1 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at MWH, including all personnel affiliated with third parties. It also applies to all visitors to MWH controlled locations.

MWH use external and internal CCTV cameras to view and record individuals on and around our premises to maintain a safe environment for staff and visitors. However, we recognise that the images of individuals recorded by CCTV cameras are personal data which must be processed in accordance with data protection legislation.

As a controller, we have registered our use of CCTV with the Information Commissioner's Office (ICO) and seek to comply with its best practice suggestions.

The purpose of this policy is to:

- Outline why and how MWH will use CCTV, and how we will process data recorded by CCTV cameras,
- Ensure that the legal rights of individuals, relating to their personal data, are recognised and respected,
- Assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence; and
- Explain how to make a subject access request in respect of personal data created by CCTV.

2 Application

This policy applies to all CCTV systems operated by MWH or by a third party when contracted to operate CCTV on behalf of MWH.

It also includes other image-based technology such as face recognition security access systems, Automatic Number Plate Recognition (ANPR), dashcams or cab-cams, if these are used in MWH premises or vehicles.

This policy does not apply to CCTV systems operated by other organisations. For example, this may include building owners where MWH rent space in a shared facility or systems operated by clients on treatment works where MWH have construction sites. These organisations will have their own policies and procedures.

It also excludes webcams used for online meetings, for example using Microsoft Teams or Zoom.

A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

This policy should be read in conjunction with:

- MP27 MWH Treatment GDPR Privacy Notice
- MP28 Data Protection Policy

3 Contents

4 Responsibilities

The Chief Executive has overall responsibility for the effective operation of this policy. The Chief Executive has delegated responsibility for overseeing its implementation to the MWH Data Protection Officer.

Suggestions for changes to this policy should be made to the Data Protection Officer privacy@mwhtreatment.com.

Any questions you may have about the day-to-day application of this policy should be referred to the HR team in the first instance.

This policy is reviewed on a regular basis, together with the ongoing use of existing CCTV cameras to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

5 Use of CCTV

5.1 Reasons for the use of CCTV

MWH may use CCTV at our premises as outlined below. We believe that such use is necessary for legitimate business purposes, including:

- to prevent crime and protect buildings and assets from damage, disruption, vandalism, and other crime,
- for the personal safety of staff, visitors, and other members of the public and to act as a deterrent against crime,
- to support law enforcement bodies in the prevention, detection and prosecution of crime,
- to assist in day-to-day management, including ensuring the health and safety of staff and others,
- to assist in the effective resolution of disputes which arise during disciplinary or grievance proceedings.

This list is not exhaustive and other purposes may be or become relevant.

5.2 Monitoring

Usually, CCTV monitors the exterior of buildings 24 hours a day and this data is continuously recorded. In some cases, CCTV may also be used internally, for example in reception areas or at entrance doors.

Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property.

Images are monitored by authorised personnel. Any Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

5.3 How we will operate any CCTV

We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters. Recorded images will only be viewed in designated, secure locations.

5.4 Use of data gathered by CCTV

To ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

For further information please see the MP28 Data Protection Policy.

5.5 Retention and erasure of data gathered by CCTV

Data recorded by the CCTV system will be stored digitally using a cloud computing system. Data from CCTV cameras will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded.

At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

5.6 CCTV used on construction equipment

Most modern construction plant, for example excavators and cranes, comes equipped with CCTV as a safety feature. These systems are owned and operated by the plant hire

company who will have their own procedures relating to how the recordings will be handled.

In the event of an incident, MWH may request copies of any CCTV data to aid in the investigation. Where this is the case the copies of the footage will be treated in compliance with MWH data protection policies.

6 Use of additional surveillance systems

Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a data protection impact assessment (DPIA).

A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. We will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

7 Requests for disclosure

We may share data with other RSK Group members where we consider that this is reasonably necessary for any of the legitimate purposes set out above in paragraph 5.

No images from our CCTV cameras will be disclosed to any third party, without express permission being given by the Data Protection Officer. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

We will maintain a record of all disclosures of CCTV footage.

No images from CCTV will ever be posted online or disclosed to the media.

8 Complaints

If any member of staff or visitor has any concerns about our use of CCTV, they should speak to the senior member of staff at the location in the first instance.

Where this is not appropriate, or matters cannot be resolved informally, employees and visitors should contact the HR team or the Data Protection Officer.

9 Personal data protection

As with all personally identifiable information, CCTV images fall within the Data Protection Act (2018). MWH will respect the rights of data subjects and process any access requests in accordance with our normal procedures.

9.1 Subject access requests

Data subjects may make a request for disclosure of their personal information, which may include CCTV images. A data subject access request is subject to the statutory conditions in place at the time and should be made in writing to the HR team in the first instance.

For us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

Where we consider it necessary to do so, we reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, to protect the privacy rights of other individuals.

9.2 Requests to prevent processing

We recognise that, in rare circumstances, individuals may have a legal right to request erasure of personal data concerning them or to restrict the processing of their personal data. Any member of staff who considers that these rights apply to them in relation to our use of CCTV should speak to the HR team in the first instance.

10 Changes to this policy

We keep this policy under regular review and reserve the right to change it at any time. This policy does not override any applicable national data privacy laws and regulations.

11 Contact Information

In the first instance any enquiries should be directed to the HR team who can be contacted at HRCentralServices@mwhtreatment.com or on 01706 367555.

The Data Protection Officer can be contacted at privacy@mwhtreatment.com.

12 Definitions

For the purposes of this policy:

CCTV means fixed and domed cameras designed to capture and record images of individuals and property.

Controllers are the people who, or organisations which, determine the way any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. We are the controller of all personal data used in our business for our own commercial purposes.

Data is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data subjects means all living individuals about whom we hold personal information because of the operation of our CCTV (or other surveillance systems).

Data users are those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy.

Personal data means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

Processing is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

Processors are any person or organisation that is not a data user (or other employee of a controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

Surveillance systems means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.