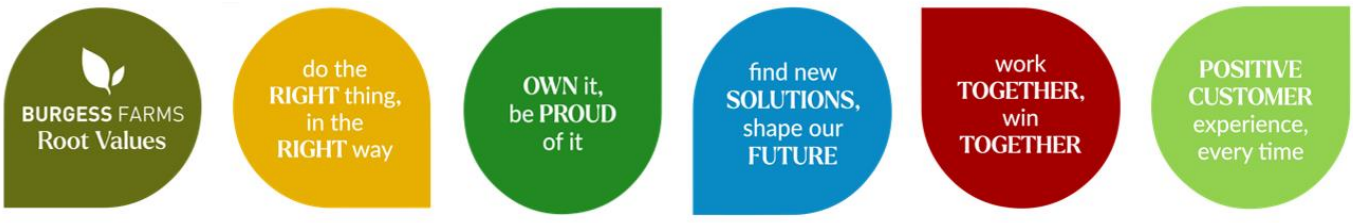
BURGESS FARMS

CCTV POLICY AND PROCEDURE			
Author:	Human Resources		
Document Reference:	BFHRPO32		
Revision no.	0.5	**Publish Date:**	February 2026
Document status:	Current		
For us by:	All employees of Burgess Farms and its subsidiary Companies		
Purpose:	To set out clear and consistent guidelines relating to how the business manages the use of closed-circuit television (CCTV) on its premises		
This document supports: *Standards and legislation*	Data Protection Act (DPA)1998, the Employment Practices Code and the Information Commissioner's Office (ICO) CCTV Code of Practice		
Key related documents:	Employee Handbook Statement of Terms and Conditions of Employment Disciplinary Policy and Procedure Grievance and Dispute Policy & Procedure Equal Opportunities Policy and Procedure Bullying and Harassment Policy and Procedure Whistleblowing Policy & Procedure Data Protection Policy		
Review date:	Changes to legislation / Changes to Company policy		



Contents

	Definitions	3
1.	Policy Statement	3
2.	Key Principles	3
3.	Scope	3
4.	Purposes of CCTV	3
5.	Location of cameras	3
6.	Recording and retention of images	4
7.	Access and disclosure of images.....	4
8.	Individual access rights.....	5
9.	Covert recording	5
10.	Evidence from CCTV footage.....	6
11.	Staff training.	6
12.	Implementation.	6
13.	Breach of policy	6
14.	Document control.....	6

Definitions

"Company" means Burgess Farms (Produce World Group)

"Subsidiary Companies" means all companies owned by Burgess Farms (Produce World Group)

1. Policy Statement

The purpose of this Policy is to set clear and consistent guidelines in how Burgess Farms manages the use of close circuit television (CCTV) on its' sites.

This policy provides the framework for the management, application and use of CCTV.

2. Key Principles

The Company uses closed circuit television (CCTV) images to provide a safe and secure environment for employees and for visitors to the Company's business premises, such as clients, customers, contractors and suppliers, and to protect the Company's property.

This policy sets out the details of how the Company will collect, use and store CCTV images. For more information on your privacy rights associated with the processing of your personal data collected through CCTV images please refer to the Company privacy notice and GDPR data protection policy.

The Company's CCTV facility records images only. There is no audio recording i.e. conversations are not recorded on CCTV (please refer to the section below on covert recording).

3. Scope

This policy applies to all employees employed by Burgess Farms and its subsidiary companies. This policy is non-contractual and may be varied or revoked by the Company at any time with or without notice.

4. Purposes of CCTV

The purposes of the Company installing and using CCTV systems include:

- to monitor the security of the Company's business premises;
- to assist in the prevention or detection of crime or equivalent malpractice;
- to assist in the identification and prosecution of offenders;
- to ensure that health and safety rules and Company procedures are being complied with;
- to assist with the identification of unauthorised actions or unsafe working practices that might result in disciplinary proceedings being instituted against employees and to assist in providing relevant evidence; and / or
- to promote productivity and efficiency

5. Location of cameras

Cameras are located at strategic points throughout the Company's business premises. Locations will vary from site to site and will be identified through appropriate signage and Company Notice Boards or communications.

The Company has positioned the cameras so that they only cover communal or public areas on the Company's business premises and they have been sited so that they provided clear images. In some cases, cameras may also be located within designated work areas or reception areas, where there are additional security or safety considerations. This may vary from site to site.

No camera focuses, or will focus, on toilets, shower facilities, changing rooms, staff kitchen areas, staff break rooms or private offices.

All cameras (with the exception of any that may be temporarily set up for covert recording) are also clearly visible. See covert recording clause below.

Appropriate signs are prominently and clearly displayed so that employees, clients, customers and other visitors are aware they are entering an area that is covered by CCTV.

6. Recording and Retention of Images

Images produced by the CCTV equipment are intended to be as clear as possible so that they are effective for the purposes set out above. Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly and that the media is producing high quality images.

Images may be recorded either in constant real-time (24 hours a day throughout the year), or only at certain times, as the needs of the business dictate.

As the recording system records digital images, any CCTV images that are held on the hard drive of a PC or server are deleted and overwritten on a recycling basis and, in any event, are not held for more than three months - this may vary from site to site or on a case by case basis. Details are available from site management. Once a hard drive has reached the end of its use, it will be erased prior to disposal.

Images that are stored on or transferred on to removable media, such as CDs, are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of one month. However, where a law enforcement agency is investigating a crime, images may need to be retained for a longer period. This may also be the case where there has been an accident or incident at site, whereby the CCTV footage will be required for longer term investigation purposes.

7. Access and Disclosure of Images

Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected.

The images that are filmed are recorded centrally at site and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system and to those line managers who are authorised to view them in accordance with the purposes of the system (see list of authorised users held at site). Viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing occurs. If media on which images are recorded is removed for viewing purposes this will be documented. A Written Log will be held at each site which will record: Who has viewed any footage (need to be on list of authorised users), the reason why, date and time, who authorised the viewing, and "any other comments".

Disclosure of images to other third parties will only be made in accordance with the purpose for which the system is used and will be limited to:

- the police and other law enforcement agencies, where the images recorded could assist in the prevention of a crime or the identification and prosecution of an offender or the identification of a victim or witness;
- prosecution agencies, such as the Crown Prosecution Service;
- relevant legal representatives;
- Company insurers or brokers or agents of the insurers;
- line managers involved with Company disciplinary or grievance processes;
- the human resources and/or SHEE department;
- third party contractors, where an incident is alleged involving one of their staff; and / or
- individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention of detection of crime or the apprehension or prosecution of offenders)

The Manager of the site (or another senior manager acting in their absence) is the only person who is permitted to authorise disclosure of images to external third parties such as law enforcement agencies. In the absence of the Manager, then this permission will be given by a member of the Human Resources Department or the Group SHEE Manager (where the incident involves external insurers).

All requests for disclosure and access to images will be documented, including date of disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

8. Individual's Access Rights

Under the UK's data protection laws, including the General Data Protection Regulation (GDPR), individuals have the right on request to receive a copy of the personal data that the Company holds about them, including CCTV images if they are recognisable from the image.

If you wish to access any CCTV images relating to you, you must make a written request to the Company's Data Protection Champion - see SharePoint or Company Notice Boards for who this is. The Company will usually not make a charge for such a request, but we may charge a reasonable fee if you make a request which is manifestly unfounded or excessive or is repetitive. Your request must include the date and approximate time when the images were recorded and the location of the particular CCTV camera, so that the images can be easily located, and your identity can be established as the person in the images.

The Company will respond promptly and in any case within 30 calendar days of receiving the request. However, where a request is complex or numerous the Company may extend the one month to respond by a further two months.

Note: The Company will always check the identity of the person making the request before processing it.

The Data Protection Champion will first determine whether disclosure of your images will reveal third party information as you have no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.

If the Company is unable to comply with your request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, you will be advised accordingly.

9. Covert Recording

The Company is aware that covert recording can only be done in exceptional circumstances for example where the Company suspects criminal activity taking place. On this basis the Company will only undertake covert monitoring if it has carried out a data protection impact assessment which has addressed the following:

- the purpose of the covert recording;
- the necessity and proportionality of the covert recording;
- the risks to the privacy rights of the individual(s) affected by the covert recording;
- the time parameters for conducting the covert recording
- the safeguards and/or security measures that need to be put in place to ensure the covert recording is conducted in accordance with the data protection laws, including the GDPR.

If after undertaking the data impact assessment the Company considers there is a proportionate risk of criminal activity, or equivalent malpractice taking place or about to take place, and if informing the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection, the Company will covertly record the suspected individual(s). In doing this the Company will rely on the protection of its own legitimate interests as the lawful and justifiable legal basis for carrying out the covert recording.

Before the covert recording commences the Company will ensure that the Managing Director (or another senior director acting in their absence) agrees with the findings of the data protection assessment and provides written authorisation to proceed with the covert recording.

Covert monitoring may include both video and audio recording.

Covert monitoring will only take place for a limited and reasonable amount of time consistent with the objective of assisting in the prevention and detection of suspected criminal activity or equivalent malpractice. Once the specific investigation has been completed, covert monitoring will cease.

Information obtained through covert monitoring will only be used for the prevention or detection of criminal activity or equivalent malpractice. All other information collected during covert monitoring will be deleted or destroyed unless it reveals information which the Company cannot reasonably be expected to ignore.

10. Evidence from CCTV footage

CCTV evidence may be used against an employee in disciplinary proceedings only where such evidence tends to show, in the reasonable belief of the Company, that the employee has been guilty of serious misconduct. The employee will be given the chance to see and respond to the images in these circumstances.

11. Staff Training

The Company will ensure that all employees handling CCTV images or recordings are trained in the operation and administration of the CCTV system and the impact of the General Data Protection Regulations (2018) on the use of the system.

12. Implementation

Site management are responsible for the implementation of and compliance with this policy and the operation of the CCTV systems. They will conduct an annual review of the sites use of CCTV within each business unit.

Any complaints or enquiries about the Company's CCTV system should be addressed to Data Protection Champion.

13. Breach of Policy

Breach of the CCTV Policy may be regarded as misconduct and may lead to disciplinary action, or legal proceedings.

14. Document Control

Version	Revision	Action	Author	Date
0.3		• Updated to comply with GDPR requirements	NMT	12.07.19
0.4		• Updated format	SA	27.11.25
0.5		• Updated format	GT	18.02.26