DATA PROTECTION
POLICY DOCUMENT

COMMERCIAL INSTALL

Helping U.K. CCTV Operators meet their
Data Protection obligations.

020 8050 7052

GDPR Safe Limited
https://www.gdprsafe.co.uk
info@gdprsafe.co.uk

GDPR Safe

Data Protection Policy

Covering the use of CCTV Equipment in a Commercial Setting

Policy Holder Name:	Rogiet Community Council	**Policy Number:**	RTPEVW7NYWNV
		Policy Issue Date:	03/11/24
Installation Address:	Rogiet Hub Westway Rogiet, Caldicot NP263SP	**Policy Expiry Date:**	03/11/25
		Last Review Date:	03/11/24
Administrative Contact:	Alice Vaughan	**Policy Version:**	C13
Administrative Address:	Rogiet Hub Westway Rogiet, Caldicot NP263SP		

Introduction

This policy document outlines the details of a CCTV installation at a Commercial property within the United Kingdom. It includes important details about how relevant individuals & organisations intend to utilise the system and the footage that it may capture whilst in operation.

Where CCTV is in use within the U.K. in a commercial setting, the U.K. GDPR and Data Protection Act 2018 (the "Data Protection Laws") apply to its use.

Data Protection Laws & Personal Data

The Data Protection Laws outline the ways in which "Personal Data" may be processed by organisations and individuals. Personal Data is defined as any information relating to an individual, which allows them to be directly or indirectly identified. This includes still images (photographs) and video recordings of individuals.

These Data Protection Laws are intended to protect the privacy of individuals whose images may be recorded by a CCTV system, and place restrictions on how the operator of the system may legally process those images.

Where an operator fails to observe & uphold the Data Protection Laws, the Information Commissioner's Office (ICO) has powers to take enforcement action against the operator, which can include significant fines.

Additionally, operators failing to observe the relevant legislation may be at risk of civil litigation from individuals claiming that their personal data (i.e., their image) has been unlawfully processed.

The purpose of this Data Protection Policy is to outline the ways in which the operator intends to meet their obligations under the Data Protection Laws, and to explain the rights of individuals and how the operator intends to respect those rights.

Where is CCTV being used?

This policy relates specifically to the Commercial CCTV installation at the following address:

Rogiet Hub Westway, Rogiet, Caldicot, NP263SP

Details of the cameras that are located at this property can be found later in this document.

Who is responsible for the CCTV installation?

UK Data Protection Laws recognise individuals that process Personal Data either as Data Controllers or Data Processors. Data Controllers are individuals who exercise overall control of the processing of Personal Data, deciding both the reasons for which it is collected, and the ways in which it is processed. Data Processors are individuals that act on behalf of, and only on the instructions of, Data Controllers.

In the context of a Commercial CCTV installation, it is possible that there will be one or more Data Controllers.

Where multiple organisations are collectively responsible for the decision-making process that led to the installation of CCTV, those organisations would be treated as joint Data Controllers, each with equal legal responsibilities for the protection of personal data captured by that CCTV system.

This might be the case where an organisation coordinates with a parent or sister company to agree on the reasons for installing the CCTV system. This may also be the case with businesses that are part of a franchise model, where the Franchisor places certain obligations on the Franchisee to ensure that CCTV is installed on their premises.

The Policy Holder has indicated that the decision to install CCTV at the aforementioned commercial property was made exclusively by employees of **Rogiet Community Council**, with no outside influence from any other individual or organisation. The sole Data Controller for this CCTV system is therefore **Rogiet Community Council.**

Individuals wishing to contact the Data Controller to discuss its use, or to exercise their rights under UK Data Protection Law should address all communications to:

Alice Vaughan

Rogiet Hub, Westway, Rogiet, Caldicot, NP263SP

Where are Cameras being used on the property?

This policy relates to footage that is captured by any of the cameras that are in use within the property. The Policy Holder has assigned a name to each of the cameras in use, relating to where they are situated within the property. They are as follows:

- CAM 01 - Hub External, SE Corner
- CAM 02 - Hub Internal, Main Entrance
- CAM 03 - Hub Internal, Sports Entrance
- CAM 04 - Hub External, SW corner
- CAM 05 - Car Park Column, Sports Pitch
- CAM 06 - Car Park Column, Play Park
- CAM 07 - Car Park Column, Car Park and Allotments
- CAM 08 - Hub External, memorial and entrance road

The Policy Holder has indicated that of those cameras listed, the following cameras capture images of public spaces (such as footpaths, highways or concourses) surrounding the boundary of the property:

- CAM 01 - Hub External, SE Corner
- CAM 02 - Hub Internal, Main Entrance
- CAM 03 - Hub Internal, Sports Entrance
- CAM 04 - Hub External, SW corner
- CAM 05 - Car Park Column, Sports Pitch
- CAM 06 - Car Park Column, Play Park
- CAM 07 - Car Park Column, Car Park and Allotments
- CAM 08 - Hub External, memorial and entrance road

When installing cameras on the property, efforts were made to ensure that the positioning of cameras minimised the extent to which images of public areas beyond the property boundary were captured, as far as was possible without impacting the effectiveness of the cameras for the legitimate purposes outlined elsewhere in this document.

The Policy Holder has indicated that Privacy Screens have not been configured for the cameras that capture footage of public areas, for the following reasons:

- The use of Privacy Screens, combined with the positioning of the cameras, would have a damaging or detrimental impact on the purpose for which CCTV is in use.

The Policy Holder has indicated that of those cameras listed, none currently capture images of neighbouring properties.

Why has the CCTV system been installed?

Any individual or organisation processing Personal Data is required by law to have a "lawful basis" for processing that data. There are several such lawful bases which may be used to justify processing, but in the context of a Commercial CCTV installation, the one that generally applies is what's referred to as a "legitimate interest".

The Data Controller has decided to install CCTV for the purposes of the following legitimate interests:

- the prevention and investigation of crime.
- public safety and the safety of employees and other visitors to the property.

Additionally, the system has been installed in response to the following events that have occurred in the past, and which the Data Controller has identified as justifications that support the use of the above legitimate interests:

- criminal damage at the property.
- anti-social behaviour occurring in the local area.

How will recorded footage be viewed?

Modern CCTV systems offer a range of ways to view recorded footage, such as via a monitor directly connected to the recording device, using software on a networked computer, or via Smart Devices such as Tablets and Mobile Phones.

The Policy Holder has stated that the footage captured for this installation will be accessible in the following ways:

- Footage can be viewed on a computer, tablet or mobile device within the property.
- Footage can be viewed remotely via an Internet Connection using a computer, tablet or mobile device.

The Policy Holder has also indicated that the following groups of people will be permitted to access recorded footage from the CCTV system:

- Employees of Rogiet Community Council working in a Security, Audit or Loss Prevention capacity.
- Current members of Rogiet Community Council...
- ...authorised by resolution(s) of Council.

The Policy Holder has indicated that a range of procedural and technological measures are being employed to ensure that only authorised individuals are permitted to view footage captured by the CCTV system.

Has signage been erected indicating that CCTV is in use?

One of the key tenets of UK Data Protection Law is transparency.

Where Personal Data is being processed, it must be made clear to those individuals whose data you're processing that you are processing their data. They must also be informed why you're processing their data, and what their own rights are as they relate to their data. This is what's more commonly referred to as the right to be informed.

Where a commercial CCTV system captures images of individuals beyond the property boundary, the Data Controller and any appointed Data Processors are processing Personal Data.

The individuals in question (known as "Data Subjects") have a legal right to be informed that you are capturing images of them, as well as the reasons why – and you have a legal obligation to make them aware of these details at the time that their data is being processed (i.e. when they're being recorded), or as soon as is practical.

For commercial CCTV systems, this is typically achieved by displaying signage that indicates that CCTV is in use, and the purposes for which it is in use.

It is not sufficient to simply indicate that CCTV is in use – the reasons for which CCTV is in use must also be indicated for signage to meet the legal requirements.

It is also strongly recommended that signage includes the details of the Individual(s) or Organisation(s) that act as the Data Controller for the CCTV installation, though this is not always strictly necessary if it is obvious who operates the system.

For example, if more than one business shares occupancy of a commercial property, it may be unclear to Data Subjects who it is that is operating the CCTV system within that property. In this situation, the organisation operating the system would be expected to display signage which makes it obvious who the operator of the system it.

If the operator of the CCTV system is the sole occupant of a building, and if other signage allows a Data Subject to easily identify the sole occupant of that building, it could be argued that the CCTV signage doesn't need to include the details of the operator – because that information can be deduced by other means.

The Policy Holder has indicated that suitable signage has been displayed on the property.

Is Facial Recognition in use?

Facial Recognition technology can be used to identify individuals entering a monitored area automatically, by extracting biometric signatures from the faces of individuals that are captured by CCTV camera. This information can then be cross-checked with a database of known individuals, or be used as a mechanism for indexing recorded footage so that footage featuring a particular individual can be more readily accessed in the future.

Facial Recognition technology is considered to be particularly intrusive, as it can be used to profile the behaviours of individuals based on their movements. Organisations choosing to use the technology should therefore ensure that they have an adequate justification for using it, which outweighs the right to Privacy of a Data Subject.

There are an ever-growing number of applications for this technology, but some common uses include quickly identifying individuals that are known to Security & Loss Prevention teams when they are detected on a retail property or alerting Security teams to the presence of unknown individuals within a property. Facial Recognition may also be used as an Access-Control mechanism, permitting, or denying access to facilities based on whether or not the individual is recognised.

The Policy Holder has indicated that Facial Recognition is not currently in use on the property.

Is Automatic Number Plate Recognition (ANPR) in use?

Automatic Number Plate Recognition technology can be used to identify vehicles entering a monitored area automatically, by extracting Registration / License plate data from recorded images.

The technology is most commonly used to enforce restrictions on Parking facilities, to identify vehicles that have either failed to pay for the use of the facility, or who have remained on the property for longer than permitted.

ANPR technology is considered to be particularly intrusive, as it can be used to profile the behaviours of individuals based on the movements of their vehicles. Organisations choosing to use the technology should therefore ensure that they have an adequate justification for using it, which outweighs the right to Privacy of a Data Subject.

The Policy Holder has indicated that Automatic Number Plate Recognition is not currently in use on the property.

Do any of the cameras capture audio?

Whilst audio capture is not commonly used with commercial CCTV systems, most modern cameras do support the ability to record audio.

The Policy Holder has indicated that none of the cameras in use on the property are used to capture audio as part of their recordings.

For how long will footage be retained?

The U.K. GDPR states that any personal data being processed should be limited only to that which is necessary to achieve the purposes for which it was originally collected.

In practice, this means that recorded footage should only be retained for as long as is necessary to achieve the purposes for which the CCTV system was installed - as outlined earlier in this Policy document.

For example, if the CCTV system has been installed for the purposes of detecting and investigating crime, you need to be able to illustrate that you are not retaining data for longer than is necessary to detect or investigate a crime.

Where a burglary or criminal damage occurs at a commercial property that is regularly occupied, it is typically the case that the burglary or criminal damage will be detected in a relatively short timeframe, allowing for footage to quite quickly be reviewed, and evidence collected. In such circumstances, a relatively short retention period would be appropriate.

However, if the same event were to occur at a remote property that is rarely occupied, it may take longer for the crime to be detected – delaying the start of any investigation into that event. This would justify a greater retention period of recorded footage.

The Policy Holder has indicated that footage will be retained for no longer than 30 days, after which it is permanently deleted or overwritten.

It is important to note that where footage is required for evidentiary purposes, following the detection of a crime, that specific footage may be retained for a longer period to allow for legal proceedings to complete.

What about the physical security of Personal Data?

The Data Protection Laws place a legal requirement on Data Controllers and Data Processors to ensure appropriate technical and operation measures are taken to secure any personal data that they hold, including CCTV footage stored on a recording device (commonly referred to as DVRs or NVRs).

This means that the device used to record CCTV footage must be adequately secured to ensure that the personal data held within it cannot be unlawfully accessed by unauthorised individuals.

For example, if the recording device were to be stolen during a burglary, this could represent a personal data breach – if the device contains footage of Data Subjects.

These requirements extend to any removable media that may be used to store footage, such as DVDs, BluRay Disks, USB Memory Devices or Hard Disk Drives.

The Policy Holder has indicated that the CCTV Recording device in use is in a physically secure location such as a locked cabinet or room.

The Policy Holder has indicated that only the following individuals have physical access to the recording device:

- employees of Rogiet Community Council, working in a Security or Loss Prevention capacity.
- Current Chair of Rogiet Community Council.

To protect against the possible theft of CCTV Recording devices, it is sometimes possible to enable the encryption of data whilst it is being stored. The advantage of encrypting footage during recording is that should the recording device ever be stolen, the data stored within it will not be accessible to anyone other than its original owner.

The encryption of data during recording is typically a feature that is limited to more advanced recording equipment, however - so is not always possible on all CCTV systems.

The policy holder has indicated that encryption is not in use on the recording device, because the equipment does not support it – however other physical security measures have been implemented that the policy holder deems appropriate to ensure the security of personal data.

How is footage being recorded?

Most CCTV systems provide the option to record footage only when motion is detected within the field of view of a given camera. This can be advantageous, as it minimises the amount of data that needs to be stored by the recording device, since footage is not recorded when nothing is moving within the camera's field of view.

Most systems also allow the sensitivity of motion detection to be adjusted, allowing recording to take place only when significant changes in the camera field of view are detected. This allows the system to avoid recording things that may not be of importance, such as trees blowing in the wind.

Alternatively, a CCTV system or Video Doorbell may be configured to continually record footage, regardless of whether movement has been detected.

The policy holder has indicated that the system is configured to record footage continually.

How may an individual request copies of CCTV footage that features themselves?

The U.K. GDPR gives individuals a legal right to request copies of any personal data relating to themselves that is held by another individual or organisation, this includes CCTV footage in which they can be identified.

This is what is commonly referred to as a Subject Access Request or "SAR", or the "Right of Access".

Data Controllers, such as those operating a CCTV system, have a legal responsibility to respond to such requests in a timely manner, without causing undue hinderance to the person making the request.

There are strict time limits which must be observed by Data Controllers when responding to Subject Access Requests. Data Controllers are typically required to respond to SARs within one month of receiving them, though there are some exceptional circumstances in which this may be extended.

Individuals wishing to exercise their right to submit a Subject Access Request can do so in several ways:

- Subject Access Requests may be submitted securely via the GDPR Safe service, which can be accessed free-of-charge online at www.gdprsafe.co.uk.

  GDPR Safe is an organisation that acts as an agent for the Policy Holder & Data Controller, assisting them in promptly responding to Subject Access Requests, as required by law.

  Our secure electronic form will ask the individual making the request for all the details that are essential to allow the Data Controller to respond to the request promptly.

- Subject Access Requests may also be submitted to the CCTV Operator in writing, at the following address: **Alice Vaughan, Rogiet Hub, Westway, Rogiet, Caldicot, NP263SP**

- Subject Access Requests may also be submitted verbally to the CCTV Operator, by speaking to the individual(s) mentioned above, indicating that you would like to make a Subject Access Request.

Typically, the individual requesting data may only request data that relates to themselves. However, an individual may request that someone else submits a request on their behalf – such as a relative, friend or solicitor – but only with their express permission. It is the responsibility of the Data Controller to ensure that in such cases, they have verified that the individual in question has indeed consented to their data being shared with that third party.

GDPR Safe Policy Holders with an active Data Protection Policy may request support from GDPR Safe in responding to Subject Access Requests. The GDPR Safe team will provide guidance on how to respond to the request, given the specific details of the request and the footage that was requested.

Paying your Data Protection Fee to the ICO

As a business operating a CCTV system, **you are required by law** to pay an annual "data protection fee" to the Information Commissioner's Office. This fee is used by the ICO to fund their efforts towards promoting and enforcing data protection legislation.

Failure to pay this fee each year can result in a fine of up to £4,350 - so we recommend that you choose to pay via Direct Debit wherever possible to ensure that you do not miss a payment.

The amount that you need to pay will depend upon the size and nature of your business:

- **Tier 1, Micro Organisations** – if your business has turnover of no more than £632,000 ***OR*** has no more than 10 members of staff, you will be required to pay **£40/year**.

- **Tier 2, Small & Medium Sized Organisations** – if your business has turnover of no more than £36 Million ***OR*** has no more than 250 members of staff, you will be required to pay **£60/year**.

- **Tier 3, Large Organisations** – if your business doesn't meet the criteria for a Micro Organisation or a Small & Medium Sized Organisation, you will be required to pay **£2,900/year**.

Your Data Protection Fee should be paid directly to the Information Commissioner's Office, in one of two ways:

Online

Simply visit the ICO Website at the following address and answer a series of questions to confirm the amount that you need to pay: https://www.gov.uk/data-protection-register-notify-ico-personal-data

You can use a Smartphone to scan the QR Code below to take you straight to the relevant page:

By Phone

You may also call the Information Commissioner's Office directly on **0303 123 1113.**

Please note that call charges do apply, and can be considerably more expensive when made from a Mobile Phone.

Be advised that following payment of the Data Protection Fee, your organisation name and address will be visible on a Public Register of Fee Payers.

How to use this Policy Document

You should make the information contained within this policy document freely available to any individual whose Personal Data may be captured or processed as part of operating your CCTV equipment.

This might include members of the public, employees, visitors / contractors etc.

Those individuals can then understand what data you are capturing and your justifications for doing so.

This document also explains the rights that those individuals are guaranteed under UK Data protection law, and how you, as a Policy Holder, intend to uphold those rights.

We also strongly recommend that all employees are provided with access to this policy document, as a Data Subject may initially approach **any** employee of the organisation when exercising their rights under the Data Protection Act (2018). Whilst you may have individuals or departments within your organisation that are specifically tasked with responding to such requests, it is important that all employees understand how to identify when a Data Subject is attempting to exercise one of their rights and know how to respond appropriately.

GDPR Safe are continually refining the details o our Policy Documents, and from time to time you may receive communications from us to inform you of changes that may require you to update your policy. It is important that you ensure you respond to any such communications as quickly as possible, to ensure that your policy remains suitable for your current use of the CCTV system.

How to contact GDPR Safe

Policy holders can contact us by telephone or email during their policy term, to discuss specific details of your policy or in relation to Subject Access Requests submitted to you by individuals.

GDPR Safe can be contacted by Telephone, Monday to Friday (9am to 5:30pm), by calling 020 8050 7052.

Policy Holders may also contact us by email, at support@gdprsafe.co.uk. Emails are monitored Monday to Friday (9am to 5:30pm) and will typically receive a response within 1 working day.