

Shinnyo-en UK CCTV Policy

1. Introduction

1.1 This policy is to control the management, operation, use and confidentiality of the Closed Circuit Television (“**CCTV**”) system at Shinnyo-en UK (“**Shinnyo-en**”, “**we**” or “**us**”), address registered to the Manor House, Woodstock, Lane North, Long Ditton, Surry KT6 5HL, United Kingdom - as data controller.

1.2 The system comprises of a fixed number of cameras that are necessary for security. All the cameras are owned by Shinnyo-en UK, and are installed on the exterior and the interior of the temple of Shinnyo-en UK. The cameras are in operation 24 hours a day, 7 days a week and they are monitored from a secured (CCTV) Control Room.

1.3 The images of all CCTV images are saved on hard drives (“**HDDs**”) for a certain period (as further explained below in the “Retention Period” section).

1.4 We are aware that images of recognizable individuals, such as temple staff and visitors of the temple (“**data subjects**”), captured by our CCTV system constitute “personal data” under the definition of personal data as defined in Article 4 (1) of the General Data Protection Regulation (GDPR).

1.5 We voluntarily follow the Home Secretary’s Surveillance Camera Code of Practice (the “SC Code”), and its 12 guiding principles, which if followed will ensure that surveillance camera systems are only operated proportionately, transparently and effectively, even though the SC Code only applies to the overt use of surveillance camera systems that are operated by relevant authorities (police forces, local authorities and parish councils).

1.6 This document has been drafted in accordance with the Information Commissioner’s Office (ICO) CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice. Copies of these codes can be found at www.ico.org.uk and <https://www.gov.uk/government/publications/surveillance-camera-code-of-practice> respectively.

1.7 The purpose of this document is to set out how the CCTV system will be managed and used by Shinnyo-en and to inform individuals whose personal data may be captured on the CCTV system about how and why that personal data may be processed by Shinnyo-en.

1.8 The use of the CCTV system is overseen by our Data Protection Manager (DPO) who can be contacted at dpo.gdpr@shinnyo.org.

2. Objectives of the scheme

2.1 The objectives of the CCTV system are:

- (a) To protect the building and its assets
- (b) To increase personal safety of our staff and visitors to our temple and reduce the fear of crime
- (c) To support our health and safety measures
- (d) To support the police in a bid to deter and detect crimes
- (e) For evidence in any civil or criminal legal proceedings
- (f) To protect members of the public and private property
- (g) To assist in managing the temple, in particular to dealing with any questions, complaints or enquiries.

2.2 The legal basis for Shinnyo-en's use of any personal data which is captured by the CCTV system is that the processing is necessary for the legitimate interests set out in this paragraph (provided that those interests are not overridden by individuals' rights and interests). Shinnyo-en may also need to use this personal data in order to establish, exercise or defend against legal claims.

3. Operation of the CCTV system

3.1 Staff members have been instructed that static cameras are to focus on our property only and not areas open to the general public outside our premises, third parties' private homes, gardens and other areas of private property.

3.2 Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorization.

3.3 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. HDDs will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. HDDs will never be released to the media for purposes of entertainment.

3.4 The planning and design has endeavored to ensure that the scheme will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3.5 Warning signs have been placed prominently around our premises to inform staff and visitors that CCTV cameras are in operation and who to contact for further information.

3.6 Access to the CCTV Control Room is strictly limited to persons with the correct access control privilege, which is primarily limited to security staff. A record is kept of all the individuals who are given access to the Control Room.

3.7 We have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. This includes the fact that the CCTV hard drives are located in a secured server room and access to this room is only via a formal approval process. Password protection, technical access control and the use of encryption are also technical protection measures that we use.

3.8 We have put in place procedures to deal with any suspected personal data breach and will notify any affected individuals and/or the ICO where appropriate.

3.9 The CCTV system will be regularly maintained in accordance with the manufacturer's instructions.

3.10 HDDs may be viewed by the police for the prevention and detection of crime.

4. Retention period

The images captured by the CCTV System on the HDDs will not be stored for any longer than is required in order to achieve the purposes identified in paragraph 2 above. HDDs are usually deleted after 10 days on a rolling-basis. Only in cases of incidents or in connection with claims including a request by a data subject made under the GDPR, the HDDs may be kept for as long as needed for the investigation or claim.

5. Sharing of your data

5.1 We share your personal information with the following parties:

(a) Suppliers, service providers and advisors to us: to manage and operate the CCTV system as our data processor and also organizations that provide us with legal, property and insurance advice.

(b) The police and other law enforcement agencies: to carry out policing, assist investigations, trace missing people and investigate alleged criminal activities.

(c) The security services: where relevant for matters of national security.

(d) Individuals who have been injured, attacked or had property damaged or stolen and their insurance providers: to assist them with any criminal or civil investigations or legal proceedings.

(e) Any relevant regulators: where we are required to do so by law or to assist with their investigations or initiatives.

5.2 We do not disclose personal information to anyone else except as set out above unless we have your consent or we are legally obliged to do so. We do not sell your data.

6. International transfer of your personal information

The personal information we collect about you is not transferred to or stored in countries outside of the UK or European Union.

7. Your rights

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data

(please note, however, that after deletion of the relevant HDDs in line with our retention policy as set forth above, you as data subject may only get access to that very information that the material has been deleted):

- The right to request a copy of your personal data which Shinnyo-en holds about you (please note, however, that if other data subjects can be identified in the same material then that part of the material will be anonymized (for example by blurring the copy or parts thereof) before giving you a copy in connection with your request);
- The right to request that the Shinnyo-en corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for Shinnyo-en to retain such data;
- The right to withdraw your consent to the processing at any time;
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller (known as the right to data portability), where applicable;
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, where applicable; and
- The right to lodge a complaint with the supervisory authority in your country of with the lead supervisory authority for us.

Usually, you will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further

information in relation to your request to speed up our response.

We try to respond to all legitimate requests without undue delay, usually within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

8. Your questions and complaints / contacting us

For any questions you may have regarding this CCTV Policy and our processing of your personal data, please do not hesitate to contact us by email: privacy.uk@shinnyo.org. You may also contact our data protection officer (DPO) by email: dpo.gdpr@shinnyo.org. If at any time you have any concerns about the way your data has been processed by us and those concerns cannot be resolved by us directly, you have the right to take those concerns externally and raise them with the relevant data protection authority.

9. Changes to this Policy

We may update this CCTV Privacy Policy from time to time. You are encouraged to regularly check for any updated versions of this document.