



CCTV Policy

Company Policy No: 57
Company: Nutrix Personnel Ltd
Issue No: 6
Revision Date: April 2026
Review Date: April 2027

CCTV Policy

1 Purpose and scope

- 1.1 Nutrix Personnel Ltd use closed circuit television (CCTV) to provide a safe and secure environment for staff, visitors and customers, and to protect company property. This policy relates to the use and management of CCTV throughout our premises. As a controller, we have registered our use of CCTV with the Information Commissioner's Office (ICO) and seek to comply with its best practice suggestions.
- 1.2 This policy sets out the accepted use of the CCTV equipment and images to ensure compliance with relevant data protection and privacy laws including: Retained Regulation (EU) 2016/679, the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) (together referred to as the 'Data Protection Legislation'), and related laws including but not limited to, the Human Rights Act 1998 (all referred to collectively in this policy as the CCTV Laws).
- 1.3 This policy has been produced in line with the ICO CCTV Code of Practice. This policy should be read alongside our *Data Protection Policy*.
- 1.4 This policy does not form part of any contract of employment or other contract to provide services. We reserve the right to change this policy at any time, and any such changes will be notified to staff, visitors and customers.

2 Your responsibility to comply with this policy

- 2.1 Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to the HR department.
- 2.2 All staff including but not limited to employees, workers, contractors, self-employed consultants and agency workers must comply with this policy and any document referenced in it. We take compliance with this policy very seriously. Failure to comply with the policy puts at risk the individuals whose personal information is being processed, carries the risk of significant civil and criminal sanctions for the individual and for us, and may, in some circumstances, amount to a criminal offence by the individual.
- 2.3 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. Non-employees, such as contract staff and consultants, may have their contract terminated with immediate effect.

3 Definitions

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

CCTV: means fixed and domed cameras designed to capture and record images of individuals and property.

Controllers: are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure

compliance with the law. We are the controller of all personal data used in our business for our own commercial purposes.

Data: is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data subjects: means all living individuals about whom we hold personal information as a result of the operation of our CCTV (or other surveillance systems).

Data users: are those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy.

Personal data: means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

Processing: is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

Processors: are any person or organisation that is not a data user (or other employee of a controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

Surveillance systems: means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

4 Data transfer

- 4.1 We do not allow personal data to be transferred to a person or entity (whether a group company or a third party) located outside the UK or to an international organisation without the prior written approval of a Director or the business of the Head of the IT department. We may transfer personal information outside the UK or to an international organisation only on the basis that that country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules or standard data protection clauses OR of compliance with an approved code of conduct.

5 Why we use CCTV

- 5.1 We have considered and determined that the purposes for which the CCTV is deployed are legitimate, reasonable, appropriate and proportionate. For ease of reference, CCTV systems are deployed at our premises for the following purposes and on the legal basis set out in our *Data Protection Policy*. We have installed CCTV systems to:

- 5.1.1 deter crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- 5.1.2 for the personal safety of staff, visitors and other members of the public and to act as a deterrent against crime;
- 5.1.3 to assist in the effective resolution of disputes which arise in the course of serious breaches of policies and procedures, disciplinary or grievance procedures;
- 5.1.4 assist law enforcement bodies with the identification, apprehension and prosecution of crime; and
- 5.1.5 to assist in day-to-day management, including ensuring the health and safety of staff and others.

5.2 The CCTV system will NOT be used:

- 5.2.1 to record sound unless in accordance with the policy on covert recording (see **Error! Reference source not found.** below);
- 5.2.2 for any automated decision taking; or
- 5.2.3 monitoring private and/or residential areas or premises.

5.3 Before installing and using CCTV systems on our premises, we have:

- 5.3.1 assessed and documented the appropriateness of and reasons for using CCTV;
- 5.3.2 established and documented who is responsible for day-to-day compliance with this policy; and
- 5.3.3 ensured signage is displayed to inform individuals that CCTV is in operation, and that CCTV operations are covered in appropriate policies.

5.4 We keep a record of the CCTV installed and used.

5.5 Once installed, reviews will be regularly undertaken to ensure that the use of the CCTV systems and the processing of the personal data obtained through it remains justified.

5.6 We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters. Recorded images will only be viewed in designated, secure offices.

5.7 We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

6 Positioning cameras

6.1 We will make every effort to position cameras to ensure they only cover our premises. As far as practically possible, cameras will not focus on residential or private accommodation or property.

Camera operators will receive training and access to written procedures for maintaining and respecting the privacy of neighbours (business and residential), staff and customers, and to ensure they understand and observe the legal requirements related to the processing of relevant data.

- 6.2 With the exception of covert monitoring, cameras will not be hidden from view and must be sited in such a way as to ensure that they only monitor spaces intended to be covered.
- 6.3 The installation of cameras in areas in which individuals would have an expectation of privacy will not be authorised under this policy, unless there are exceptional circumstances, and subject to approval by the Head of IT OR the Head of HR.
- 6.4 We will clearly display signs at the entrance of the surveillance zone so that staff, visitors and customers/clients are aware they are entering an area covered by CCTV.
- 6.5 Our CCTV signs will state that CCTV is in operation. The signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.
- 6.6 If neighbouring domestic areas are included in the camera view, the occupants of the property will be consulted prior to any recording and the purposes of the recording explained. We will take reasonable steps to minimise the impact of recording.

7 Image quality

- 7.1 Images produced by the equipment must be as clear as possible so that they are effective. To achieve this:
 - 7.1.1 the equipment be properly installed, serviced, checked and maintained (and maintenance logs maintained) to ensure it works properly;
 - 7.1.2 any recording media, if needed, will be of good quality and will be replaced if the quality of the images has begun to deteriorate;
 - 7.1.3 where time/date of images are recordable the equipment will be set accurately and this will be regularly checked and documented;
 - 7.1.4 cameras will be correctly positioned;
 - 7.1.5 assessments will be made as to whether constant real-time recording is necessary, or if recording can be limited to those times when suspect activity is likely to occur;
 - 7.1.6 cameras will be protected from vandalism so far as is possible; and
 - 7.1.7 if cameras break down or are damaged, the *IT department* is responsible for arranging timely repair.

8 Data and image retention and erasure

- 8.1 Images and recording logs must be retained and disposed of in accordance with the Data Protection Policy. Images stored on removable media will similarly be erased or destroyed once the purpose of the recording is no longer relevant. Data will only be retained for legal and/or compliance reasons in accordance with the relevant retention and disposal of data policies.
- 8.2 For digital recording systems, CCTV images held on the hard drive of a PC or server will be permanently overwritten on a recycling basis once the drive is full, and unless authorised by **HR** will not be held for more than 30 days. If images are retained longer than this, the reason(s) will be recorded in the CCTV register.
- 8.3 In all other cases, recorded images will be kept for no longer than 90 days.
- 8.4 Where a request to retain information is authorised, reasonable steps will be taken to safeguard any footage which may otherwise be deleted.
- 8.5 All digital recordings will be placed on a separate standalone server which is password protected to maintain security. Access to digital recordings is restricted to the Head of the IT department and the HR Department. Recording media no longer in use will be permanently and securely destroyed. Where images have been authorised to be used for any disciplinary purpose or other legal reason, the footage must be retained securely in the relevant case file.
- 8.6 Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.
- 8.7 We will maintain a comprehensive log of when data is deleted.

9 Access to images

9.1 Staff images

- 9.1.1 Staff images will only be accessed if a serious event occurs, such as criminal activity, fraud, gross misconduct, or behaviour that puts others at risk.
- 9.1.2 Access to recorded images will be restricted to requests from senior managers or of equivalent level in relation only to the locations for which they are responsible, and will not be made more widely available. The request, date, time and the reason for authorisation for release of images and CCTV footage will have to be recorded by HR team for audit purposes on a CCTV register. Requests must be approved by HR before the HR team will make the necessary access arrangements.
- 9.1.3 The following information must be kept on a CCTV register maintained for that purpose and held by the Data Protection Officer when media are removed for viewing:
 - (a) the date and time they were removed;
 - (b) the name of the person removing the media;

- (c) the name(s) of the person(s) viewing the images including the department to which the person viewing the images belongs or, if they are from an outside organisation, the organisation's name (e.g. the police);
- (d) the reason for viewing the images; and
- (e) the date and time the media were returned to the system or secure storage (if applicable).

9.1.4 Viewing of recorded images will take place in a restricted or secure area, to which no other member of staff will have access, while viewing is occurring. Images retained for evidence will be securely stored with limited access for authorised staff only.

9.2 Access to and disclosure of images to third parties

9.2.1 Access to and disclosure of images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are protected, and also ensure that the images can be used as evidence if required. Images may only be disclosed in accordance with the purposes for which they were originally collected. Our Data Protection Policy should also be consulted in relation to the capture, storage, access to and disposal of personal data, in this case images of an identifiable individual.

9.2.2 Disclosures to third parties will only be made in accordance with the purpose(s) for which the system is used and will be limited to:

- (a) police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder;
- (b) prosecution agencies (such as the Crown Prosecution Service);
- (c) relevant legal representatives of people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings);
- (d) individuals who have been caught on our CCTV in accordance with a request made such as one described at 11 below;
- (e) in exceptional cases, for others (such as insurers) to assist in identification of a victim, witness or perpetrator in relation to a criminal incident; and
- (f) staff involved with our disciplinary processes.

9.3 If a police officer requests images from our CCTV system in relation to an investigation that has not been initially reported by the business, then please refer them to a Director of the Company. It may be that we are required to disclose the images or we have a discretion whether to do so.

10 Disclosure

10.1 The Data Protection Officer is the only person who can authorise disclosure of information to the police or other law enforcement agencies. All requests for disclosure should be documented for audit purposes in the CCTV register. If disclosure is denied, the reason should also be recorded in the CCTV register.

10.2 Before any images are disclosed the following must be recorded in the CCTV register:

10.2.1 if the images are being removed from the CCTV system or secure storage to another area, the location to which they are being transferred;

10.2.2 any crime incident number, if applicable; and

10.2.3 the signature of the person to whom the images have been transferred.

11 Subject access rights to individuals' own data

11.1 The UK GDPR gives an individual the right to access personal data about themselves, which may include CCTV images and footage. A data subject access request is subject to the statutory conditions from time to time in place and all requests for access to images by any individual (when they are asking for access to images of themselves) should be addressed to the Data Protection Team in a written format, such as email or letter.

11.2

11.3 In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include:

11.3.1 the full name and address of the person making the request (the 'data subject');

11.3.2 a description of the data subject and/or details of what they were wearing or information identifying the individual;

11.3.3 the approximate date and time when the images were recorded;

11.3.4 the location where the images were recorded.

11.4 Requests from an individual for CCTV images or footage must be handled, and responded to, in accordance with our Data Protection Policy. Please refer to our Data Protection Policy for further details.

11.5 Staff responsible for CCTV systems will record and respond to such requests unless the request is made by a member of staff, in which case it will be actioned by HR.

11.6 If we cannot comply with the request, the reasons for not being able to comply will be documented and the data subject will be advised of these in writing.

11.7 The assigned manager responsible for the CCTV system will liaise with the Data Protection Team to determine whether disclosure of the images will reveal third-party information.

11.8 Particular care should be exercised when images of other people are included in the materials for disclosure. Images of other individuals will, if possible, be redacted unless there would be an expectation that their images would be released in such circumstances. Non-disclosure will be appropriate in most circumstances. If there is any doubt about what information must be provided to enquirers, please contact the Data Protection Team.

12 Requests to restrict processing and objections to processing

- 11.1 The UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data. The UK GDPR also gives individuals the right to object to the processing of their personal data in certain circumstances.
- 11.2 All such requests should be addressed in the first instance to the Data Protection Team, who will provide a written response within one month of receiving the request, setting out their decision on the request. A copy of the request and response will be retained for an appropriate period determined on a case-by-case basis. Further information is given in *the Data Protection Policy*.

13 Responsibility for CCTV systems and staff training

- 13.1 Directors will nominate a suitable and qualified manager or senior member of the department with the day-to-day responsibility of the systems and the training of staff responsible for operating or administering CCTV. However, the overall responsibility lies with the Data Protection Team set out at 2.1 above.

14 Complaints

- 14.1 Complaints and enquiries about the operation of our CCTV systems should be made by staff in line with our Grievance Procedure available on our staff intranet (Wiki) or, by customers and visitors, under our Data Protection Policy.
- 14.2 Enquiries relating to the DPA 2018, UK GDPR or CCTV Laws should be addressed to the Data Protection Team at data@nutrixmedical.co.uk. If a member of staff believes that there has been a breach of the DPA 2018, UK GDPR or any CCTV Laws they must contact either the Data Protection Team or their line manager as a matter of urgency in accordance with the data breach reporting process set out in our Data Protection Policy.
- 14.3 If a complainant or enquirer is not satisfied with the response received, they can write to the ICO. Details of how to do this can be found on the ICO website: www.ico.org.uk.

15 Enforcement and compliance

- 15.1 All authorised users of our surveillance technology and its underlying data are required to adhere to the controls around the use of CCTV as set out in this policy and as may be advised separately from time to time. The use of the CCTV system for any purpose other than those specifically authorised will be subject to a full investigation and could lead to disciplinary action up to and including dismissal without notice.
- 15.2 The misuse of our surveillance systems and unauthorised use of images and CCTV footage may constitute a criminal offence.
- 15.3 Any concerns regarding the use of CCTV should be shared with your line manager or, if you are not comfortable with escalating concerns via your line manager, in accordance with our Grievance Procedure.