THE BRIDGE CCTV POLICY - JANUARY 2023

The Bridge has had a new CCTV system in place from October 2022 and its usage will adopt the Home Office 'Surveillance Camera Code of Practice' issued in June 2013.

The Bridge has agreed to abide by the following 12 'Guiding Principles' from the Code of Practice:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

The legitimate aim is to protect The Bridge, its premises and users from anti-social behaviour, vandalism, criminal damage, the threat of violence and any other potential problem Bridge/its users may encounter.

With regard to children on The Bridge's premises, the presence of CCTV should assist with regard to their safety should there be intruders onto the premises. CCTV cameras will provide a visual record should there be any such intruders or any other threat to a child's welfare whilst on The Bridge's premises.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

Annual reviews of the Data Impact Assessment will be undertaken to ensure that the CCTV system remains justified in its use.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

Signage informing the Centre's users is prominently placed for internal and external viewing. The contact person is Ruth Cracknell (The Bridge's Operations Manager) who can be contacted on ruth@thebridgese10.co.uk/ 07748 270501.

4. There must be clear responsibility and accountability for all surveillance

camera system activities including images and information collected, held and used.

The only person authorised by The Bridge to operate the CCTV system is the Bridge's Operations Manager, who is the designated 'responsible person'. Images will only be stored on the CCTV's system hard drive for up to a period of 30 days. Only the Police will have the right to save images from the hard drive to a computer, other than in exceptional circumstances where images are needed for investigation purposes or for saving before onward transmission, or potential onwards transmission, to the police. In such instances the responsible person will save them to the Operations Manager's work laptop and will ensure they are saved securely and only accessible by the responsible person, who will delete them as soon as is reasonably practicable once the purpose for saving the images has been discharged.

From time to time as may be necessary, the CCTV installation company may access footage (only with the responsible person's permission) purely for the purposes of carrying out maintenance of the CCTV system.

The limiting of access in this way should prevent unauthorised access to the images.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

Signage is in prominent positions in The Bridge's premises. The Bridge's CCTV Policy is available upon request.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

The CCTV hard drive is an automatic overwrite system with approximately 30 days storage capacity.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only

take place when it is necessary for such a purpose or for law enforcement purposes.

Access to the CCTV recording system's hard drive is limited to: (i) the responsible person; (ii) the Police if so requested by them; and (iii) by the CCTV installation company for the purposes of maintenance and repairs only. With regard to (i), the hard drive is only accessed by the responsible person for the purposes of assessing and identifying (confirmed or suspected) health and safety issues and unlawful acts. Unlawful acts /suspected unlawful acts may be reported to the Police.

With regard to requests for access to footage under relevant Data Protection legislation, The Bridge confirms that (unless an exemption applies) it will provide access to footage (i.e. footage that has yet to be deleted by the CCTV system's overwrite function as specified above) if the request is made by:

1) a person who seeks access to footage of themselves; or
2) a parent/guardian making a request on behalf of a child where they have a right under the relevant legislation to make a request on behalf of the child in question.

Granting access may be effected by allowing the requesting person to view footage or sending them a copy of the footage, depending on practicalities.

When providing access, attempts will be made to redact (by 'blurring out') third parties in the footage (other than the person requesting the footage/the child on whose behalf an adult is requesting access to footage of the child) where possible.

If it is not possible to carry out redaction as specified above, The Bridge will give consideration to asking any third parties in the footage (or their parent/guardian etc\ for consent to the footage containing their images to be released, but this may not be practicable.

Where it is not possible or appropriate to redact /obtain consent from the third parties that appear in the relevant footage, The Bridge will balance the requesting person's rights against the third party's rights and decide if it is reasonable to share the footage without the consent of the third party, and will documents its decision in writing.

8. Surveillance camera system operators should consider any approved

operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

The Bridge follows the Home Office Surveillance Camera Code of Practice. The responsible person will be kept up to date with any training or standards relevant to the operation of the CCTV system.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

The CCTV's hard drive system is password protected and knowledge and use of the password is restricted to the responsible person. As above, images may be viewed by the police and the CCTV installation company as necessary.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

An annual review of the usage of the CCTV system will be carried out by The Bridge to ensure compliance to the above principle.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

Issues arising from the stated aims for the CCTV system may be reported to the Police.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

No images will be stored by or on equipment operated by The Bridge other than the limited capacity hard drive of the CCTC system as set out above.

<u>COMPLAINTS</u>

All complaints regarding the use of CCTV at The Bridge should be put in writing to Ruth Cracknell, The Bridge's Operations Manager, on the email address set out at point 3 above.

PRIVACY POLICY

This policy operates within a broader Privacy Policy, details of which are displayed on The Bridge's internal notice board.