published in July 2010
March 2015 (First Revision)
March 2017 (Second Revision)