Digital Recordings Policy

Policy

1. Introduction

1.1 In accordance with the IVH Data Governance Policy, Irwell Valley Homes (IVH) accepts that it is a controller and processor of personal data about, but not limited to, its colleagues and customers and carers, who all have a legitimate expectation the organisation will process their data appropriately. Through its policies and procedures, IVH is expected to remain complaint with the Data Protection Act (the Act), UK GDPR, and any other data-related legislation. Processing includes the capture, collection, storage, and management of still and moving images and audio recordings of/about people or additional data from which information about them can be derived e.g., biometric data, automated number plate recognition (ANPR), or workplace monitoring systems etc.

2. Purposes of data capture

2.1 IVH captures images and audio in and around its schemes and other buildings, or of people used in IVH social media or promotional material. Any digital recordings which contain a living person remains personal data about that person (the 'data subject'). The purpose of this policy is to set out how we operate recording capture technology then store and manage the resulting images and audio to ensure they comply with the IVH Data Governance Policy.

2.2 IVH may seek to capture still or moving images or audio of buildings, rooms, structures, or land for asset management, security, promotional, or development purposes. A range of technology may be used to capture this data, including: -

- Ceiling/post/wall-mounted closed-circuit television (CCTV) cameras
- Doorbell image and sound-capturing devices
- Digital cameras/camcorders
- "Go-pro"-type products/technology.
- Cameras within mobile phones
- Hand-held video or audio recording devices
- Computer mounted/incorporated cameras.
- Drone technology with mounted cameras
- Telephone/communications technology
- Body-worn video used for safety/security reasons.

2.3 While undertaking work for IVH, and unless approved by the IVH IT Team, colleagues shall not use personal/non-IVH devices for capturing images and audio and shall not store IVH-captured images and audio on personal/non-IVH devices, in personal file areas, or non-IVH social media/email accounts.

2.4 Images and audio intentionally capturing/recording people for social media or promotional materials should only be done so with the consent of the data subject as per the IVH Data Governance Policy.

2.5 Images and audio intentionally capturing/recording property or land to assist development, repairs, or property improvements (including cleaning or clearing for the safety of people) should avoid the inclusion of people. They should be retained as a component of a property file and subject to the retention period of that file. Images and audio of data subjects without consent or expired consent shall be deleted by the colleague capturing the image or automatically by IT systems and, if required, re-taken with no persons present.

2.6 CCTV is intrusive and will only be used by IVH to assist with the prevention / detection of crime, the apprehension / prosecution of offenders ('Criminal Justice Purposes') by law enforcement services, and for the protection of people and property.

2.7 IVH does not independently engage or initiate in covert surveillance techniques or technology, and only processes data in this way on case-by-case basis and in cooperation with law enforcement and intelligence services when required.

3. Data protection impact assessment

3.1 IVH will adopt a 'privacy by design' approach when installing or adopting new image and audio capturing technology and software. This will involve conducting a 'Data Protection Impact Assessment' (DPIA) prior to deployment to ensure that the proposed installation is compliant with the IVH Data Governance Policy and relevant guidance.

3.2 The Checklist at appendix B of this document is suitable as a DPIA for cameras and, once completed, should be submitted to the Risk & Assurance Team for logging.

4. Siting of cameras

4.1 All overt cameras, including mobile, permanent, or temporary cameras, and data-capturing doorbell devices, will be sited in such a way as to meet the purposes for which the device is operated. Signage warning of the presence of cameras will be sited in prominent positions where they are clearly visible to colleagues, customers, and others to inform individuals that they are in an area with a camera operating, including on IVH vehicles/vans.

4.2 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. IVH will make all reasonable efforts to ensure that areas outside of IVH premises are not recorded.

4.3 Cameras may be in communal areas of properties. Where this is the case, colleagues, customers, and others will be made aware via appropriate signage and if necessary, by other means such as informing them directly.

4.4 Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as toilets.

5. Siting of cameras by customers

5.1 The decision to use cameras or data-capturing doorbell devices for their own personal and household activities remains with customers. However, customers are expected to consult and seek permission from IVH before any installation works are undertaken that affect the physical fabric of IVH-owned properties.

5.2 IVH has no control over such devices and the use of resulting data by customers and property co-habitants. When they enquire, IVH will advise customers that they (and not IVH) will be the data controller and subject to data protection legislation, including the UK GDPR, where recordings capture anything past their private property, alleviating IVH of any responsibility regarding the data. To further inform them, customers may be directed to the ICO guidance: - https://ico.org.uk/for-the-public/domestic-cctv-systems/

6. Storage and retention of data

6.1 Any images and/or audio recorded by IVH systems will be retained in accordance with the IVH Data Governance Policy Data Retention Schedule available on the IVH intranet.

6.2 In accordance with a DPIA, IVH will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

- Data subjects will be made aware, by signage or verbally, that images and audio are being captured of them.
- Any decision to reposition cameras will have to be authorised by the Homes or Asset Management Team who may seek support from the Risk & Assurance Team and/or IT Team for further regulatory or technical advice.
- Data storage systems being encrypted, or password protected, and footage access / extraction only permitted by authorised IVH colleagues, and physically and digitally located in restricted areas.
- A log shall be maintained by relevant colleagues of (at least) camera location, data storage details, positioning changes, persons authorised to access, and any access to footage, including time and dates of access, and a record of colleagues accessing the images and when.
- Where people are directly approached to obtain their image or audio data, consent will be obtained in advance from data subjects in accordance with the IVH Data Governance Policy unless images are subject to exemption as per the policy.
- As per policy, images and audio will only be used for their intended purpose and consent may be withdrawn by the data subject at any time. If data subjects are colleagues, they will be reminded as they exit IVH that they may withdraw such consent (and may still do so after exiting IVH).
- Where advanced specialist technology is used (e.g., drones, ANPR etc.), colleagues will provide evidence that they are appropriately trained in its use and understand data protection implications, recording these in a DPIA.
- The Risk & Assurance Team shall review the data processing logs, including DPIAs, annually.

7. Recording of colleagues by customers

7.1 People may create recordings (images or audio) purely for their own personal and household activities, and these are not subject to the Act or UK GDPR.

7.2 If they were to use or share these recordings for a purpose outside of their own personal and household activities, then those individuals may become subject to the Act and UK GDPR.

7.3 It is difficult to determine whether the purpose for which they might use recordings would be beyond the context of purely personal or household activities and within the boundaries of private property, and this would need to be considered on a case-by-case basis with support from the Risk & Assurance Team.

7.4 To protect colleagues from pressured work environment, if people are seen to be recording colleagues while they are at work and without consent, regardless of how the recording may be used in future, colleagues may: -

- ask the customer why they are seeking to make a recording,
- politely advise the person to cease recording by switching off equipment or them moving to another room on the property,
- leave and arrange a new appointment when a recording will not take place or, if on IVH premises, colleagues may ask the person to cease and/or leave,
- request any recordings posted on public social media be removed and reserve the right to report these to the ICO as a data breach,
- record the event on the housing management system and report as per a H&S event.

These incidents must be recorded on the IVH housing management system customer record and reported to the Risk & Assurance Team, who may engage with the customer and the ICO in support of colleagues.

7.5 To discourage customers from making recordings IVH will not accept or seek to view or hear recordings made without the consent of a colleague. However, if a formal complaint leads to a tribunal in connection with gross misconduct, then the tribunal may decide to accept such a recording as evidence, to be determined by the tribunal on a case-by-case basis.

7.6 Recordings of colleagues that allege criminal behaviour would be a matter for law enforcement or intelligence service and fall outside of IVH responsibilities.

8. Recording of colleagues by colleagues

8.1 Colleagues are not permitted to covertly record IVH-related meetings and conversations with other colleagues, either informal or formal, at work on either their work and/or personal mobile devices or laptops. This also includes recording meetings held through video conferencing and the recording of telephone conversations. Covert filming or audio recording will be regarded as a potential disciplinary offence. Any recording should only take place with agreed prior consent, and it must be done overtly and in advance.

8.2 Recording of internal meetings or other activities while video conferencing using MS Teams/Zoom/recording equipment by colleagues for convenience, note-taking, or training purposes can only be captured with the consent of data subjects and retained for an agreed period before deletion, using a shared privacy statement (appendix A).

8.3 If it is intended to record a meeting, the meeting organiser/chair must notify participants in advance and confirm how the recording will be used. At the start of the meeting or activity, the meeting organiser/ chair should request permission of those present before recording starts and display a privacy statement. All meeting participants will be automatically alerted at the start of the recording. Such recordings should not be shared outside of IVH without further explicit consent from all participants and taking advice from the Risk & Assurance Team. Colleagues retain the same UK GDPR rights to access, review, complain, seek information on, and seek deletion etc. as all data subjects.

9. Subject Access Requests

9.1 Images and audio of data subjects remain personal data, subject to the same rights as they would with other personal data e.g., a text document. These include right of access i.e., a Subject Access Request (SAR). Any request by a data subject for the images or audio of themselves will be dealt with in accordance with IVH's SAR procedures.

9.2 When a SAR is made, the Risk & Assurance Team will review the data in question and redact or anonymize where required.

9.3 If the images and/or audio contain only the data subject making the request, then those images and/or audio will most likely be extracted and placed on a suitable medium which can be sent securely to them e.g., via a secure file transfer portal, or an IVH memory stick which is capable of being encrypted. Alternatively, the data subject may be permitted to attend IVH offices and personally view/hear the footage if they prefer. This must be strictly limited to images and audio which contain only the data subject.

9.4 If the images and/or audio also contain other individuals, and IVH does not possess the ability to obscure those parts of the images and/or audio, then the Risk & Assurance Team must decide whether those images should be disclosed, considering whether:

- The other individuals in the footage have consented to the disclosure of the footage.
- It is otherwise reasonable in the circumstances to disclose the footage without the other individuals' consent.
- If consent has not been obtained or it is not reasonable in the circumstances to disclose without consent, then the footage can be lawfully withheld.

9.5 The Risk & Assurance Team must also consider whether any other UK GDPR exemptions may apply (see IVH Data Governance Policy for further details).

10. Disclosure of data to third parties

10.1 IVH will only disclose images and/or audio to third parties where it is permitted to do so in accordance with the IVH Data Governance Policy, with written evidence of the request being retained (whether disclosed or not) and using secure methods for transmitting the information.

11. Misuse of image capture technology or data

11.1 Misuse of personal data is a serious matter which may lead to severe consequences for both individual colleagues and IVH due to potential regulatory action by the ICO and reputational damage.

11.2 Any colleague who breaches this policy may be subject to disciplinary action in accordance with relevant policy and procedures.

Responsibilities

12. Responsibilities

12.1 The Head of Finance, Risk and Assurance is primarily responsible for the effective implementation, review and any updating required of this policy.

12.2 The Data Protection Officer (DPO) is responsible maintaining and monitoring the effectiveness and lawfulness of this policy against data protection legislation. Colleagues must consult the Risk & Assurance Team if they are uncertain about any aspect of this policy or related guidance.

12.3 The Head of People has operational responsibility for colleague welfare and is responsible for monitoring colleague awareness. Additionally, providing support on disciplinary process where recordings may be considered for viewing/hearing.

12.4 Managers are responsible for ensuring that all team members are aware of this policy and principles and support in those instances where a member of their team suspects they are being recorded.

12.5 All colleagues have a duty to make sure that they understand their role in the effective application of this policy.

12.6 Contractors and consultants, who are directly engaged by the organisation should be made aware of this policy by IVH contract managers.

12.7 Anyone who has concerns about this policy should seek guidance from the Risk & Assurance Team for clarity.

12.8 All aspects of the policy and its implementation will be accountable to the IVH Board.

Performance Indicators/Targets/Standards

13. Performance indicators

13.1 Breaches of this policy will be regarded as Personal Data Security Incidents (PDSIs) and reported to the Risk & Assurance Team who will investigate. The data will be reported in aggregate and by theme to the Audit & Risk Committee by way of the quarterly Combined Assurance Framework (CAF) report and monitored against PDSI aggregates for the same period in the previous year, explaining any significant increase.

13.2 Any escalation of data breaches to the ICO will also be considered a breach of the governance risk appetite trigger and reported to the Audit & Risk Committee via the CAF.

Equality, Diversity and Inclusion Implications

14. EDI implications

14.1 IVH is committed to treating people with honesty, dignity, respect, and trust. This applies to colleagues, customers, potential customers, contractors, and Board Members. At IVH:

- Equality is about ensuring that every individual has an opportunity to make the most of their lives and talents.
- Diversity is recognising difference and responding positively to those differences; and
- Inclusion is about creating an environment where our services and employment opportunities are accessible to all.

14.2 IVH will be mindful of the Equality Act 2010 in all its actions and will consider all the protected characteristics of the Act which are: Race, Sex, Gender Reassignment, Disability, Sexual Orientation, Religion or Belief, Age, Marriage/Civil Partnership and Pregnancy and Maternity explicitly. Further to the protected characteristics, IVH will be mindful of socio-economic disadvantage and will do everything in its power to minimise this and other forms of disadvantage.

14.3 Circumstances may arise where protected characteristics or specialist categories are collected and processed to the benefit and safety of the data subjects. This will be subject to an assessment and guidance from the Risk & Assurance Team and the consent of the data subjects, which they may withdraw at any time.

15. Cross Reference

15.1 This policy should be read with the following documents and legislation: -

- IVH Data Governance Policy.
- ICO Guide to UK GDPR.
- 'In the picture: A data protection code of practice for surveillance cameras and personal information' – ICO CCTV Code of Practice.
- 'Surveillance Camera Code of Practice' - issued under Protection of Freedoms Act 2012
- Data protection impact assessments (guidance for carrying out a data protection impact assessment on surveillance camera systems) ICO/Surveillance Camera Commissioner
- Drones: how to fly them safely and legally (https://www.gov.uk/government/news/drones-are-you-flying-yours-safely-and-legally)
- The UK General Data Protection Regulation.
- The Data Protection Act 2018.
- Protection of Freedoms Act 2012.
- The Human Rights Act 1998.
- The EU Charter of Fundamental Rights

Privacy notice for Video Conferencing and Communication

Updated October 2023

IVH provides IT systems as a part of its normal business and may require colleagues, customers, and other stakeholders to use its IT systems during their relationship with IVH. This may require the use of video conferencing and communication where this is convenient.

Video conferencing may create a recording that may collect the following information: Host and participant names, start and end times, locations, images, voices, telephone numbers and other contact details, participant IP addresses and device/hardware information, audio transcripts, and message/chat logs. IVH would not routinely require any special categories of personal data in the use of video conferencing and communication. However, we may have such information if it is provided to us directly, for example so we can make appropriate adjustments for a disability.

Data controller: IVH will be the data controller for that information and software companies providing access to the video conferencing and communication are acting as data processors.

Consent: By engaging with the video conference, participants are consenting to the recording of the meeting/conference, have seen this privacy notice, and reserve the right to decline.

Processing: To be made clear verbally by the organiser prior to recording starting, the recording may be used for: -

1. notetaking after the meeting to ensure an accurate record and will be deleted by the host/organiser or their secretary/administrative support once any minutes or notes have been documented.
2. a record to be shared with people who were unable or unwilling to attend at the time yet will benefit from observing.

The recording will not be shared externally or uploaded to any social media without further consent by the participants, who may decline and seek redaction as per their rights. Depending on the topic/content of the recording, the recording will be retained in accordance with the IVH data retention schedule or deleted within 30 days by the meeting organiser.

Legal basis for processing: IVH requires its stakeholders to use its IT systems during their relationship with the business. The processing is therefore necessary for the performance of a contract to which the data subject is party, potentially at times where there may be the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Some IVH activities are wholly reliant on the provision IT systems, and it would not be able to fulfil its obligations without them.

Your rights: If participants wish to update, access, erase, limit the use of information, or complain about the use of their information please contact the IVH Data Protection Officer in the first instance by emailing information.governance@irwellvalley.co.uk. You may also wish to contact the Information Commissioner's Office.

Digital Recordings Policy Appendix B

CCTV/Digital Recording Checklist

CCTV is necessary for the prevention and detection of crime and for protecting the safety of individuals, or the security of premises. The system will not be used for any incompatible purposes and regular reviews will be conducted of the use of CCTV to ensure that it is still necessary and proportionate.

The system may process footage of identifiable individuals and is processing personal data and Irwell Valley Homes is registered as a controller and submitted a relevant data protection fee to the Information Commissioner's Office (ICO) and renews annually. Irwell Valley Homes has identified and documented an appropriate lawful basis for using the system, taking into consideration Article(s) 6, 9 and 10 of the UK GDPR and relevant Schedules of the DPA 2018. This checklist forms a part of the Digital Recording Policy and should be read in conjunction with the Data Governance Policy.

The system should produce clear images which we can easily disclose to authorised third parties, e.g., law enforcement bodies (usually the police) require access to investigate a crime. The Risk & Assurance Team will support colleagues with any requests for data from law enforcement or intelligence services and requests will be accepted in a documented form.

The cameras are positioned in such a way to avoid any unintentional capture of non-IVH land or individuals not visiting the premises.

There are visible signs showing that CCTV is in operation. Contact details are displayed on the sign(s) if it is not obvious who is responsible for the system. Data subjects may access the IVH privacy statement on its website https://www.irwellvalley.co.uk/privacy-notice/

IVH securely stores images from this system for a defined period as documented in the IVH retention schedule and only a limited number of authorised individuals may have access to them. Recorded images may be saved to the housing management system or as part of an investigation and be re-defined, altering the retention period.

Individuals making data subject requests will be directed to the Risk & Assurance Team for action.

CCTV/Digital Recordings will be subject to annual audit to monitor compliance with this checklist including the number and success of: -

- personal data breaches
- complaints
- subject access requests
- requests from law enforcement or intelligence services
- technical failures or malfunctions
- cyber-attacks
- retention failures

Ask for a word version of the spreadsheet on the next page, complete it, and submit to the Risk & Assurance Administrator using via information.governance@irwellvalley.co.uk

Digital Recordings Policy Appendix B

Scheme and address of IVH cameras:											
Describe the context of the site requiring surveillance:											
Why do we have/need cameras?											
Is this a new deployment, an expansion of current systems, replacement, or refresh/review of current?											
Who will the cameras capture (customers, public, colleagues, contractors, children, vulnerable groups)?											
Location of cameras on site	fixed camera make / model / serial no	re-deployable camera make / model / serial no	Drone make / model / serial no	Stand-alone video camera make / model / serial no	ANPR make / model / serial no	Motion capture or continuous recording?	Body Worn make / model / serial no	Audio Y/N	Night vision Y/N	Facial recognition Y/N	What spaces are the cameras looking at?
Camera 1:											
Camera 2:											
Camera 3:											
Camera 4:											
Camera 5:											
Camera 6:											
Camera 7:											
Camera 8:											
Camera 9:											
Camera 10:											
Camera 11:											
Camera 12:											
Camera 13:											
Camera 14:											
NB: if you attach a diagram of the layout, please reference.											
Installer(s)											
Software suppliers (if applicable)											
Signage location 1											
Signage location 2											
Signage location 3											
Signage location 4											
Signage location 5											
Signage location 6											

How clear is the footage?	Full body and clothing (clear/unclear)	People's faces (clear/unclear)	Small/hand-held items (clear/unclear)	Car makes or models (clear/unclear)	Car registration (clear/unclear)	Colours (Y/N)	

Is the footage date and timestamped? (Y/N)
How/where is the footage stored?
How do we ensure the security and integrity of the data?

Digital Recordings Policy Appendix B

How long is the footage stored for? NB: retention period is usually 30 days
How is the footage disposed of?
Who/which colleague(s) will be making decisions about the uses of the system and which other parties are likely to be involved?
Who has access to the footage? (name(s) & role)
How is footage accessed?
What security is in place for the stored footage?
Can we redact/blur out 3rd party images/data? (Y/N)
How is it used?
Monitored in real time to detect and respond to unlawful activities (Y/N)
Monitored in real time to track suspicious persons/activity (Y/N)
Compared with reference data of persons of interest through processing of biometric data, such as facial recognition (Y/N)
Compared with reference data for vehicles of interest through ANPR software (Y/N)
Linked to sensory technology (Y/N)
Used to search for vulnerable persons (Y/N)
Used to search for wanted persons (Y/N)
Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies (Y/N)
Recorded data disclosed to authorised agencies to provide intelligence (Y/N)
Other (please specify)
Please insert a diagram (if you have one) referencing the location of cameras and signage