Body Worn Video Camera (BWVC) Policy

Table of contents

1. Purpose

1.1 The purpose of this policy is to regulate the management, operation and use of Body Worn Video Camera (BWVC) systems across RelyOn.

1.2 RelyOn has produced this policy in line with the Information Commissioner's Office (ICO) CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice, which includes the use of BWVC.

1.3 When used effectively a BWVC allows person audio and visual images to be captured to provide a clear and irrefutable record of events. With proper use the introduction of this technology will assist with:

- Allowing for more detailed examination of the events leading up to and management of incidents.
- Enhance evidence capture.
- Promoting positive behaviour and interaction between staff and the public.

2. The use of BWVC within RelyOn

The use of BWVC within the RelyOn must adhere to the ICO Code of Practice for surveillance cameras and personal information.

2.1 Review of Local Security Strategies (LSS)

- RelyOn must ensure that they review their Local Security Strategies (LSS) to ensure they are in accordance with the instructions set out in this Policy Framework.
- RelyOn must ensure that contingency plans and incident management are reviewed to include the necessity to secure all digital footage promptly.
- RelyOn must ensure robust management of the BWVC equipment, system and data management, including have sufficient and competent local resource for the system management identified roles within the policy guidance (such as Administrator, Approval Officer, System Owner).

3 Camera Operation

RelyOn must ensure that the capabilities of BWVC equipment are clear to staff, and the public. This signage must include its ability to capture audio as well as visual imagery. Procurement can assist with procuring the signage as required.

Officers must complete the required training and understand the principles on use of BWVC equipment within 90 days of first drawing a camera.

As a minimum all operational staff must collect a camera from the camera docking station at the beginning of their shift. When removed from the camera docking station the camera will enter 'stand-by' mode and commence a 'pre-record' function, the footage captured by 'pre-record' will only be saved when camera recording is activated by the user.

When removed from the camera docking station the camera will enter 'stand-by' mode and commence a 'pre-record' function, the footage captured by 'prerecord' will only be saved when camera recording is activated by the user.

When worn, BWVC must be turned on and set in the pre-record mode. An officer can record an event immediately through touch activation of the record button. In pre-record mode BWVC records on a rolling buffer. When the camera is activated by the operator, video and sound recording starts and automatically includes the back-captured buffer video.

Where RelyOn consider it necessary and proportionate to deploy BWVC's to other roles, including none-operational roles, within their establishment, where there are sufficient surplus cameras available, the rationale for deployment of BWVC should be recorded within the controlled Relyon document.

3.1 Point to start recording

Officers should start to record as early as possible. Officers should make a verbal announcement that they are recording to ensure those captured by the camera lens/microphone are aware they are now being recorded.

All users must be reminded that the use of BWVC footage is to support and not replace written statements.

3.2 During recording

The Security Officers must always ensure that BWVC is only used as an overt audio or overt visual recording mechanism and is not intentionally used covertly. BWVC are designed to operate with notifications (such as lights, beeps, and physical vibrations) so that both officers, and the public are aware that a camera is present and may be recording audio and images.

Upon activating their BWVC, officers must make a clear verbal announcement to anyone in the vicinity that the recording of both audio and visual images is taking place. This must take place as soon as it is possible and safe to do so. If the BWVC is activated prior to arriving at the scene of an incident, then the announcement must be made to those at the scene once it is possible and safe to do so. An agreed establishment wide standard form of words covering these points can be adopted for continuity purposes. For example: for your safety and the safety of others you need to be aware that everything you say and do will be recorded.

Recording must, where practicable, be restricted to those individuals and areas that are necessary to record to obtain material relevant to the incident or event. It is important that users minimise the risk of collateral intrusion on those not involved in the incident wherever possible. However, and importantly, this must not be at the expense of failing to obtain enough coverage of the incident/event or restricting the user's movements and ability to manage the incident.

The use of BWVC in areas where there is a higher than usual expectation of privacy (such as toilets, showers, changing rooms, search areas and medical treatment rooms), will require compelling reasons for doing so, for example in response to an incident where the safety or security of others is at risk. Where footage is recorded in these areas' consideration should be given to placing restrictions on viewing the recording or pixilating the recording at the earliest opportunity (see pixilation section).

Officers will be further aware of the sensitivity of using BWVC in places of worship where this may be viewed as disrespectful and will require compelling reasons for doing so, for example in response to an incident where the safety or security of others is at risk.

Any footage or recording must generally be uninterrupted from the beginning of the incident until the end.

Where incidents or events are protracted and there are lengthy periods of inactivity or because of the need to isolate confidential details such as victim details or witness details from the footage, there may be cause to conduct selective filming. Users should be aware that this could lead to challenge and must ensure that explanation and justification is given for selective recording in the accompanying documents. If using selective recording due to inactivity and where multiple BWVC are available users should consider having one camera continuing to record whilst others stop recording and explain their rationale for using selective recording on camera before switching any camera off.

3.3 Cessation of Recording

In the same way that an officer will record their decision to activate BWVC so too will the decision to cease recording be documented. In making this decision users must be satisfied that the risk of not capturing further helpful material is minimised.

Under normal circumstances officers must cease recording either when It is no longer justifiable, necessary, or proportionate to continue recording.

3.4 Post Recording

The Security Officers will at the end of their duty return the BWVC to the docking station.

Post incident/event users will complete supporting documentation in the form of Use of Force, Incident report, Intelligence report or adjudication paperwork or digital tools in the usual way and indicate whether BWVC was activated.

Post incident/event line managers must ensure that when recording an incident on the Incident Report System at Relyon (IRS) that the presence of BWVC footage is recorded within the report. Additionally, the presence of BWVC footage should be noted in any resulting Intelligence Report - BWVC will be used to corroborate and not replace evidence from other sources.

Where more than one BWVC is present at the scene of an incident, or the area is also covered by CCTV the system administrator and designated Approval Officer must ensure that all available material of the incident is secured as evidence in anticipation of any defence argument that may be presented.

All BWVC material should be uploaded on to the secure shared server as soon as practicably possible; this is completed automatically when the camera is placed in the docking station and will ensure that the audio and visual data is secure.

The Security Officers must justify their actions, perceptions, and decisions as per normal within their written Use of Force (UoF) statement. The writing of UoF statements must be completed before any captured footage is viewed, this will enable staff to detail the threat perceived at the time of the incident and not on reflection having viewed any footage. Officers must reference BWVC footage was captured within the UoF statement. The use of BWVC is a tool to support and not replace written statements. If footage is viewed following the writing of the UoF statement and the user wishes to make a further statement, this can be provided as an addendum to the original statement, clearly stating this is being provided following viewing the footage.

3.5 Deletion of unintentional recordings

A BWVC user may unintentionally record footage of no evidentiary value by inadvertently activating the BWVC record button, or by forgetting to return a BWVC to standby mode following an incident which required camera activation.

If a Security Officer becomes aware that they have unintentionally recorded something, then they must notify their line manager. The line manager will submit a Request for deletion / amendment of body-worn video recording form to the local system administrator for review. If the local system administrator agrees that a recording should be deleted, they should record the deletion on the BWVC data retention log and attach a copy of the request form to the retention log.

3.6 Partial recording

If the Security Officers attend an incident and are recording the scene or any part of the incident/location using BWVC then the entire incident should be recorded unless there are exceptional reasons not to do so or a manager instructs them to stop filming. The reasoning for ceasing to record should be captured on camera before the recording is stopped.

3.7 Transcripts

Where a transcript is produced it should be treated as evidence and handled in accordance with evidence handling processes for the establishment and relevant policy framework, the accompanying footage will be retained, and a note made on the retention log cross referencing the details of the transcript.

3.8 Dealing with objections to being filmed

Any objection by the public or other person to the use of BWVC to record, must be addressed by the BWVC user with a clear and concise explanation why recording is taking place. The user must explain the benefits of recording the encounter, which may include explaining that the recording is to safeguard all parties by ensuring an accurate reflection of any action or comments made by either party. Where the objection is within the establishment users may also direct visitors to the signage which explains that BWVC/CCTV is used in the establishment and in the case of a complaint advise to write to the RelyOn.

The Security Officer may also explain that non-evidential material is only retained for a maximum period of 90 days and that any access to the material is both limited and controlled; BWVC material is restricted and any disclosure of personal information in relation to the public must not be disclosed even to close relatives without consent. In the event of disclosure to third parties, (such as the police or courts, this would be in line with the Data Protection Act 2018 (DPA). Further guidance can be found in Information Requests Policy Framework.

If the member of public continues to object, then the officer must decide, based on the circumstances, of the incident or event. Stop filming at the request of the person would however be an exceptional occurrence and the normal policy would be to continue to film and to record the persons objections on film and within the accompanying written document.

Where such footage contains intimate body parts, consideration must be given to pixilation of the footage where there is a need for copies to be made or for it to be made available for viewing (such as part of an adjudication). It is important that the master copy remains "unchanged" on the system. Please consult the redaction / pixilation section of this guidance for further information.

If at any time the officer considers it inappropriate to continue to record specific events the officer could take the decision to end recording and in doing so explain verbally before the recording is stopped. The officer must then also record the rationale for the decision in the accompanying paperwork/report.

Equally Security Officers may be approached by a person with a request to film an encounter or situation. It is for the officer to decide if this is appropriate and consider the reasons for the request, however there should be a presumption in favour of doing so. The officer's decision will be explained to the person. If they do refuse to switch the camera on, then BWVC officers must log the refused request using the system in place at the individual establishment and submit an Intelligence Report.

4 Professional Standards

Users should not intentionally obscure the camera lens or fail to record all or part of an incident without exceptional cause/justification. RelyOn may wish to consider whether an obvious and intentional action, including the misuse of the equipment/software, may render the officer liable to internal investigation/disciplinary action.

Any line managing member of staff, with express permission from the RelyOn may access the footage for professional standards or related purposes where there is a clear and justifiable need to do so, including for:

- Specific quality assurance purposes (such as Use of force oversight review meetings) or oversight requirements.
- Conducting supervision or assisting with training and professional development
- Identifying establishment-wide or individual training needs.
- Investigating specific allegations, specific patterns of complaints and conducting disciplinary investigations.
- Where specific intelligence has been received that would indicate that viewing of BWVC footage is proportionate and necessary.

RelyOn must ensure there is not a practice of routinely reviewing recorded footage, without a clear and justifiable need to do so. Such action is not within the stated purpose and outcomes of the policy, can create mistrust in the use of BWVC by staff. Such misuse of the equipment/software may render the reviewer liable to internal investigation/disciplinary action.

Any potential corruption or misconduct issues captured by BWVC must be reported in line with Counter Corruption and Reporting Wrongdoing Policy Framework and PSI 6/2010 – Conduct and discipline.

Any incidental footage captured indicating staff misconduct obtained without the express knowledge of the subject cannot be reasonably ignored or disregarded by RelyOn and in any event this will be retained and processed in line with the data management.

RelyOn must consider whether intentional covert recording, may render the officer liable to internal investigation/disciplinary action.

5. Incident Response – Medical Intervention

The use of BWVC to record footage is mandated to be "incident related" – which is therefore likely to include incidents involving injury to or illness of a person. This may also include situations where medical interventions are taking place.

On attending an incident involving medical intervention BWVC users must consider any sensitivities of the circumstances. This is particularly relevant when attending an incident where a person is receiving lifesaving medical intervention and therefore is unable to be informed of, or consent to, being filmed. Officers should conduct a dynamic risk assessment and where no threat to the safety or security of others exist, officer should maintain audio capture to record any decisions and rationales during interventions, but should consider non-intrusive capturing of the medical intervention. This may be through directing the camera away from intervention.

The BWVC user will record the necessity, proportionality, and justification for their actions in the accompanying written documents.

6. Spontaneous Use of Force (UoF)

Users must justify their actions, perceptions, and decisions as per normal within their written Use of Force (UoF) statement. The writing of UoF statements must be completed before any captured footage is viewed, this will enable staff to detail the threat perceived at the time of the incident and not on reflection having viewed any footage. Staff must reference BWVC footage was captured within the UoF statement. The use of BWVC is a tool to support and not replace written statements. If footage is viewed following the writing of the UoF statement and the user wishes to make a further statement, this can be provided as an addendum to the original statement, clearly stating this is being provided following viewing the footage.

BWVC footage of UoF must be tagged and retained in line with UoF paperwork:

- The full name of the person sealing in the evidence bags.

7 Evidence

When BWVCs are used transparently, consistently, and fairly they can have a positive impact on staff's perceptions of safety. Positive perceived impacts included:

- staff increased levels of perceived safety
- potential deterrence and effective de-escalation of incidents.
- an increase in how fairly authority is perceived to be exercised.
- provision of evidence that protects both staff and the public that helps to build open and trusting relationships.

In producing this policy, due regard has been given to the following:

- UK General Data Protection Regulation.
- The Data Protection Act 2018.
- The Freedom of Information Act (FOI) 2000.
- The Code of Practice for surveillance cameras and personal information produced by the Information Commissioner's Office.
- The Prison Rules 1999.
- Young Offenders Institution Rules 2000.
- Protection of Freedoms Act 2012.
- The Regulation of Investigatory Powers Act (RIPA) 2000.
- The Home Office Surveillance Camera Code of Practice 2013.
- Human Rights legislation.
- The Health and Safety at Work Act 1974.

- The Management of Health and Safety.
- The Police and Criminal Evidence Act at Work Regulations 1999 (PACE) 1984.

8 Scenes of Crime/Evidence Preservation

RelyOn security staff must focus on direct management of the incident at hand and not assume any of the investigatory role which remains to be the role of the police.

In responding to incidents users may arrive at a potential “crime scene” and footage captured may prove useful for any subsequent police investigation. It is important when capturing a “crime scene” the user must not interfere, move or change any element therein.

It is extremely important that all staff understand that it may harm a police investigation or prosecution if BWVC is used to pursue lines of investigation where significant statements are obtained in the absence of a caution particularly where the suspected perpetrator is interviewed. Audio and visual recording of suspect interviews may be completed in certain limited circumstances, to be considered by officer in charge of the investigation, however staff should limit the initial questioning in order to:

- Identify if an offence has been committed.
- Identify and mitigate against any ongoing or further risks – manage the incident and those involved.

Establishments must set out in their local contingency plans the necessity to secure all digital footage, which can be achieved by prompt uploading of the footage to the networked solution.

9 Post Incident procedures

Post incident procedures may include a number of routine working practices such as cell clearance, where the occupant was involved in an incident and has subsequently been relocated. Whilst BWVC must not be used to record routine working practices, however in the direct aftermath of an incident it may be appropriate to record such procedures. Such recordings must only be made on the clear instruction of the Incident Manager and factors requiring this clearly set out in the accompanying written statements.

When dealing with incidents involving Potential Traumatic Events (PTE) (which is defined as an event that may cause acute stress reactions afterward). Incident Managers and supervisors must consider the potential effect reviewing those involved in the incident reviewing captured footage and the possible impact of re-traumatisation. It is not possible to identify here every scenario which has the potential to give rise to post trauma stress reactions in all cases, as such reactions are very personal and individual.

10 Staff training and development

When BWVC footage is being considered for use in training, staff must first consider whether any alternative methods would serve the same purpose, other than using BWVC footage.

The following are points of consideration:

- Is anyone in the footage identifiable (also from anyone’s knowledge of the incident)? (If so, the footage must be pixelated)
- What is the setting of the incident recorded and is it contentious (such as toilets, showers, or places of worship)? This would point against using the footage for training purposes.
- Is the footage being used informally in a debrief setting, or is the footage going to be used as part of a larger/more formal training event? Use of footage for training and de-briefs should be carefully considered to ensure that only the minimum detail necessary is included and consider the potential effects of Potential

Traumatic Events (PTE) or acute stress reactions in those reviewing the footage. These considerations are even more significant if the footage is going to be shown to large numbers of people or retained for a long period of time.

RelyOn Guarding & Security Services could suffer reputational damage whenever personal information is being used or shared incorrectly. Considerations of the use incident footage which may create PTE or acute stress reactions in those who view the footage. If no alternative is viable or appropriate, then BWVC footage can be used, subject to the requirements in the policy framework would apply to its use. But this must be considered on a case-by-case basis.

Showing footage for training which is highly emotive, challenging or distressing has the potential to cause harm to staff. Directors must consider the sensitivity of any footage used in any training and development scenario.

If you have considered the above and these cannot be met, using this footage for training purposes could be high risk in terms of data protection, and you should complete a Data Protection Impact Assessment (DPIA) to consider the risk and determine if its use is justifiable. Information on DPIAs can be found via the below link:

https://intranet.justice.gov.uk/guidance/knowledge-information/protectinginformation/privacy-reform/data-protection-impact-assessments-dpias/

For more information on individual cases, please refer to the Information Security and Services Team (FMB).

Staff captured in the footage must give their express permission for its use in training and this must be recorded in the risk assessment for retention of material. Staff may agree but conditional to the images being redacted but where staff decline this permission then the footage must not be used. Similarly, if staff withdraw their consent for the use of footage containing their images the footage must be withdrawn from training.

11 Allegations, Complaints, and Investigations

All allegations and complaints received from the public regarding the conduct of others must be dealt with in accordance with the establishment's own procedures.

BWVC officers must inform the appropriate line manager investigating a complaint of the presence of BWVC material at an early stage so that a decision can be made whether the footage should be tagged and how any material will be used.

The investigating member of staff must consider the requirements of RelyOn's policies & procedures, in respect of the requirements to disclose relevant BWVC material to the member of staff under investigation.

BWVC material may be shown to the complainant and noted in the relevant record. However, only the specific material relating to the incident/complaint subject matter must be reviewed and consideration must be given to obscuring/redacting images of non-connected person(s) and the decision to obscure/redact or not disclose should be recorded.

BWVC material must be retained on the system and marked as required for an investigation/complaint until it is confirmed that all potential uses of it, including appeal mechanisms have been completed.

12. Constraints

12.1 Camera operation

BWVC must not be routinely used during the conducting of full searches due to the potential impact upon privacy rights of the person being searched. Where a safety or security incident occurs during a full search and the overwhelming proportionality and necessity requirements for recording the incident outweigh the impact on privacy of the individual (such as where Use of Force is required to be used). Once the incident is resolved, if the full search is to recommence the BWVC recording must be stopped before the search starts.

12.2 Professional Standards

The coverage captured by BWVC provides only a limited view of an incident; showing only one angle; it does not record what might be happening behind the lens or behind the officer who is filming; it does not record smells, feelings of tension or the atmosphere building up to; or surrounding, an incident.

Caution should be exercised as to adding undue weight to its evidential value, whilst it is potentially compelling viewing and there is a risk that other important evidence could be ignored or given less value. From a complaint handling and investigation perspective, initial written accounts are useful because they have the potential to record much more detail, including the officer's perceptions of the event and how that informed their actions and decisions. This information can be pivotal in assessing whether an action was reasonable.

Managers must ensure that users do not become overly reliant on BWVC at the expense of existing mechanisms. For example, BWVC must not be used to record a place of the required second officer. BWVC footage does not replace the need to produce an Incident Report or Use of Force documentation. BWVC is a tool to support and not replace and all other protocols must still be complied with. Further requirements on the use of BWVC during cell searches and Use of Force are contained within this policy and within the respective policy frameworks.

13. Disclosing footage for criminal evidential purposes

Where material is being disclosed to the Police pursuant to a criminal investigation; evidence should be shared digitally where possible; where this is not possible, a secure courier service should be used. Two copies of the material must be burned to a disc or USB flash drive, one labelled "Master Copy" and sealed in a signed evidence bag and one "Working Copy" also sealed in a separate signed evidence bag– the two copies must be recorded in the establishment evidence log, detailing:

- The seal numbers.
- The BWVC user details
- The time date of recording.
- The full name of the person making the duplicate copies.
- The full name of the person sealing in the evidence bags.

Having stored the evidence in a secure store the evidence log must maintain an accurate log of the time, date, and location of storage.

When the copies are handed to the police, they must be signed out of the evidence store and the log duly notated with names/shoulder numbers of the person taking the evidence.

The onward storage location of the discs must also be recorded in the establishment evidence log for Information Commissioner's Office audit purposes.

The original footage must be tagged and stored until conclusion of any court process and subsequent appeal; the risk assessment for retention will evidence the need for criminal investigation.

14 Data Management

RelyOn Guarding & Security Services must have one or more managers and an identified deputy to take on the role of Approval Officer for retention of footage past the 90-day point, whose role will also include management of the process and overall system in accordance with all necessary obligations. These roles and responsibilities must be communicated to staff in the establishment and set out in the establishments policies.

BWVC footage must be classified as official-sensitive; it must therefore be managed robustly and all access, use and movement must be documented in the establishment's evidence log. This log will provide an audit trail for the data controller & RelyOn management team.

Users who have recorded any BWVC material must not be given IT authority to delete any data. In situations where the system administrator is also an operational member of staff who also uses a BWVC, the system administrator must seek approval from the Head of Security to manually delete any data they themselves have recorded. Details of this approval must be recorded.

14.1 Data Retention and Deletion

All staff need to be aware that under the Data Protection Act 2018 (DPA) – personal data processed and held for any purpose must not be kept for longer than is necessary for that purpose. The DPA does not contain any interpretation of that principle, but the retention periods and justification requirements set out in this instruction have taken the requirements of the DPA into consideration.

RelyOn Guarding & Security Services must maintain clear decision logs for the retention of all BWVC footage.

Once uploaded BWVC material will be routinely stored on the system for a period of up to 90 days at which point unless the footage is tagged it will be automatically deleted.

To retain footage past the 90 days, a designated Approval Officer or designated manager will complete a risk assessment setting out the justification for retaining the footage in line with the DPA.

The justification assessment will include a brief description of the content, details of the person capturing the footage, date time and place and the reason for retention i.e. Adjudication, Use of Force, Police Referral, Disciplinary Investigation, litigation.

Guidance on retention periods for potential litigation purposes are listed below:

- BWVC footage which relates to personal injuries should be retained for 3 years 4 months. This is in line with limitation periods for personal injury claims.
- BWVC footage relating to all assaults, even those which result in low-level injuries, should be retained for 3 years 4 months.
- BWVC footage relating to Use of Force incidents should be kept for 6 years, in line with the retention requirement for Use of Force.
- Once the retention justification is made the footage can be stored on the storage system for a maximum period of 6 years from date of incident.

The DPA requires that the decision for necessity to retain is periodically reviewed, and the RelyOn considers a review every 3 months as a minimum review to be appropriate, to ensure that the justification remains. These review periods are set in order to provide assurance that the justification, necessity and proportionality of retaining the footage is considered at appropriate intervals.

15 System Access

Each RelyOn Office must ensure that all access to the data management system and recorded footage is managed, logged, and robustly controlled, with a minimised number of people with access to footage.

Access levels must be carefully attributed and limited to maintain the integrity of the system.

Data edit functionality must be restricted to a senior member of staff, the designated “Owner” of both System and recorded data.

Footage must be viewed in isolation of staff areas with obscured sight lines and where audio access is facilitated via headphones.

16 Legal Privilege/confidential communications

Users of BWVC must be careful to respect legal privilege/confidential communications and must not deliberately record material that is or is likely to be subject to legal privilege or to which confidential access has been given (further details on this type of material can be found in PSI 04/2016). Where images are inadvertently captured, and the footage is to be retained (for example incidents involving use of force) then these images must be edited, redacted, or pixelated.

17 Disclosing footage for Intelligence purposes

Where material is being disclosed to the Police for intelligence purposes; evidence should be shared digitally, via the secure sharing feature within digital data management platform; where possible. Where this is not possible one copy of the material must be burnt to a disc or USB flash drive and sealed in a signed evidence bag and recorded in the establishment evidence log detailing:

- The seal numbers.
- The BWVC user details.
- The time date of recording.
- The full name of the person making the duplicate footage.
- The full name of the person sealing in the evidence bags.

The material can be handed to the police as a voluntary disclosure or via an Operating Partnership Team 1 application and a note made in the evidence log.

All requests must be authorised by the relevant line manager and the following details should be provided:

- How the material will be used.
- How it will be disclosed (and to whom).
- How it will be stored.
- How long it will be stored.

The Head of Intelligence (Regional/Tactical/Strategic/Agency) will assume responsibility for ensuring that the material is stored, used, and shared appropriately (in full consideration of any handling restrictions imposed by the RelyOn Data Controller).

Where material is being disclosed to the National Intelligence Analysis Unit evidence should be shared digitally, via the secure sharing feature within digital data management platform; where possible. Where this is not possible one copy of the material must be burnt to a disc and sealed in a signed evidence bag and recorded in the establishment evidence log detailing:

- The seal numbers.
- The BWVC user details.
- The time date of recording.
- The full name of the person making the duplicate footage.

18. Outcomes

BWVC will only be used for overt recording and to support:

- De-escalation of conflict or confrontation.
- Prevention, detection and investigation of crime or disorder.
- The apprehension and prosecution of any person who has committed a crime (including the use of images as evidence in criminal proceedings and internal disciplinary hearings).
- Safe resolution of staff disciplinary investigations.
- Interest of public and employee Health and Safety.
- The protection of staff and the public.
- Safeguarding the security of the establishment.
- Development of staff skills through use of operational footage for training purposes.
- General good management of RelyOn to safeguard the security, good order and discipline of the establishment.

19. Data sharing for law enforcement

In processing personal data for any of the law enforcement purposes, personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments:

- personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and
- every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

In processing personal data for any of the law enforcement purposes, a clear distinction must, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as:

- persons suspected of having committed or being about to commit a criminal offence.
- persons convicted of a criminal offence.
- persons who are or may be victims of a criminal offence.
- witnesses or other persons with information about offences.

All reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes.

For that purpose:

- the quality of personal data must be verified before it is transmitted or made available,
- in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and
- if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

20 Key Roles

Managing Director	Daniel Boyle
Head of Group Services (Data Controller)	Philippa Wood
Operations Director (Security) (Deputy Data Controller)	Simon Thomas
Deputy Data Controller	Nick Headland