Harbertonford Community Shop and Post Office

CCTV and Video Surveillance Policy

Incorporating CCTV, audio recording and live remote (mobile app) surveillance

Revision History

Version	Date	Author	Summary of changes
v01	01.03.2025	Jonathan Roberts	Original policy drafted
v02	10.03.2025	Jonathan Roberts / Krystyna Krzyzak	Typo corrections; ratified by Committee
v03	07.09.2026	Laura Hobden, Jonathan Roberts	Updated to include camera types, locations and data storage information. Included references to legal requirements and current ICO standards. Updated to include access control measures.

1. Policy Statement and Scope

Harbertonford Community Shop and Post Office ("the Shop", "we", "us") operates a Closed-Circuit Television and video surveillance system ("the CCTV System") on and around its premises. This policy explains why we use the CCTV System, how it is operated, who can access footage and live feeds, how long images are kept, and the rights of anyone whose image or voice is captured.

This policy applies to all trustees and members of the Management Committee, employees, volunteers, contractors, customers and any other visitor whose image, voice or personal data may be captured by the CCTV System. It applies equally to recorded footage and to live remote viewing of camera feeds (for example, via a mobile phone app).

This policy should be read together with the Shop's Data Protection Policy, Privacy Notice, Subject Access Request Procedure, Data Retention Policy, Disciplinary Policy, Complaints Policy, Appropriate Policy Document and CCTV Incident Procedure.

The Harbertonford Community Limited is registered with the ICO and holds a Data Protection Registration Certificate reflecting its status as a data controller for CCTV footage. Refer to Appendix D

2. Legal and Regulatory Framework

This policy has been prepared to reflect the following legislation, regulatory guidance and codes of practice applicable in England:

- UK General Data Protection Regulation (“UK GDPR”) – the retained EU Regulation 2016/679 as it forms part of UK law under the European Union (Withdrawal) Act 2018, as amended.
- Data Protection Act 2018 (“DPA 2018”), including Part 2 and Schedule 1 (conditions for processing special category and criminal offence data).
- Data (Use and Access) Act 2025, which received Royal Assent on 19 June 2025 and amends the UK GDPR/DPA 2018 regime, including provisions affecting subject access requests (e.g. the “stop the clock” provision where clarification is needed from a requester) and the legal basis for certain routine processing.
- Human Rights Act 1998, incorporating Article 8 of the European Convention on Human Rights (right to respect for private and family life), which is engaged by any covert or overt surveillance capturing identifiable individuals.
- Protection of Freedoms Act 2012, Part 2, Chapter 1, and the Surveillance Camera Code of Practice issued under section 30 of that Act. The Code applies as a legal duty only to “relevant authorities” (police and local authorities). Still, the Information Commissioner and the Surveillance Camera Commissioner's office both recommend it as good practice for any organisation operating CCTV, and this policy adopts its 12 guiding principles voluntarily.
- Information Commissioner's Office (ICO) guidance “Video surveillance, including guidance for organisations using CCTV” (current guidance, which replaced the ICO's earlier 2015 CCTV Code of Practice), and the ICO's small-organisation guidance “CCTV for your organisation: things you need to do.”
- ICO guidance “Employment practices and data protection: monitoring workers” (published 3 October 2023), which applies because staff will be captured by the cameras in the shop, garage/kitchen and storeroom during their work.
- Regulation of Investigatory Powers Act 2000 (RIPA) – relevant if covert monitoring of an individual is ever considered; this policy does not authorise covert surveillance (see section 5).
- Computer Misuse Act 1990 – unauthorised access to or interference with the CCTV system or its footage (including the mobile app or cloud account) may constitute a criminal offence.
- Private Security Industry Act 2001 – relevant only if a third-party CCTV monitoring/installation contractor is used and requires SIA licensing for certain activities.

3. Purpose of the CCTV System

The Management Committee has identified the following specific, documented purposes for the CCTV System. CCTV is not used speculatively or “just in case”:

- To help prevent and detect crime, including theft, robbery and criminal damage, and to help protect the Shop's stock and assets.
- To support the safety and security of staff, volunteers and customers, including in response to previous incidents of shoplifting and verbal abuse and to support the Shop's Zero Tolerance approach to abuse of staff.
- To safeguard staff, volunteers and customers from harm where possible, and investigate reported incidents quickly, so the causes can be established and rectified to prevent further incidents.
- To assist the police in the prevention, investigation and prosecution of crime.
- To allow designated individuals to check the live feed if they have reason to believe the premises may have been accessed outside opening hours — for example, following a call from a neighbour, an alarm activation, or a police report. The cameras do not currently send motion notifications, so this is a reactive check rather than an automatic alert; the Shop does not rely on CCTV alone for out-of-hours security.

The Shop has considered less intrusive alternatives (for example, improved lighting, security tagging, and staff procedures) and concluded that CCTV remains necessary and proportionate for the purposes set out above. This assessment is recorded in the Data Protection Impact Assessment at Appendix A.

4. Description of the System

The CCTV System comprises the following, as installed at the date of this policy:

- System: Blink (Amazon) camera system with cloud subscription.
- Cameras: seven (7) fixed cameras, sited internally only (the Shop does not operate any camera covering an area outside the premises). Exact camera positions and each camera's field of view are set out in the floor plan at Appendix C, which should be read alongside this policy.
- Audio: audio recording is enabled on one camera only – the camera covering the tills/Post Office counter – in response to a documented history of verbal abuse and intimidation of staff by customers at that location. Audio is turned off on all other 6 cameras. See section 6 for the specific controls that apply.
- Storage: footage is stored in the Blink cloud subscription for up to 30 days on a rolling basis, after which it is automatically overwritten/deleted (see section 9).
- Live viewing: the system provides a live video (and, for the till/Post Office camera, audio) feed accessible via the Blink mobile app, which designated individuals can view in real time (see section 7).

Confirmed by the system installer and recorded in full in Appendix A: footage is processed by Blink (Amazon.com Services LLC / Immedia Semiconductor LLC) and stored on AWS Cloud in the EU-West-1 region (Ireland). This does involve a restricted transfer, as Amazon's US-based entities may access data; the safeguard relied on is the UK-US Data Bridge (the UK extension to the EU-US Data Privacy Framework), and Amazon.com, Inc. holds an active DPF certification. The Management Committee should periodically re-check that this certification remains current (see Appendix A).

5. Lawful Basis and Data Protection Impact Assessment (DPIA)

The Shop relies on recognised legitimate interests (Article 6(1)(ea) UK GDPR) as its lawful basis for routine CCTV recording, namely the prevention of crime and protection/safeguarding of people and property. As the CCTV is specifically used for safeguarding and crime detection and prevention, which are Recognised Legitimate Interests, a Legitimate Interest Assessment (LIA) is not required.

Because the CCTV System involves (a) audio recording at one location, (b) monitoring of staff in their working areas, and (c) a live remote feed accessible on personal/managers' mobile phones, this processing is likely to result in a high risk to individuals' rights and freedoms. A Data Protection Impact Assessment (DPIA) is therefore mandatory under Article 35 of the UK GDPR and must be completed and approved by the Management Committee before any change to the system (including adding cameras, enabling audio elsewhere, or changing who can access the live feed). The current DPIA is at Appendix A and must be reviewed at least annually or sooner if the system changes.

This policy does not authorise covert (secret) monitoring of any individual. Covert monitoring targeted at a specific person would require a separate, senior-level authorisation, a distinct legal basis and consideration of RIPA and Article 8 ECHR, and is expected to be used only in rare, serious cases (e.g. suspected serious theft) on legal advice.

Criminal-offence data element (incident Records, internal alerts) relies on the separate Schedule 1, Part 2 condition set out in the Appropriate Policy Document.

6. Audio Recording – Specific Controls

The ICO is explicit that audio recording is significantly more intrusive than video alone and is very difficult to justify. Its guidance states that organisations “should not normally use surveillance systems to directly record conversations between members of the public,” that “continuous audio and video recording can be highly intrusive” and that any audio capability should be switched off by default unless there is evidenced and justified need. The Management Committee has considered previous incidents of verbal abuse and intimidation of staff at the tills/Post Office counter and concluded that audio recording is justified at that single location only. The following controls apply:

1. Audio recording is enabled only on the camera covering the tills/Post Office counter. It remains disabled on all other 6 cameras.
2. The justification for audio at the tills/Post Office counter – the documented pattern of verbal abuse and intimidation of staff – is recorded in the DPIA (Appendix A) and must be re-evidenced, not simply assumed, at each policy review.
3. Audio recording must not be extended to any other camera unless the Management Committee documents an equivalent specific, evidenced need in the DPIA that cannot reasonably be addressed by video alone.
4. Signage at the tills/Post Office counter must clearly state that audio, as well as video, is being recorded there (a standard “CCTV in operation” sign referring only to images is not sufficient for that camera).
5. Audio recording must never cover areas where there is a reasonable expectation of privacy, including any staff rest area, WC, or private telephone calls.
6. The Management Committee must review, at least every six months, whether the justification for audio recording at the tills/Post Office counter still applies, and turn off the audio if it does not.

7. Live Remote Viewing (Mobile App / “Live Feed”) – Specific Controls

Viewing a live feed is “processing” of personal data under the UK GDPR in the same way as recording footage, even though nothing may be stored. The ICO's guidance on live streaming confirms that collecting or viewing data in real time still constitutes processing and remains subject to full UK GDPR/DPA 2018 obligations. Live remote access to any of the 7 cameras (including audio from the tills/Post Office counter camera) via personal or managers' phones therefore carries particular risk, because it is harder to supervise and audit than access to stored recordings. The following controls apply:

7.1 Who may have live access

- The Blink app uses a single shared login for all users; the system does not support separate credentials or admin-level permissions per person. Because of this, access is controlled entirely by who is given the login details, not by the system itself — anyone with the login can view and change anything on the account, including camera settings and audio.
- The shared login is protected by two-factor authentication (2FA), verified via a dedicated shop mobile phone kept on the premises and used for no other purpose. This phone must be passcode-locked, and its loss or damage reported to Steve Wollett immediately, as it is the only way to complete 2FA for the account.
- Access to the shared login is restricted to the list of individuals named and approved by the Management Committee, as recorded in Appendix B and reviewed at least every six months.
- Access cannot be revoked for one person without affecting everyone; therefore, the shared password must be changed immediately whenever someone with access leaves their role, changes role, or is suspended — and the new password must be given only to those remaining on the approved list.
- There is no technical way to restrict what a logged-in user can see or change; so this policy relies on keeping the approved list as short as possible and on the personal accountability of everyone on it. Any concern about a named individual's conduct should be raised under section 7.3 or as a disciplinary matter (section 14).

7.2 Device and technical security

- The Blink app may be installed only on the shop mobile and on 1 personal device per person named in Appendix B. The app must not be installed on any other device. If someone needs to switch devices, the app must be removed from the previous device first.
- The app must only be installed on a device secured with a passcode/biometric lock and, where possible, remote-wipe capability.
- Notification previews that show camera thumbnails on a locked screen should be disabled, so that footage is not visible to anyone who happens to see the phone.
- Screenshots, screen recordings, downloads or forwarding of live feed images to third parties (including other staff, family members, or on social media) are strictly prohibited other than where necessary to report a crime to the police or as part of a formal disciplinary or legal process, and then only via the access and disclosure procedure in sections 10–11.
- If a device with app access is lost, stolen or replaced, this must be reported immediately to the Management Committee so that access can be revoked and, where relevant, treated as a potential personal data breach (section 12).

7.3 Realistic oversight of live viewing

The Shop recognises that requiring every live glance at the app to be individually logged and to be notified to the Management Committee in advance is not practical or enforceable, and that a policy

that relies on this is unlikely to be followed in practice. Instead, the Shop adopts a proportionate, realistic approach to oversight of live access:

1. The number of people with live access is kept to the minimum necessary (see 7.1), which is the primary control – fewer people with access means less risk, rather than relying on after-the-fact reporting.
2. Anyone accessing the live feed for a reason connected to a specific incident (e.g. checking a till discrepancy, a reported theft, or a safety incident) must record this in the Access Log (Appendix B), including the date, time, reason and outcome. Routine security glances (e.g. checking the shop is empty before closing) do not need to be logged individually.
3. Blink/Amazon account activity (sign-ins and, where the platform provides it, a record of app opens) should be periodically checked by the committee's designated representative listed in Appendix B1 against the approved access list in 7.1 and to confirm no unrecognised devices are linked to the account, so that oversight does not depend solely on self-reporting.
4. Any use of the live feed to specifically monitor a named individual's conduct or performance (rather than general security) must be treated as workplace monitoring under section 8 and requires prior documented justification, not just informal access.
5. Any concern that live access is being misused (e.g., viewed for reasons unrelated to the purposes in section 3) should be raised as a complaint or disciplinary matter under sections 13 and 14.

8. Surveillance in the Workplace – Staff and Volunteers

Because cameras cover areas where staff and volunteers work (the shop floor, garage/kitchen and storeroom), the ICO's guidance on monitoring workers applies in addition to its general CCTV guidance. In line with that guidance, the Shop will:

- Consult with staff and volunteers before making material changes to the CCTV System (for example, enabling audio on a further camera, adding cameras, or changing who has live access), and take their views into account as part of the DPIA process.
- Ensure staff and volunteers are clearly told, through induction, signage and this policy, of the nature and extent of monitoring and its purpose, including which camera(s) record audio and why.
- Do not routinely use CCTV installed for security purposes to monitor or discipline staff performance without prior warning; where footage is used in a disciplinary process, it will follow the Shop's Disciplinary Policy and be limited to what is relevant and proportionate to the specific allegation.
- Avoid continuous, targeted monitoring of any individual worker, which is likely to be justifiable only in the rarest circumstances (for example, a specific, evidence-based investigation) and would require its own documented assessment.
- Ensure staff know they can raise concerns about the CCTV System with the Management Committee, and that they may also complain to the ICO if they consider the system is being used unfairly.

9. Siting of Cameras and Signage

- All 7 cameras are sited internally to meet the purposes in section 3; the Shop does not operate any camera covering an area outside the premises. Camera positions and fields of view are shown in the floor plan at Appendix C.
- Cameras must not be sited in areas where individuals have a reasonable expectation of privacy, such as a WC, changing area or private staff rest area.

- Clear signs are displayed at the shop entrance and near each camera, stating that CCTV is in operation, the purpose of the system, the identity of the data controller, and contact details for queries.
- An additional sign at the tills/Post Office counter specifically states that audio and video are recorded there (see section 6).
- Whenever the floor plan in Appendix C is updated (for example, if a camera is moved or added), this policy and the DPIA in Appendix A must be reviewed to ensure they remain accurate.

10. Management, Access and Security of Recorded Footage

- The CCTV System is overseen by the Management Committee and operated day-to-day by trained, designated staff.
- Access to stored (recorded) footage is restricted to the individuals named in Appendix B and is only used for the purposes in section 3.
- Any allegation against a member of staff involving CCTV footage is referred to the Chair, who will determine who needs to view the footage and the appropriate next steps, in line with the Disciplinary Policy.
- Access to stored footage is password-protected/encrypted, and the ability to export or download copies is restricted to specifically designated individuals.
- A log is kept of all access to stored footage, recording the date, time, individual accessing the footage, and reason (Appendix B). This is distinct from and in addition to the live-access login section in section 7.3.
- The system is checked periodically (at least monthly) to confirm it is operating correctly, including that the date/time stamp is accurate and signage remains visible.

11. Storage and Retention of Images

Recorded footage is retained for a maximum of 30 days on a rolling/overwrite basis via the Blink cloud subscription, unless a specific, documented reason exists to retain particular footage for longer (for example, footage relevant to an ongoing police investigation, insurance claim or disciplinary process, which will be extracted and stored securely and separately until no longer required for that purpose).

The Management Committee has considered whether 30 days is proportionate and necessary, rather than simply the default period offered by the subscription, and will review this at each policy review. The UK GDPR and DPA 2018 do not set a fixed retention period for CCTV – the test is what is necessary for the documented purpose – so retention will be shortened if a shorter period is shown to be sufficient in practice.

12. Data Subject Rights, Subject Access Requests and Breach Reporting

- Any individual recorded (visually or by audio) has a right, subject to limited exemptions, to request a copy of any footage in which they appear as part of a subject access request (SAR) under Article 15 of the UK GDPR / section 45 of the DPA 2018.
- Subject Access Requests (SARs) are handled in accordance with the Shop's Subject Access Request Procedure and must be responded to within one calendar month. Under the Data (Use and Access) Act 2025, if the Shop reasonably needs further information from the requester to locate the relevant footage (for example, the date, approximate time, and camera location), the one-month period is paused (“stop the clock”) until that information is provided.

- Where footage contains third parties, the Shop must consider whether their images can be redacted/blurred, whether their consent can reasonably be obtained, or whether disclosure is otherwise reasonable without consent, in each case recording the decision made.
- A record must be kept of all SARs (Subject Access Requests) and other disclosures: when the request was made, how third-party images were handled, who viewed or received the footage, and in what format.
- Any actual or suspected personal data breach involving CCTV footage or live-feed access (for example, a lost phone with app access, unauthorised viewing, or a hacked account) must be reported immediately to the Management Committee. Where the breach is likely to pose a risk to individuals' rights, it must be reported to the ICO within 72 hours and to affected individuals without undue delay.

13. Disclosure of Images to Third Parties

- Footage will only be disclosed to third parties (including the police) where permitted under the Data Protection Legislation and necessary for the purposes in section 3.
- Requests from the police should specify what footage is required and why; the same recording obligations in section 12 apply to any disclosure made.
- Any court order requiring disclosure must be complied with, but its precise scope should be carefully checked; if in doubt, seek advice before disclosure (for example, from the ICO, a solicitor, or a relevant charity/umbrella body's data protection advice line).
- Footage must never be posted to social media, shared in group chats, or otherwise made available to an indefinite audience.
- Internal security alerts to staff (warning colleagues about a suspected offender, under the CCTV Incident Procedure, section 7) are not third-party disclosure, but are held to an equivalent standard: authorised only by Steve Wollett (see section 17), issued to staff only, and shown in person on a device already covered by the access controls in section 7.2 wherever possible — never printed, and never sent by text, email or messaging app except as a limited, logged fallback.

14. Misuse of the CCTV System

Misuse of the CCTV System – including unauthorised viewing, copying, sharing, or disclosure of live feeds or recorded footage – may constitute a criminal offence (including under the Computer Misuse Act 1990 and section 170 of the DPA 2018, unlawfully obtaining personal data). It will be treated as gross misconduct under the Shop's Disciplinary Policy.

15. Review of this Policy and the CCTV System

- This policy, and the accompanying DPIA, will be reviewed annually, or sooner if: the camera system, storage arrangements or provider changes; audio recording is turned on or off; the list of individuals with live or recorded access changes materially; there is a relevant complaint, breach or near-miss; or there is a material change in law or ICO guidance (for example, further ICO guidance following the Data (Use and Access) Act 2025).
- The Management Committee is responsible for ensuring the review takes place and for minuting the outcome.

16. Complaints

Any complaint about this policy or about the operation of the CCTV System should be made in accordance with the Shop's Complaints Policy. Individuals also have the right to complain directly

to the Information Commissioner's Office (ico.org.uk / 0303 123 1113) if they remain concerned after raising the matter with the Shop.

17. Roles and Responsibilities

- Data controller: Harbertonford Community Shop and Post Office (acting through its Management Committee).
- Day-to-day responsibility for the CCTV System is designated to the shop manager.
- Approval of the DPIA, this policy, and any material system change: the Management Committee, on the recommendation of the Chair/nominated data protection lead.
- Register of individuals with access (live and recorded) and periodic audit: nominated trustee /Designated Management Committee Member (see Appendix B).
- Jo Roberts will maintain the system and extend it if necessary.
- Steve Wollett is the committee member designated to oversee the CCTV system and will step in to coordinate alternative arrangements if Jo or the Shop manager is unable to fulfil their duties. Permission to access the system and/or live footage can only be granted by Steve. Please note that the Blink app does not have an admin-level permission system; therefore, this is a procedural rule only. Steve is the only person with the authority to share login information.

Appendix A – Data Protection Impact Assessment (DPIA)

To be completed and approved by the Management Committee before any material change to the CCTV System, and reviewed at least annually.

A1. Who will be captured on CCTV?
Staff, Volunteers, Customers, sub-contractors, anybody entering the premises.

A2. What personal data will be processed (including whether audio will be captured and whether any special category or criminal offence data is likely to be captured)?
All cameras capture video, and one near the till also captures audio to protect staff from verbal abuse.

A3. What are the purposes of operating the CCTV System, and why is CCTV the least intrusive way to achieve them?
Record as evidence shoplifting and unlawful entry to the premises. To deter shoplifting. Record for investigation purposes Health and Safety Incidents/accidents. Record for evidence of verbal and abusive behaviour towards staff/volunteers at the counter.

A4. What lawful basis is relied on, and has a Legitimate Interests Assessment been completed?
The CCTV is used for safeguarding and preventing and detecting crime, which is a Recognised Legitimate Interest (RLI) (Article 6(1)(ea) UK GDPR), and therefore does not require us to complete a Legitimate Interest Assessment.

A5. Who is responsible for the operation of the system day-to-day, and for this DPIA?
The manager is responsible for day-to-day management; Jo Roberts is responsible for maintenance, repair/replacement of the camera, and system setup. The management committee is responsible for the overall operation, maintenance, and management of the system, including legal compliance and subject access requests.

A6. Describe the system: camera locations and why chosen; whether audio is enabled on each camera and the justification; who has live (mobile app) access and why; where footage/data is stored (including any international transfers) and the retention period; and the security measures in place.
The system comprises 7 fixed Blink cameras, sited only internally (locations and fields of view shown in the floor plan in Appendix C). Audio is enabled only on the camera covering the tills/Post Office counter, due to a documented history of verbal abuse and intimidation of staff there (see section 6). Footage is retained for up to 30 days on a rolling basis. International transfer and storage details, as confirmed by the system installer, are set out in the table below.

Live app access uses a single shared account, as the system has no per-user login or admin-permission capability; this is secured by 2FA tied to a dedicated shop mobile phone kept on the premises. Full controls are set out in section 7.1.

Cloud Service Provider and International Transfer Details (as confirmed by the system installer)

Service Provider	Blink (Amazon.com Services LLC / Immedia Semiconductor LLC)
Data Types Processed	CCTV video footage, audio recordings (tills/Post Office counter camera only), and account holder metadata.
Primary Storage Location	AWS Cloud, EU-West-1 (Ireland).

Restricted Transfer Involved?	Yes. Data is processed and may be accessed by Amazon's US-based entities.
Transfer Mechanism / Safeguard	UK-US Data Bridge (UK Extension to the EU-US Data Privacy Framework).
Verification of Safeguard	Amazon.com, Inc. holds an active certification under the DPF Program.

The Management Committee should periodically re-check (at least at each policy/DPIA review) that Amazon's DPF certification remains active via the Data Privacy Framework list at dataprivacyframework.gov.

A7. Have staff, volunteers and (where practical) customers been consulted, and what was their feedback?

Staff and volunteers have been consulted and feedback since installation has included:

- Concern over use of audio on breaks
- Concern over use of CCTV to monitor staff performance and behaviour
- Request for audio to be turned on at the counter, as there was no evidence to provide to police relating to previous incidents of verbal abuse and threatening behaviour.

A8. What are the risks to individuals' rights and freedoms (e.g. from audio recording, live remote access on personal phones, potential loss of a device, staff monitoring)?

Risk	Risk Description
Chip and PIN visibility	The till/counter camera includes a chip-and-PIN machine in its field of view, which is a security and data protection issue.
Audio picking up private conversations.	The till/counter camera includes audio and may capture private conversations, including health and financial information.
Special category data captured incidentally.y	Camera footage may show a customer's religious dress, mobility aids, or physical medical conditions, which are special category data under Article 9.
Live feed on personal phones	Loss, theft, or unauthorised access to a phone running the Blink app could expose live footage and audio to someone outside the approved access list.
Screenshots or informal sharing of footage	A person with live access could screenshot, forward or otherwise share footage or audio to others in contravention of this policy.
Function creep i.e. using footage to assess staff performance	Footage could be used informally to monitor staff timekeeping or performance rather than the purposes stated in this policy.
International transfer/third-country access	Footage is stored on AWS in Ireland but may be accessed by Amazon’s US entities, under the US Cloud Act.

Cloud-content compromised (cyber-security)	A phishing or credential-stuffing attack could access the Blink account.
Footage not deleted after 30 days.	The automatic overwrite either fails or is improperly configured, undermining our retention commitment under this policy.
Bystanders and 3rd parties.	Delivery drivers, customers and others not involved in incidents are captured and entitled to the same rights as anyone else.
Single shared login / no per-user permissions	The Blink app has no admin-level controls, so anyone given the shared login can view or change anything — camera settings, audio, everything — with no way to give someone reduced or view-only access.
Loss or compromise of the 2FA device	The shop's mobile phone used for 2FA is a single point of failure — if lost or damaged, it could lock the whole team out of the account; if stolen or accessed by someone else, it could allow them to complete 2FA on the shared login.

A9. What measures are in place to reduce each identified risk?

Risk	Control/Mitigation Measures
Chip and PIN visibility	The camera in the till/counter area uses a masking region to blur sensitive information, so you cannot see PINs, signatures, or addresses.
Audio picking up private conversations.	Audio is enabled only on the till/Post Office camera and not extended elsewhere; the microphone's pickup range cannot be technically restricted, so ambient conversation near the counter may be captured beyond the immediate transaction. This is accepted as a proportionate residual risk given the narrow, evidenced justification (documented abuse of staff), and is kept under six-monthly review (section 6). Signage at the counter makes it clear that audio recording is taking place there.
Special category data captured incidentally.	No special processing, i.e. facial recognition or profiling, is applied. Footage is retained or passed on to police, etc., only as stated in this policy.
Live feed on personal phones	Each approved individual is limited to one personal registered device plus the shop mobile and the app must not be installed elsewhere (section 7.2). This is checked as part of the six-monthly access list and linked-device review (section 7.3).
Screenshots or informal sharing of footage	Section 7.2 prohibits this; any breach of this will be treated as gross misconduct.

Function creep i.e. using footage to assess staff performance	Section 8 covers this; any disciplinary use of footage is off by the Chair as per Section 10; informal use by a manager cannot be used for disciplinary purposes.
International transfer/third-country access	Rely on UK-US Data bridge safeguard. Periodically check Amazon DPF certification and any changes to their terms and conditions.
Cloud-content compromised (cyber-security)	Enforce2FA/MFA on the account as per section 7.1. Limit the number of linked devices to the approved list in Appendix B.
Footage not deleted after 30 days.	Quarterly spot-check that footage older than 30 days is genuinely inaccessible.
Bystanders and 3rd parties	No mitigation needed; signage is displayed, and redaction is covered in section 12.
Single shared login / no per-user permissions	Keep the approved access list (Appendix B) as short as possible; change the shared password whenever the list changes; rely on individual accountability and disciplinary action (section 14) for misuse, since it cannot be technically restricted.
Loss or compromise of the 2FA device	Keep the phone passcode-locked and on the premises at all times; report loss or damage to Steve Wollett immediately; ask Blink/Amazon support whether a backup 2FA method can be registered.

Additional control/mitigation measures in place;

- The policy is provided to all staff and volunteers and available to customers on request.
- The ICO certificate is displayed in the shop.
- Appropriate signage is displayed in the shop to inform customers about the use of CCTV and audio.
- Permission is required to access the system/live footage, but there are no administrative settings or controls within the system to physically restrict this access for existing users.

A10. Is any residual risk high despite the mitigations in place? If so, the ICO must be consulted before processing begins.

The one accepted residual risk is the till/Post Office microphone's pickup range, which cannot be technically limited (see Q8/Q9) — this is considered proportionate given the narrow, evidenced justification and is reviewed every six months under section 6. No other high residual risks have been identified.

A11. When will this DPIA next be reviewed?

Annually, or when camera locations change or additional cameras are added, whichever comes first.

Approval

Approved by (Chair/Data Protection Lead): _____

Date: _____

Appendix B – Access Registers

B1. Live (mobile app) access register

Name / Role	Device	Date access granted	Reason for access	Date access removed
Fiona Jardine - Manager	Shop Mobile and own phone	2026	Weekly checks and securing footage following incidents	
Steve Wollett - Management Committee Member	Shop Mobile and own phone	2025	Oversight and management of the system on behalf of the management committee	
Jo Roberts - Volunteer	Shop Mobile and own tablet	2025	Maintenance and management of the system	
Denise Chalk - Post Mistress	Shop Mobile and own phone	2026	Post office duties and securing footage following post office incidents.	

B2. Recorded footage access / disclosure log

Date	Individual accessing footage	Reason (incident / SAR / police / other)	Third parties in footage? Redacted?	Copy provided? To whom/format

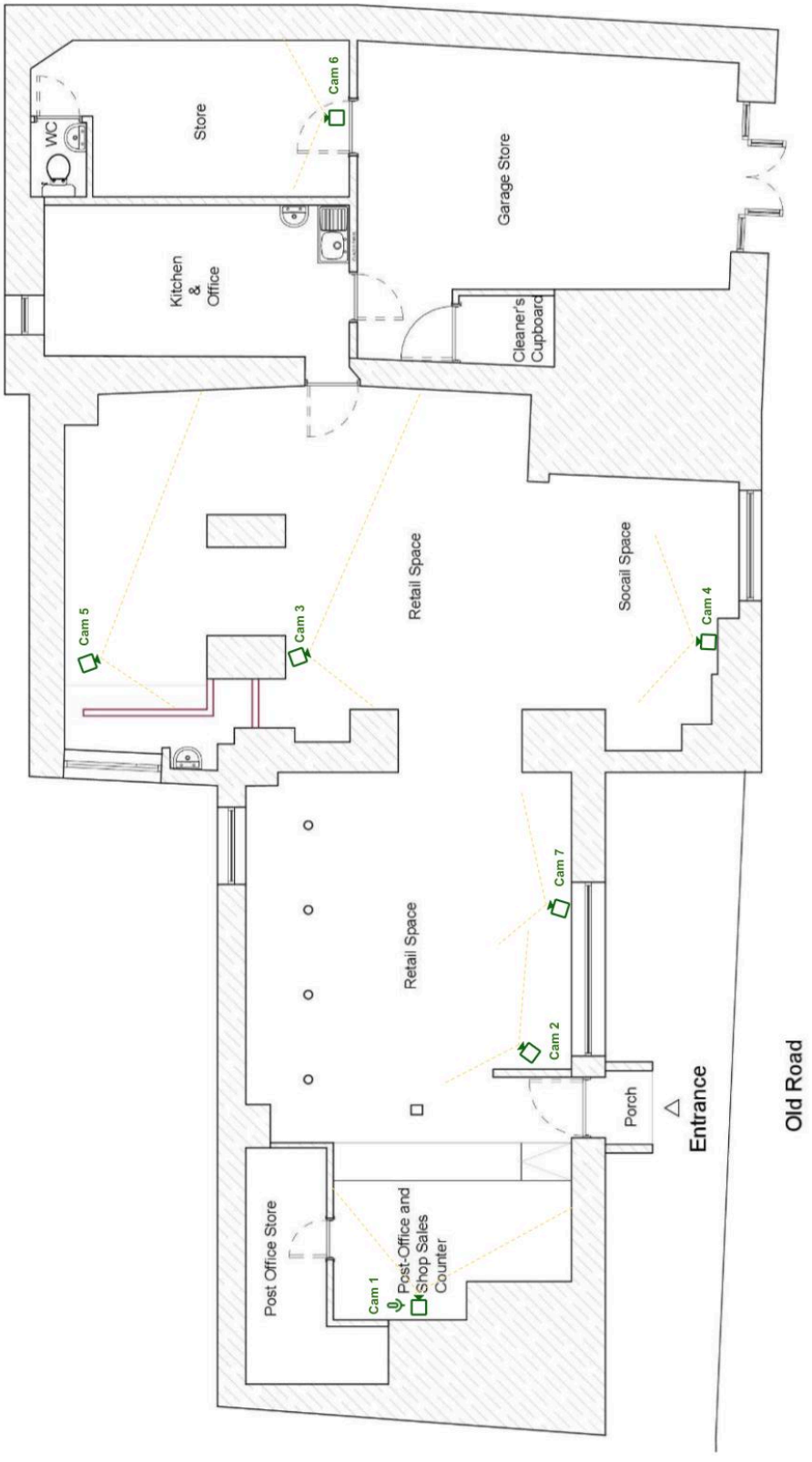
B3. Incident-related live-view log (section 7.3)

Date/time	Viewed by	Reason / incident	Outcome

Appendix C - Premises Plan with CCTV

This appendix contains a floor plan of the premises showing the locations of the cameras and approximate field of view.

= CCTV Camera, = CCTV Camera with audio. Yellow lines indicate field of vision.



Appendix D – Data Protection Registration Certificate

Data Protection Registration Certificate

The Harbertonford Community Limited

Riversdale
Ashburton Road
TOTNES
Devon, TQ9 5JU

Registration reference: ZB798945
Date registered: 21 October 2024
Registration expires: 20 October 2026

Issued by: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Telephone: 0303 123 1113
Website: ico.org.uk

Appendix E – Sources and Further Reading

- Information Commissioner's Office, “Video surveillance, including guidance for organisations using CCTV”: ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/
- Information Commissioner's Office, “CCTV for your organisation: things you need to do”: ico.org.uk/for-organisations/advice-for-small-organisations/cctv-and-dashcams/
- Information Commissioner's Office, “Employment practices and data protection: monitoring workers” (October 2023): ico.org.uk
- Home Office, Surveillance Camera Code of Practice (Protection of Freedoms Act 2012, s.30): gov.uk/government/publications/update-to-surveillance-camera-code
- Data (Use and Access) Act 2025: legislation.gov.uk
- Data Protection Act 2018 and UK GDPR: legislation.gov.uk
- Human Rights Act 1998, Article 8 ECHR: legislation.gov.uk