CCTV Policy v1.0

1 Definitions

- The term ‘hackspace’ refers to Cheltenham Hackspace Ltd.
- Directors refers to the current active directors of Cheltenham Hackspace Ltd.

2 Introduction

The hackspace uses closed circuit television (CCTV) images to protect the hackspace’s property and to provide a safe and secure environment for members and visitors to the hackspace’s premises. This policy sets out the details of how the hackspace will collect, use and store CCTV images.

The hackspace’s CCTV facility will only record images. There is no audio recording i.e. conversations are not recorded on CCTV.

3 Purposes of CCTV

The hackspace has carried out a data protection impact assessment and on the basis of its findings it considers it necessary and proportionate to install and use a CCTV system. The data collected from the system will assist in:

- Prevention or detection of crime or equivalent malpractice.
- Identification and prosecution of offenders.
- Monitoring of the security of the hackspace.
- Ensuring that health and safety rules and hackspace procedures are being complied with.

4 Location of Cameras

Cameras are located at strategic points throughout the hackspace’s premises, principally to view the entrance/exit points and main rooms. The hackspace has positioned the cameras so that they only cover communal or public areas on the hackspace’s premises where there are no legitimate expectations of privacy and sited so that they provide clear images. No camera focuses, or will focus, on private areas such as the onsite toilets.

All cameras are also clearly visible.

Appropriate signs are prominently displayed so that members, the public and other visitors are aware they are entering an area covered by CCTV.

5 Recording and Retention of Images

Images produced by the CCTV equipment are intended to be as clear as possible so that they are effective for the purposes set out above. Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly and that the media is producing high-quality images.

Images may be recorded either in constant real-time (24 hours a day throughout the year) or only at certain times, as the needs of the business dictate.

As the recording system records digital images, any CCTV images that are held on the hard drive of a PC or server are deleted and overwritten on a recycling basis and, in any event, once the hard drive has reached the end of its use, it will be erased before disposal.

Images which are stored digitally are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be 12 months. However, where a law enforcement agency is investigating a crime, images may need to be retained for a longer period.

6 Access to and Disclosure of Images

Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected.

- The images that are filmed are recorded centrally and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system and to those members who are authorised to view them in accordance with the purposes of the system.
- Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:
- The police and other law enforcement agencies, where the images are recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.
- Prosecution agencies, such as the Crown Prosecution Service.
- Relevant legal representatives.
- Directors of the hackspace in regards to dispute resolution or investigation of rules and code of conduct breaches.
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

The directors of the hackspace (or another designated member acting in their absence) are the only people who are permitted to authorise disclosure of images to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

7 Individuals' Access Rights

Under the UK's data protection laws, including the General Data Protection Regulation (GDPR), individuals have the right on request to receive a copy of the personal data that the hackspace holds about them, including CCTV images if they are recognisable from the image.

If you wish to access any CCTV images relating to you, you must make a written request to the hackspace's directors. This can be done by using the address found on our privacy page. The hackspace will usually not make a charge for such a request, but we may charge a reasonable fee if you make a request which is manifestly unfounded, excessive, or is repetitive. Your request must include the date and approximate time when the images were recorded and the location of the particular CCTV camera, so that the images can be easily located and your identity can be established as the person in the images.

The hackspace will usually respond promptly and in any case within one month of receiving a request. However, where a request is complex or numerous the hackspace may extend the one month to respond by a further two months.

The hackspace will always check the identity of the person making the request before processing it.

The directors will always determine whether disclosure of your images will reveal third-party information, as you have no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.

If the hackspace is unable to comply with your request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, you will be advised accordingly.

9 Covert Recording

Covert recording is specifically barred by the hackspace and its directors. If you suspect that covert recording is occurring within the hackspace then please contact the directors.

10 Staff Access

The hackspace will ensure that only the designated data owner will have access to the images. Nobody else will be permitted to access the system.

11 Data Protection

The hackspace will process the personal data collected in connection with the operation of the CCTV policy in accordance with its data protection policy and any internal privacy notices in force at the relevant time. Inappropriate access or disclosure of this data will

constitute a data breach and should be reported immediately to the directors in accordance with the hackspace's data protection policy.

POLICY UPDATED	25 March 2026 approved by the Directors
CHANGES	- Initial version
REVIEW DATE	2 years after date of policy