

CCTV Privacy Notice

This privacy notice explains how Norfolk and Norwich University Hospitals NHS Foundation Trust (the Trust) uses information of individuals when processed via Closed Circuit Television (CCTV).

Who will be using your data?

The Trust will be handling the data as Data Controller for the CCTV imaging.

The Trust has 24-hour CCTV in operation at various sites, including its hospitals, Trust offices and other premises.

The Trust's CCTV activities will capture (collect) and process images in real time wherever the cameras are pointed, capturing footage of individuals whilst they are on the Trust premises. Cameras are situated both inside and outside the buildings. There are signs in place to inform people where cameras are in use.

CCTV footage will only be processed internally by Trust staff who are authorised to do so and where there is a lawful fair and proportionate reason for their involvement.

Cameras are operated by Serco, who are licensed to operate, view and review the video footage as a contracted supplier (Data Processor) to the Trust. All the security officers have undertaken training by the Security Industry Authority (SIA) to be licenced CCTV operators to view and review the video footage.

What types of personal data is used?

- Video images of people and premises.
- Vehicle registration numbers.

What types of special category (sensitive) data is used?

The Trust does not deliberately set out to capture any special category data, any violent or aggressive incidents for purposes of prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security as defined in Section 10 and Section 31 of the Data Protection Act 2018 respectively. However, cameras may incidentally record information which falls within these categories.

This footage may be used as evidence in relation to the purposes set out below.

Purposes for processing information via CCTV

- Ensuring the health and safety of employees, service users and visitors to the sites.
- Detecting, preventing or reducing the incidence of crime.
- Reducing the fear of crime.
- For the prevention of threats to public security
- Preventing and responding effectively to all forms of possible harassment and disorder.

- Creating a safer environment.
- Providing emergency services assistance.
- For monitoring purposes, to see if there are any issues with security or access.
- For employment related issues, for example, disciplinary investigations or detection of fraud, where lawful, fair and proportionate to do so.
- Defending the Trust or its employees with regards to legal or insurance claims.
- Other statutory and public interest obligations applicable to the Trust on a case-by-case basis where lawful, fair and proportionate to do so.

Legal reasons allowing the Trust to process data via CCTV

Our legal basis for processing CCTV related personal data is:

- For employment and contractual related matters.
- To meet a legal obligation.
- To perform tasks in the public interest.

Our legal basis for processing special category data on a case-by-case basis when:

- There is a substantial public interest in processing this information, for the purposes of detecting and preventing crime.

Any processing of the CCTV footage will be conducted in line with the Protection of Freedoms Act 2012 which forms the basis for the Surveillance Camera Code of Practice (2022).

Who do we share information with?

- To provide footage to assist the police with any criminal damage or their investigations.
- To provide footage to insurance companies should there be an incident involving car accidents or damage to cars parked on Trust premises.

Information will only be shared if an appropriate legal basis for the exchange is provided by the requester.

Will personal data be transferred overseas?

The Trust may for operational purposes transfer personal data overseas on an ad-hoc case-by-case basis. In these cases, we will ensure your personal data is protected and there are safeguards for the protection of your rights. Please contact the Trust's Information Governance Team for further details.

How long is data kept for?

This information is retained and held by the Trust for 30 days, except for specific circumstances requiring a longer retention period. This is determined on a case-by-case basis, i.e. in the case of an investigation or legal proceedings.

Does the service make decisions using fully automated processes?

No

What rights do you have over this data?

To be informed about how we use your data	To access a copy of your data which we process	To ask us to rectify or correct your data which we process
To restrict our processing of your personal data	To object to the use of your data	

Some of these rights are subject to exceptions.

Contact the Data Protection Officer

If you have any concerns about how the Trust is using your data, you can contact the Trust's Data Protection Officer by writing to:

Data Protection Officer, info.gov@nnuh.nhs.uk
Norfolk and Norwich University Hospital Foundation Trust
20 Rouen Road
Norwich
NR1 1QQ.

Contact details of the Information Commissioners' Office

If you are not satisfied with how your data has been processed by the Trust or you feel your data protection rights have been breached, you have the right to complain to the Information Commissioner's Office at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Telephone: **0303 123 1113**

Website: www.ico.org.uk

