

Laurel Bank Surgery

Old Hall Street, Malpas, Cheshire SY14 8PS
Tel: 01948 860205 Practice Code: N81038

Partners:

Dr Richard W S Henney
Dr Mark R Edney
Dr Christine L Snowden
Dr Amy L Evitts
Mr Edward Rigby

CCTV Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
1.0	20/03/2024		Practice Manager	New Policy
1.1	20/03/2024	Practice Manager	Practice Manager	Annual Review
1.2	23/03/2026	Practice Manager	Practice Manager	Annual Review

Contents

Introduction	2
Data Protection Statement	2
Retention of Images	3
Access to Images	3
Access to Images by Practice Staff	3
Removal of Images for Use in Legal Proceedings.....	3
Access to Images by Third Parties	4
Access by Data Subjects	4
Procedures for Dealing with an Access Request	4
Annual Review.....	5
Complaints	5

NOTE: Only applicable at Malpas site.

Introduction

Closed circuit television (CCTV) is installed at the Practice premises for the purpose of staff, patient and premises security.

Cameras are located at various places on the premises, and images from the cameras are recorded.

The use of CCTV falls within the scope of the Data Protection Act 2018. In areas of surveillance, signs will be displayed prominently to inform individuals that CCTV is in use.

In order to comply with the requirements of the 2018 Act, data must be:

- Fairly, lawfully and transparently processed.
- Processed for limited purposes and not in any manner incompatible with those purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept for longer than is necessary.
- Processed in accordance with individuals' rights.
- Secure.
- Accountable.

Data Protection Statement

1. The Partners of Laurel Bank Surgery are the Data Controllers in accordance with Data Protection legislation.
2. The Partners of Laurel Bank Surgery are Responsible for the CCTV system.
3. CCTV is installed for the purpose of staff, patient and premises security.
4. The legal basis for the use of CCTV under Article 6 of the UK GDPR is Legitimate Interest.
5. Access to stored images will be controlled on a restricted basis within the practice.
6. Live-feed CCTV may be used to monitor the movements and activities of staff and visitors whilst on the premises.
7. CCTV images may be used where appropriate in implementing the practice Zero Tolerance policy, which governs the Practice response to abusive patient behaviour.
8. External and internal signage is displayed on the premises stating the presence of CCTV.
9. Use of images, including the provision of images to a third party, will be in accordance with Data Protection legislation.
10. The CCTV system at Laurel Bank Surgery DOES NOT record sound. It is image-only technology.
11. CCTV recording is only in reception areas, waiting areas, corridors, stair wells and the staff room (This recording is to cover the window access/exit point only).
12. There is no recording in Private areas such as toilets, consulting rooms, confidential rooms or offices.

Retention of Images

Images from cameras are stored on the CCTV recorder – a stand-alone hard drive computer. This is not connected to the staff network.

Where recordings are retained for the purposes of security of staff, patient and premises, this will be for a period of 30 days, and access will be only available to the Data Controllers and delegated staff.

Access to Images

It is important that access to, and disclosure of, images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes.

Access to the live-feed CCTV is available for security purposes remotely, via mobile application. Access is only available to the Data Controllers and Practice Manager.

Access to Images by Practice Staff

Access to recorded images is restricted to the Data Controllers, who will decide whether to allow requests for access by data subjects and/or third parties (see below).

Viewing of images must be documented as follows:

- The name of the person removing from secure storage, or otherwise accessing, the recordings.
- The date and time of removal of the recordings.
- The name(s) of the person(s) viewing the images (including the names and organisations of any third parties) .
- The reason for the viewing.
- The outcome, if any, of the viewing .
- The date and time of replacement of the recordings.

Removal of Images for Use in Legal Proceedings

In cases where recordings are removed from secure storage for use in legal proceedings, the following must be documented:

- The name of the person removing from secure storage, or otherwise accessing, the recordings.
- The date and time of removal of the recordings.
- The reason for removal.
- Specific authorisation of removal and provision to a third party.
- Any crime incident number to which the images may be relevant.
- The place to which the recordings will be taken.
- The signature of the collecting police officer, where appropriate.

- The date and time of replacement into secure storage of the recordings.

Access to Images by Third Parties

Requests for access to images should be made in writing to the Practice Manager, who will defer to the Data Controller.

The Data Controller will assess applications and decide whether the requested access will be permitted. Release will be specifically authorised. Disclosure of recorded images to third parties will only be made in limited and prescribed circumstances. For example, in cases of the prevention and detection of crime, disclosure to third parties will be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry.
- Prosecution agencies.
- Relevant legal representatives.
- The press/media, where it is decided that the public's assistance is needed to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account.
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings).

All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented as above.

Access by Data Subjects

This is a right of access is provided by the Data Protection Act 2018. Requests for access to images should be made in writing to the Practice Manager, who will defer to the Data Controller.

The requestor needs to provide enough information so that they can be identified in the footage, such as a specific date and time, proof of their identity and a description of themselves. Any footage provided may be edited to protect the identities of any other people.

The Practice may charge a reasonable fee to provide the footage if the request to see a copy of the personal information is deemed unfounded or excessive.

Procedures for Dealing with an Access Request

All requests for access by Data Subjects will be dealt with by the Practice Manager. The Data Controller will locate the images requested. The Data Controller will determine whether disclosure to the data subject would entail disclosing images of third parties.

The Data Controller will need to determine whether the images of third parties are held under a duty of confidence. In all circumstances the practice's indemnity insurers may be asked to advise on the desirability of releasing any information.

If third party images are not to be disclosed, the Data Controllers will arrange for the third party images to be disguised or blurred. If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out.

If an editing company is used, then the Data Controller must ensure that there is a contractual relationship between them and the editing company, and:

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images
- The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the Data Controllers.
- The written contract makes the security guarantees provided by the editing company explicit.

The Practice Manager will provide a written response to the data subject within 28 days of receiving the request setting out the Data Controllers' decision on the request.

A copy of the request and response should be retained.

Annual Review

The purpose and legal basis for CCTV surveillance, as well as the operation of CCTV at Laurel Bank Surgery will be reviewed annually by the Practice Manager.

Complaints

All complaints will be managed in accordance with the Laurel Bank Surgery complaints procedure.