

Privacy Policy

Last Updated: 7 July 2026

Privacy Policy

The **UK Safety Camera Network (USCN)** is committed to protecting your privacy and ensuring that personal data is processed fairly, lawfully, and transparently.

This Privacy Policy explains what personal data we collect, why we collect it, how it is used, how long it is retained, and the rights you have under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1. Who We Are

The **UK Safety Camera Network (USCN)** installs and manages public-facing CCTV systems in partnership with community property hosts to support crime prevention, public safety, and the protection of property.

Data Controller

Bert Scanlon, trading as the **UK Safety Camera Network (USCN)**

General Enquiries: info@uscn.uk

Data Protection: data@datahandling.uscn.uk

Support: supportteam@uscn.uk

Telephone: 0330 520 2254

USCN is currently transitioning into a formally registered UK non-profit organisation. As our legal structure develops, this Privacy Policy will be updated where appropriate. USCN is committed to complying with the UK GDPR and the Data Protection Act 2018.

2. What Personal Data We Collect

We only collect personal information where it is necessary for the operation of our services.

A. CCTV Cameras

Our cameras may record:

- Images of individuals in public areas
- Vehicle registration numbers where visible
- Motion detection events and related system metadata
- Date, time and location of recorded footage

Our cameras are positioned to minimise unnecessary recording. Privacy masking is applied where appropriate to reduce the capture of private property such as windows, gardens and entrances.

B. When You Contact Us

If you contact USCN, we may collect:

- Your name
 - Email address
 - Telephone number
 - Any information included within your enquiry
 - Documents or files you voluntarily provide
-

C. Subject Access Requests (DSARs)

When you request CCTV footage or exercise your privacy rights, we may collect:

- Your name
- Contact details
- Proof of identity
- Details of the incident
- Approximate time and location
- Any correspondence relating to your request

Identity documents are used solely to verify your identity and are securely deleted once verification has been completed unless there is a legal requirement to retain them.

3. Our Lawful Basis for Processing

We only process personal data where a lawful basis exists under Article 6 of the UK GDPR.

Depending on the circumstances, processing is based upon:

- **Legitimate Interests** – maintaining public safety, preventing crime and protecting property.
- **Legal Obligation** – complying with applicable legislation or lawful requests.
- **Consent** – where you voluntarily provide information or where consent is legally required.

The lawful basis for operating our CCTV systems is **Legitimate Interests** under Article 6(1)(f) UK GDPR.

Before installing each camera, USCN carries out a Legitimate Interests Assessment (LIA) and a Data Protection Impact Assessment (DPIA) to ensure that CCTV use is necessary, proportionate and balanced against the rights and freedoms of individuals.

4. How Long We Keep Data

We only retain personal data for as long as necessary.

| Data Type | Retention Period |
|------------------------------|------------------------------------------------------------------------------------------------------|
| CCTV footage | Maximum of 31 days unless required for an active investigation, insurance claim or legal proceedings |
| Subject Access Requests | Up to 12 months after closure |
| General correspondence | Up to 12 months after closure |
| Website server security logs | Retained only as required for security and operational purposes |

Where footage becomes evidence in an investigation, it may be retained until the investigation or legal proceedings have concluded.

5. Who Can Access Data

Access to personal data is restricted using technical and organisational security controls.

Property Hosts

Approved property hosts may view live and recorded footage only from cameras installed at their own premises.

Host access:

- is limited to their assigned camera(s);

- is available only whilst connected to the camera's local network;
 - does not permit remote viewing;
 - is protected by secure authentication.
-

Authorised Personnel

Only authorised volunteers, employees or approved temporary personnel may access administrative systems.

Administrative access:

- requires secure login credentials;
- is restricted according to role;
- is fully audited;
- is regularly reviewed.

Mobile applications are not used for multi-camera management.

Sharing Footage

USCN never sells CCTV footage or personal information.

Footage may only be disclosed where:

- required by law;
- requested by authorised law enforcement agencies;
- required by a court order;
- necessary to protect life or prevent serious harm;
- required for legitimate insurance or legal proceedings.

All disclosures are recorded within our audit logs.

6. International Data Transfers

CCTV footage is stored locally within the United Kingdom.

USCN does not routinely transfer CCTV footage or personal data outside the United Kingdom.

Should international transfers become necessary, appropriate safeguards required under UK GDPR will be implemented.

7. Data Processors

Where USCN uses carefully selected third-party providers to assist with services such as email, IT support or system maintenance, those providers only process personal data on our behalf under written agreements that comply with UK GDPR.

They are not permitted to use personal data for their own purposes.

8. Your Rights

Under the UK GDPR you have the right to:

- Request access to your personal data.
- Request correction of inaccurate personal information.
- Request deletion of your personal data where applicable.
- Request restriction of processing.
- Object to processing carried out under Legitimate Interests.
- Request data portability where applicable.
- Withdraw consent where processing relies upon consent.
- Lodge a complaint with the Information Commissioner's Office (ICO).

We aim to respond to all valid privacy requests within one calendar month.

9. Automated Decision Making

USCN does not use automated decision-making, automated identification or profiling in relation to CCTV footage.

Our systems do not use live facial recognition technology.

10. Data Security

We take appropriate technical and organisational measures to protect personal information.

These include:

- Encrypted local storage for CCTV footage
- Secure authentication
- Role-based access controls
- Audit logging of all administrative access

- Regular security reviews
 - Data Protection Impact Assessments (DPIAs)
 - Routine software updates and security maintenance
 - Multi-factor authentication where appropriate for administrative systems
-

11. Cookies and Website Analytics

Our website currently does not use tracking cookies or third-party analytics.

Basic server logs necessary for security, maintenance and operation may be generated automatically by our web hosting provider.

Should cookies or analytics be introduced in the future, this Privacy Policy will be updated and consent will be obtained where required by law.

12. Changes to This Policy

We may update this Privacy Policy from time to time.

Any changes will be published on this page together with a revised "Last Updated" date.

13. Contact Us

For questions regarding this Privacy Policy or to exercise your privacy rights, please contact us.

Data Protection Enquiries

Email: data@datahandling.uscn.uk

Telephone: 0330 520 2254

General Enquiries: info@uscn.uk

Support: supportteam@uscn.uk

If you remain dissatisfied with our response, you have the right to lodge a complaint with the Information Commissioner's Office (ICO), the UK's independent regulator for data protection.
