Millennium Farm Trust

GN11 CCTV Policy V02

Next review date Jan 2028

Version Control

Version number	Date of changes	Who	Review summary
01	Jan 2019	TCF	
	07/02/23	TCF	Scheduled review. No changes
02	26/03/25	MLL	Scheduled review. Added impact assessment template and logs

This policy in drafted in accordance with the requirements of the General Data Protection Regulation ("GDPR"). It will come into effect on 25 May 2018.

Policy Statement

Millennium Farm Trust uses Close Circuit Television (CCTV) within the premises of Depden Care Farm. The purpose of this policy is to set out the position of the Trust as to the management, operation and use of the CCTV at the farm. This policy applies to all members of our staff, farm helpers, visitors and all other persons whose images may be captured by the CCTV system.

This policy takes account of all applicable legislation and guidance, including:

- The General Data Protection Regulation
- Data Protection Act 2018
- CCTV Code of Practice produced by the Information Commissioner
- Human Rights Act 1998

This policy sets out the position of the Trust in relation to its use of CCTV.

Purpose of CCTV

MFT uses CCTV for the following purposes:

- To provide a safe and secure environment for staff, farm helpers, support workers and visitors
- To prevent the loss of or damage to MFT buildings and/or assets
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

Description of system

MFT uses fixed cameras at the farm. Cameras are not equipped for sound recording.

Siting of Cameras

CCTV cameras are sited in such a way as to meet the purpose for which the CCTV is operated. Cameras are sited in prominent positions where they are clearly visible to staff, farmhelpers and visitors. Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. MFT will make all reasonable efforts to ensure that areas outside of the farm premises are not recorded. Signs have been erected to inform individuals that they are in an area within which CCTV is in operation. Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing areas or toilets.

Locations

Camera	Location/view area	Purpose
1	South end of HQ overlooking drive/garage	Monitor access to rear of HQ and farm
2	West side of HQ, looking at workshop door	Monitor access to workshop area
3	Front of HQ looking over carpark	Monitor vehicles arriving
4	Above entrance to HQ	Monitor HQ arrivals and security of veg shed

Privacy Impact Assessment

Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by MFT (Appendix 1) to ensure that the proposed installation is compliant with legislation and ICO guidance. MFT will adopt a privacy by design approach when installing to avoid recording and storing excessive amounts of personal data.

Management and Access

The CCTV system will be managed and operated by Tim Freathy, Director. The viewing of live and recorded CCTV images will be restricted to members of staff at the farm, for the purposes set out above. No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images. Recorded on the CCTV Access Log (Appendix 2) The CCTV system is checked monthly by the Director to ensure that it is operating effectively.

Storage and Retention of Images

Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded. Recorded images are stored only for a period of thirty-one days unless there is a specific purpose for which they are retained for a longer period. MFT will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures at the farm include:

- CCTV recording systems is in a restricted area.
- The CCTV systems is encrypted and access is password protected
- Copies of data is restricted to the director.
- A log of any downloading of the CCTV images, including time and dates of access and record of the individual accessing the images will be maintained by MFT.

Disclosure of Images to Data Subjects

Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation and has a right to request access to those images. Any individual who requests access to images of themselves or of a person for whom they have support/ care responsibilities (e.g. vulnerable adults and farm helpers) will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the trust's Subject Access Request Policy. When such a request is made the Director will review the CCTV footage, in respect of relevant time periods, in accordance with the request. If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Director must take appropriate measures to ensure that footage is restrict in this way. If the footage contains images of other individuals the MFT must consider whether:

- The request requires the disclosure of the images of individuals other than the requester, e.g. can the images be distorted so as not to identify others.
- The other individuals in the footage have consented to the disclosure of the images or their consent can be obtained.
- If not, then whether it is otherwise reasonable in the circumstance to disclose those images.

A record must be kept, and held securely, of all disclosures which sets out:

- When the request was made;
- The process followed by the Director in determining whether the images contained third parties;
- The considerations as to whether to allow access to those images;
- The individuals that were permitted to view the images and when; and
- Whether a copy of the images was provided, and if so to whom, when and in what format.

Disclosure of Images to Third Parties

MFT will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation. CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place. If a request is received from a law enforcement agency for disclosure of CCTV images the Director must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images. The information above must be recorded in relation to any disclosure using the CCTV Image Disclosure log (Appendix 3). If an order is granted by a Court for disclosure of CCTV images, then this should be complied with.

Review of Policy and CCTV System

The CCTV system and the privacy impact assessment relating to it will be reviewed every three years.

Misuse of CCTV systems

The misuse of CCTV system could constitute a criminal offence. Any member of staff who breaches this policy may be subject to disciplinary action.

Complaints relating to this policy

Any complaints relating to this policy or to the CCTV system operated by the Trust should be made in accordance with MFT's Complaints Policy.

Appendix 1 CCTV Privacy Impact Assessment template

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons

Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 2: CCTV Access Log

Date	Name	Camera details	Date/time period accessed	Reason for viewing	If incident give brief description of incident

Appendix 3: CCTV image disclosure log

UK GDPR and the Data Protection Act 2018 require organizations to handle personal data (including CCTV footage) lawfully and transparently. Logging disclosures helps demonstrate compliance. A log provides a record of who accessed or received CCTV footage, why, and when, which is crucial for accountability and auditing. A log demonstrates transparency to individuals whose images are captured by CCTV, if they request access to the footage.

Date and Time of Disclosure: Record the exact date and time the footage was shared.
Third Party: Clearly identify the individual or organization to whom the footage was disclosed.
Reason for Disclosure: Document the specific purpose for which the footage was shared (e.g., law enforcement investigation, security incident, etc.).
Extent of Information Disclosed: Specify what footage was shared (e.g., specific time period, location, etc.).
Denial of Disclosure: If a request for disclosure is denied, record the reason for denial.
Method of Disclosure: Record how the footage was shared (e.g., secure email, physical copy, etc.