

CCTV Policy (Online Version)

I believe that CCTV plays a legitimate role in helping to maintain a safe and secure environment for my sites. Images recorded by CCTV are Personal Data and as such will be processed in accordance with data protection laws. I am committed to complying with my legal obligations in order to appropriately handle and protect Personal Data and ensure that the legal rights of individuals relating to their Personal Data, are recognised and respected.

This policy is intended to enable individuals to understand how James Carnochan t/a Computer Fixer & Alpha.ICT uses CCTV and the rights individuals may have in relation to CCTV, who has access to CCTV images and how individuals can raise any queries or concerns they may have.

1. Definitions

For the purposes of this policy, the following terms have the following meanings:

CCTV: means cameras, devices or systems including fixed CCTV and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

CCTV Data: means any Data in respect of CCTV, e.g. video images, static pictures, etc.

Data: means any information which is stored electronically or in paper-based filing systems.

Data Subject: means any individuals who can be identified directly or indirectly from CCTV Data (or other Data in my possession). Data Subjects include staff, guests, customers, and potential customers, suppliers and contractors, and members of the public.

Data Controller: is the organisation or authority which, determines how and for what purpose the Personal Data are processed. When operating CCTV, James Carnochan is the relevant Data Controller and is responsible for ensuring compliance with the Data Protection Laws.

CCTV users: are those of my employees (or employees of any Data Processors which I appoint) whose work involves processing CCTV Data. This will include those whose duties are to operate CCTV to record, monitor, store, retrieve and delete images. Data users must protect the CCTV Data they handle in accordance with this policy.

Service Provider: is any organisation that is not a CCTV user (or other employee of a Data Controller) that processes CCTV Data or Personal Data on my behalf and in accordance with my instructions.

Data Protection Laws: means: a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (the "GDPR") and any equivalent or implementing legislation;

b) all other applicable laws, regulations or court judgements relating to the processing of personal data, data privacy, electronic communications, marketing and/or data security; and

c) any and all legally binding guidelines, recommendations, best practice, opinions, directions, decisions, or codes issued, adopted or approved by the European Commission, the Article 29 Working Party, the European Data Protection Board, the UK's Information Commissioner's Office and/or any other supervisory authority or data protection authority from time to time in relation to the processing of personal data, data privacy, electronic communications, marketing and/or data security;

in each case as from time to time in force and as from time to time amended, extended, consolidated, re-enacted, replaced, superseded or in any other way incorporated into law and all orders, regulations, statutes, instruments and/or other subordinate legislation (including the Data Protection Bill 2017 when in force) made under any of the above in any jurisdiction from time to time.

Processing: is any activity which involves the use of CCTV Data, whether or not by automated means. It includes collecting, obtaining, recording or holding CCTV Data, or carrying out any operation or set of operations on the CCTV Data including organising, structuring, amending, retrieving, using, disclosing or erasing or destroying it. Processing also includes transferring CCTV Data to third parties.

Sites: means the premises at his home address and shop address.

2. About this policy

2.1: I currently use CCTV to view and record individuals at my Sites, 24 hours per day, 7 days per week. This policy sets out why I use CCTV, how I will use CCTV and how I will process any CCTV Data recorded by CCTV to ensure that I am compliant with Data Protection Law.

2.2: The images of individuals recorded by CCTV are Personal Data and therefore subject to the Data Protection Laws. James Carnochan is the Data Controller of all CCTV Data captured at both Sites.

2.3: This policy covers all staff, guests, customers, and potential customers, suppliers and contractors and may also be relevant to members of the public in the direct vicinity of the Sites.

3. Responsible Person

James Carnochan has overall responsibility for ensuring compliance with Data Protection Laws and the effective operation of this policy as well as the day-to-day operational responsibility for CCTV and the storage of CCTV Data recorded.

4. Why CCTV is used

4.1: I currently use CCTV around my Sites as outlined. I believe that such use is necessary for the following legitimate purposes:

(a) to prevent or detect crime and protect buildings and assets from damage, disruption, theft, vandalism and other crime;

(b) for the personal safety of staff, guests, customers, and potential customers, suppliers and contractors and other members of the public and to act as a deterrent against crime; and

(c) to support law enforcement bodies in the prevention, detection and prosecution of crime.

5. Monitoring

5.1: The locations of the CCTV are chosen to minimise the viewing of spaces/individuals which are not relevant to the legitimate purpose of the monitoring as specified above.

5.2: Currently, 1 of my cameras records sound, namely the front garden camera located at my home address, and none of the other CCTV cameras records sound.

5.3: A live feed from the CCTV is not monitored continuously and images are only revisited in the event of an incident or if a request is made.

6. How CCTV is operated

Where CCTV is in use at my Sites, I will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. The signs will contain details of the CCTV operator if it is not already obvious (such as cameras attached to the side wall of any of my sites) and who to contact for further information.

I will ensure that feeds from the CCTV are only viewed by appropriately authorised persons for legitimate purposes.

7. How the Data will be used

7.1: In order to ensure that the rights of individuals recorded by my CCTV are protected, I will ensure that CCTV Data gathered from such systems is stored in a way that maintains its integrity and security. This may include encrypting the Data, where it is possible to do so.

7.2: I will ensure that any CCTV Data is only used for the purposes specified in section 4.1 above. I will not use CCTV Data for another purpose unless permitted by Data Protection Laws.

8. Retention and erasure of Data

8.1: Data recorded by my CCTV systems will be stored locally on servers at my Sites. I will not retain this Data indefinitely but will permanently delete it once there is no reason to retain the recorded information. Exactly how long the Data will be retained for will vary according to the purpose for which it was recorded. For example, where images are being recorded for crime prevention purposes, CCTV Data will be kept only for as long as it takes to establish that a crime has been committed. In all other cases, recorded images will be kept for no longer than 14 days before being overwritten and permanently deleted.

8.2: At the end of its useful life and in any event within 7 years all Data stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs or hard copy photographs will be promptly disposed of as confidential waste.

9 Ongoing review of the use of CCTV

9.1: I will periodically review my ongoing use of existing CCTV at my Sites to ensure that its use remains necessary and appropriate and in compliance with Data Protection Laws.

10. Rights of Data Subjects

10.1 As CCTV Data will identify individuals, it will be considered Personal Data under applicable Data Protection Laws. Under Data Protection Laws, Data Subjects have certain rights in relation to the Personal Data concerning them. These are as follows:

(a) the right to access a copy of that Personal Data and the following information (this may include CCTV Data captured by my CCTV):

(i) the purpose of the processing;

(ii) the types of Personal Data concerned;

(iii) to whom the Personal Data has or will be disclosed; and

(iv) the envisaged period that the Personal Data will be stored, or if not possible, the criteria used to decide that period;

(b) the right to request any inaccurate Personal Data that I hold concerning them is rectified, this includes having incomplete Personal Data completed;

- (c) the right to request the Personal Data I hold concerning them is erased without undue delay, where it is no longer necessary for me to retain it in relation to the purposes it was collected;
- (d) the right to request restriction of my processing of Personal Data in certain circumstances; and
- (e) the right to lodge a complaint with the Information Commissioner's Office, if the Data Subject considers that my processing of the Personal Data relating to him or her infringes Data Protection Laws.

11. Requests of disclosure by third parties

12.1: No images from my CCTV cameras will be disclosed to any third party except in instances permitted by Data Protection Laws.

12.2: In other appropriate circumstances, I may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

13. Complaints

13.1: If any individual has questions about this policy or any concerns about my CCTV systems, then they should speak to James Carnochan in the first instance.