Closed Circuit Television (CCTV) Procedure

1. Aim and scope of procedure

We own and process Closed Circuit Television (CCTV) for the following purposes:

- Investigating cases of anti-social behaviour
- For the safety of our staff and customers.
- Identifying and investigate any alleged crime or incident and in the defence of civil claims.
- To protect our properties and assets.
- For crime reduction, prevention and detection purposes

This procedure outlines how we use, manage and where applicable, appropriately disclose to authorised persons or authorities. We will manage the CCTV footage and recordings in line with our data protection obligations.

This procedure also sets out our position in relation to customers' own CCTV.

2. Procedure

Location of CCTV equipment:

CCTV equipment are located at some of our properties and offices. For more information about where we have CCTV please contact the Governance Team.

We are legally required to provide notification to individuals (whether members of staff, customers, or the public) if they are in an area where CCTV surveillance is being carried out. The area covered by CCTV must have sufficient signage to alert individuals to the use of CCTV, to provide our contact information as well as telling them why these cameras are in place. The signs must be visible and maintained.

Prior to installing any CCTV, you must undertake a data protection impact assessment (DPIA) to understand the impact of the technology used (pan, tilt, zoom camera, focus, range, quality, runtime, overwrite functionality, Wi-Fi security just to name a few) to ensure that we remain compliant with data protection laws and other applicable legislation or standards. The Surveillance Camera Commissioner has published useful guidelines to follow for best practice purposes.

Retention of CCTV footages:

CCTV footage and recordings are kept for a limited amount of time, each individual digital video recorder (DVR) has a set retention where after this period they are securely deleted or overwritten.

Any footage required for dealing with a complaint, a police investigation or court case can be retained for 6 months. If recordings are needed for longer than 6 months, the Governance team should be notified, and the decision must be recorded.

Who can access and share CCTV:

We have Nominated Persons (NP's) who can access and share CCTV, they are:

- Tenancy Enforcement Officers/ Tenancy Enforcement Manager
- People Business Partners (ONLY FOR HR related requests)
- Information Governance Manager
- Insurance Manager
- Fleet Manager
- Facilities Manager

Each of the above must have their own confidential folder which can be accessed by the Information Governance Manager, where they store a CCTV log. Each request will have its own subfolder which contains relevant details of the CCTV being accessed and why.

Requests usually come from other agencies, namely the Police. There can also be internal requests from Tenancy Enforcement Officers and from Neighbourhood Officers for the purposes of collecting evidence of ASB and for estate management, such as fly tipping or damage in communal aeras.

NP's can also show the footage or still images to parties involved for the purposes of identifying parties within the footage. They should consult the Information Governance Manager if they are unsure whether this is appropriate. If it's appropriate to show other parties the footage, the decision to do so should be documented and the viewer should sign a disclaimer that if they recognise anyone in the footage, they will not take matters into their own hands.

Anyone other than the Nominated People above that want to request CCTV must seek approval from the Information Governance Manager.

Once a request is received it should be passed to a NP (if it wasn't received by them), the NP must raise a CCTV request case on OpenHousing and provide the following information:

- Address/premises
- Which cameras
- Date and time to be recovered

If a DP2 was received this should be uploaded to the case images.

Once the task is complete, it'll raise the repairs email and you'll receive a notification email with a tracking number.

Once you have the job number, you'll need to answer the following 3 questions

- What is the repairs job number?
- Job priority code?
- Is it a Schedule 2 Offence?

The NP will then need to confirm with the requesting party that the request has been received and actioned where necessary.

CCTV Footage will be downloaded at the site by the Access and Security Engineer and uploaded to the relevant team channel for the NP to view and release where necessary.

If Access and Security Engineer are unable to recover footage, they must inform the NP with an explanation (if this is the case the case on OpenHousing and spread sheet must be updated).

The NP will record their decision whether to approve or reject the request by completing the last stage of the OpenHousing case and organise the release of the CCTV if applicable.

Releasing CCTV:
The NP will contact the requesting person / organisation to advise that the CCTV is ready to be collected. The NP must inform them that they will need to bring a secure portable storage device to upload the CCTV footage onto - we will not provide any USB/CD. The NP will book a time for this to happen as they will need to be present. Alternatively, CCTV can be shared via an approved system, such as the police's video sharing stream.

The CCTV case, log file and spreadsheet is to be updated and closed.

If the CCTV is not released, then the NP must delete the footage

Schedule 2a offences – if the incident requested on the DP2 is serious, footage can be released to the police without viewing it first. Tenancy Enforcement Officers hold current lists of what incidents are deemed serious and must approve the footage can be released without viewing first. Examples of serious incidents are listed in the ASB Crime and Policing Act 2014 and include murder, rape, serious road traffic accidents and use of offensive weapons.

The NP is responsible for the decisions associated with the management of the CCTV request(s) they are handling. Guidance and support is available from the Tenancy Enforcement Manager and/or the Information Governance Manager.

The Information Governance Manager will review the NPs logs periodically to ensure the procedure is being followed.

3. Customers' CCTV

General principles
Some customers feel strongly that they would like to install CCTV for their own safety and security. Other customers feel that CCTV is a breach of their privacy.

Privacy is a civil matter and VIVID will not become involved in disputes over customers' CCTV installations. CCTV installations will not be classed as anti-social behaviour. However, if there is a disagreement over CCTV, VIVID may refer the matter to Assessment or mediation, which are services run by an independent organisation which helps customers resolve their differences.

Permission for CCTV

Customers are not required to request permission for CCTV unless there is a clause in their tenancy relating to permission for installations. Any permission granted will be for the physical installation, such as making sure it is installed in safely and not in breach of any planning regulations, for example. VIVID will not grant or refuse permission to customers to use CCTV.

Advice for Customers
We advise customers to check with the Office of the Information Commissioner before considering installing CCTV and to follow any advice and guidance issued by this organisation.

If residents are unhappy with another customer's CCTV, they should seek their own legal advice, or get free advice by contacting the Citizens Advice Bureau or the Information Commissioner's Office.

Related Documents:
Data Protection Policy
Data Protection Impact Assessment (DPIA)

Author	Owner	Date approved	Review date
Lauren Cannon	Head of Governance	May 2021	May 2022