

BRAYDEN KANE LTD

Data Protection Notices

Tenants, Guarantors and Licensees

This document contains:

Part 1 — Fair Processing Notice (v3.0)

Part 2 — CCTV and ANPR Policy (v2.0)

Part 3 — Cookie Notice (v2.0)

Date: April 2026

Review Date: April 2027

Data Controller: Brayden Kane Ltd

ICO Registration: ZA773835

BRAYDEN KANE LTD

Part 1

Fair Processing Notice

April 2026

Personal Data Fair Processing Notice

Tenants, Guarantors and Licensees — Version 3.0

1. Introduction

This Fair Processing Notice explains what personal data Brayden Kane Ltd collects about you, how we use it, who we share it with, and the rights you have in relation to that data.

We are committed to protecting your personal data and to being transparent about the information we hold. We process personal data in accordance with the UK General Data Protection Regulation (UK GDPR), as amended by the Data (Use and Access) Act 2025, and the Data Protection Act 2018.

This notice applies to tenants, prospective tenants, guarantors, and licensees (including parking and storage unit licensees).

Summary of changes from version 2.0

- Updated section 6 to include Teambuild Consultancy Limited as a data processor providing property administration support.
- Updated section 8 to disclose the international transfer of personal data to the Philippines and the safeguards in place.
- Added detail at section 3.1 acknowledging that identity documents may incidentally reveal special category data.
- Updated section 12 to align with the Information Commissioner's Office February 2026 guidance on data protection complaints.

2. Who We Are

Data Controller: Brayden Kane Ltd, 161 Gloucester Crescent, Wigston, LE18 4YH

ICO Registration Number: ZA773835

Data Protection Officer: Brayden Cooper

Contact: office@braydenkane.com

If you have any questions about this notice or how we handle your personal data, please contact the Data Protection Officer using the details above.

3. What Personal Data We Collect

3.1 Tenant and Guarantor Data

When you apply for accommodation or act as a guarantor, we may collect the following:

- Full name, date of birth, nationality, and marital status
- Contact details including email address, telephone number, and postal address (current and previous)
- National Insurance Number
- Next of kin details

- Employment status, employer details, payroll number, length of employment, salary information, and details of any other income
- Bank account details including account number and sort code
- Details of any hire purchase agreements, loan agreements, credit cards, or store cards
- Details of any welfare benefits you receive or are eligible for
- Name of university or college (where applicable)
- Names of co-occupants or friends you are staying with (where applicable)
- Property address, tenancy term, rent, deposit, and utility and service responsibilities

Where you provide identity documents (such as a passport, driving licence, or biometric residence permit), those documents may incidentally reveal special category data such as racial or ethnic origin. We do not process this incidental information for any purpose other than verifying your identity and right to rent.

3.2 Licensee Data (Parking and Storage Units)

Where you licence a parking space or storage unit from us, we collect:

- Full name and contact details (email, telephone, postal address)
- Vehicle registration number (parking licences)
- Licence term and payment details

3.3 CCTV and ANPR Data

We operate CCTV systems in the communal areas of our managed properties and at our office premises. CCTV captures images and video footage of individuals present in those areas.

We also operate Automatic Number Plate Recognition (ANPR) technology in the car parks of our properties. ANPR captures vehicle registration numbers and associated images of vehicles entering and leaving the car park.

Vehicle registration numbers are personal data because they can be linked to identifiable individuals. Please refer to Part 2 (CCTV and ANPR Policy) of this document for full details, including who has access to footage and data.

3.4 Website Data

When you visit our website, certain data may be collected automatically through cookies and similar technologies. Please refer to Part 3 (Cookie Notice) of this document for further details.

3.5 Photographs

Where we photograph an occupied property for marketing purposes (for example, to advertise the property for re-letting), images may incidentally capture a tenant's personal belongings. We will only take such photographs with your prior consent.

3.6 Special Category Data

We do not routinely collect special category data (such as health or disability information). However, we may need to collect such data in limited circumstances, for example where a reasonable adjustment or property adaptation is requested. Where this is necessary, we will explain the purpose at the time and obtain your explicit consent unless another lawful basis applies.

4. How We Collect Your Data

We collect personal data from the following sources:

- Directly from you, through your application for accommodation, licence application, or correspondence with us
- From third parties acting on your behalf, such as letting agents
- From referencing and due diligence checks carried out through our referencing partner, Goodlord
- Through our maintenance reporting platform, Fixflo, when you submit repair requests
- Through CCTV and ANPR systems at our properties and office
- Through our website when you interact with it

5. Why We Process Your Data and Our Lawful Bases

The UK GDPR requires us to have a lawful basis for processing your personal data. The table below sets out the purposes for which we process your data and the corresponding lawful basis.

Purpose	Lawful Basis
To perform our obligations under your tenancy agreement or licence	Performance of a contract (Article 6(1)(b))
To carry out tenant and guarantor referencing, affordability, and due diligence checks	Performance of a contract (Article 6(1)(b)) and legitimate interests (Article 6(1)(f))
To manage and administer your tenancy or licence, including rent and licence fee collection via GoCardless	Performance of a contract (Article 6(1)(b))
To manage maintenance and repair requests via Fixflo	Performance of a contract (Article 6(1)(b)) and legitimate interests (Article 6(1)(f))
To comply with legal and regulatory obligations, including obligations under housing and landlord and tenant legislation, tax law, and anti-money laundering regulations	Legal obligation (Article 6(1)(c))
To protect and manage our properties via CCTV in communal areas and at our office	Legitimate interests (Article 6(1)(f)) — the prevention and detection of crime, the safety of tenants, licensees, staff and visitors, and the protection of property
To manage car park access and enforce parking restrictions via ANPR	Legitimate interests (Article 6(1)(f)) — the management and security of car parking facilities, the prevention of unauthorised use, and the protection of property
To disclose CCTV or ANPR data to law enforcement agencies for the detection, investigation, or prevention of crime	Recognised legitimate interests (Article 6(1)(ea) and Annex 1, UK GDPR, as inserted by the Data (Use and Access) Act 2025) — no balancing test is required for this specific purpose
To recover debts owed under your tenancy or licence	Legitimate interests (Article 6(1)(f))

To register your tenancy deposit with the relevant tenancy deposit scheme	Legal obligation (Article 6(1)(c))
To disclose information to the relevant local authority, freeholder, factor, facilities manager, or utility provider in connection with your tenancy or licence	Performance of a contract (Article 6(1)(b)) and legal obligation (Article 6(1)(c))
To photograph an occupied property for marketing purposes where your belongings may be visible	Consent (Article 6(1)(a))
To use AI tools (Microsoft Copilot, Anthropic Claude) to assist with administration, correspondence drafting, and analysis	Legitimate interests (Article 6(1)(f))
To engage Teambuild Consultancy Limited and its authorised personnel (based in the Philippines) to provide property administration support	Legitimate interests (Article 6(1)(f)) and performance of a contract (Article 6(1)(b))
To analyse data for the purposes of administering, supporting, improving, and developing our business and services	Legitimate interests (Article 6(1)(f))
To process special category data where a property adaptation or reasonable adjustment is required	Explicit consent (Article 9(2)(a)) or compliance with employment or social security law (Article 9(2)(b))

Legitimate interests: Where we rely on legitimate interests under Article 6(1)(f) as our lawful basis, we have carried out a legitimate interests assessment, including a balancing test, to ensure that our interests do not override your fundamental rights and freedoms. You have the right to object to processing based on legitimate interests. Please contact us if you wish to do so.

Recognised legitimate interests: The Data (Use and Access) Act 2025 introduced a new lawful basis of “recognised legitimate interests” under Article 6(1)(ea) of the UK GDPR for certain specified purposes, including the detection, investigation, and prevention of crime. Where we rely on this basis, we must demonstrate that the processing is necessary for the relevant Annex 1 purpose, but a balancing test is not required.

Consent: Where we rely on your consent, you have the right to withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.

6. Who We Share Your Data With

We may share your personal data with the following categories of recipients, where necessary for the purposes described in this notice:

6.1 Third-Party Service Providers (Data Processors)

We use the following third-party service providers who process personal data on our behalf. Each operates under a written data processing agreement with us:

- **Goodlord** — tenant and guarantor referencing and due diligence checks
- **Fixflo** — maintenance and repair reporting platform
- **Xero** — accounting and financial record-keeping

- **GoCardless** — collection of rent and licence fee payments by direct debit
- **Microsoft 365 (including Copilot)** — business productivity, communication, and AI-assisted document processing
- **Anthropic (Claude)** — AI-assisted business operations, correspondence drafting, and analysis
- **Wix** — website hosting
- **Meters UK Ltd** — sub-meter utility data collection and billing (personal data processed under Meters UK Ltd's own privacy policy)
- **Teambuild Consultancy Limited** — property administration support services. Personnel engaged by Teambuild may access your personal data from the Philippines. See section 8 below for the safeguards we have in place for this transfer.

6.2 Other Third Parties

We may also disclose your personal data to:

- The relevant local authority in connection with the creation, renewal, or termination of a tenancy
- Tenancy deposit scheme administrators
- Utility and service providers, freeholders, factors, and facilities managers
- Credit reference agencies and debt recovery agents, where you are in arrears under your tenancy or licence
- Courts, tribunals, and legal advisors in connection with legal proceedings
- Law enforcement agencies for the purposes of the detection, investigation, or prevention of crime
- Any successor business entity in the event of a merger, acquisition, or restructuring
- Any other person or organisation where required by law or regulation

We will not otherwise sell, share, or distribute your personal data without your consent, unless required to do so by law.

7. Use of Artificial Intelligence Tools

We use AI-powered tools, specifically Microsoft Copilot and Anthropic's Claude, to assist with business operations such as drafting correspondence, analysing documents, and general administrative tasks. Personal data may be input into these tools where necessary to carry out these functions.

We take care to minimise the personal data input into AI tools to what is strictly necessary. Both Microsoft and Anthropic operate under data processing terms that govern how data submitted to their services is handled. Data submitted to these tools is not used by the providers to train their AI models, in accordance with our configuration of those services.

We do not use AI tools to make solely automated decisions about you that produce legal effects or similarly significant effects. Any AI-assisted output is reviewed by a member of our team before it affects you.

We process personal data through AI tools on the basis of our legitimate interests in operating our business efficiently, having conducted a legitimate interests assessment against your rights and interests. You have the right to object to this processing — see section 11 below.

8. International Transfers of Personal Data

Some of our third-party service providers may process your personal data outside the United Kingdom. Where this occurs, we ensure that appropriate safeguards are in place in accordance with the UK GDPR.

The Data (Use and Access) Act 2025 introduced a revised test for international transfers. The standard of protection in the receiving country must now be “not materially lower” than the standard provided in the UK (replacing the previous “essentially equivalent” test). Where we transfer data internationally, we ensure compliance with this revised standard, relying on one or more of the following:

- Transfers to countries that have received a UK adequacy regulation
- Transfers subject to the International Data Transfer Agreement (IDTA) issued by the Information Commissioner's Office, or the UK Addendum to the EU Standard Contractual Clauses
- Transfers to providers who are certified under an approved certification mechanism or who operate binding corporate rules

8.1 Transfer to the Philippines (Teambuild Consultancy Limited)

We engage Teambuild Consultancy Limited, a UK company, to provide property administration support. Personnel engaged by Teambuild are based in the Philippines and access your personal data remotely. The Philippines does not currently have a UK adequacy regulation.

We have the following safeguards in place for this transfer:

- A written International Data Transfer Agreement (IDTA) issued by the Information Commissioner's Office, between Brayden Kane Ltd and Teambuild Consultancy Limited, providing the safeguards required by Article 46 UK GDPR
- A separate written Data Processing Agreement governing how Teambuild and its personnel handle your data
- A documented transfer risk assessment confirming that the level of protection for your data is not materially lower than the UK standard
- Mandatory technical and organisational measures including encrypted access, multi-factor authentication, application whitelisting, and a prohibition on local storage of personal data
- A confidentiality undertaking signed by each individual at Teambuild who accesses your personal data, confirming compliance with our security policies

8.2 Other International Transfers

In particular, Goodlord may transfer personal data outside the UK and EEA as part of their referencing services. Please refer to Goodlord's privacy policy at <https://www.goodlord.co/privacy-policy> for further information.

Microsoft and Anthropic may process data in data centres located outside the UK. Both providers offer appropriate safeguards for international transfers as described in their respective data processing terms.

9. Data Security

We take the security of your personal data seriously and have implemented appropriate technical and organisational measures to protect it against unauthorised or unlawful processing and against accidental loss, destruction, or damage. These measures include:

- Storing data on secure servers and cloud platforms within the UK/EEA where possible

- Restricting access to personal data to authorised personnel only
- Using password protection and multi-factor authentication
- Application whitelisting and endpoint protection on devices used to access our systems
- Ensuring our third-party processors maintain appropriate security standards
- Regular review of our data security practices

10. How Long We Keep Your Data

We retain your personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. Our standard retention periods are:

Data Type	Retention Period
Tenancy records (including agreements, correspondence, and financial records)	Duration of tenancy plus six years (aligned with the Limitation Act 1980)
Guarantor records	Duration of the guarantee plus six years
Licence records (parking and storage)	Duration of the licence plus six years
Referencing and due diligence data	Duration of tenancy plus six years
CCTV footage	30 days (unless retained longer in connection with an incident or investigation)
ANPR data	30 days (unless retained longer in connection with an incident, dispute, or enforcement action)
Maintenance request records (Fixflo)	Duration of tenancy plus six years
Accounting records (Xero)	As required by HMRC — typically six years from the end of the relevant financial year
Website analytics data	As set out in our Cookie Notice

At the end of the applicable retention period, we will securely delete or anonymise your personal data.

11. Your Rights

Under the UK GDPR, you have the following rights in relation to your personal data:

- **Right of access** — you have the right to request a copy of the personal data we hold about you (a “subject access request”). When responding to your request, we are required to conduct a reasonable and proportionate search of our records.
- **Right to rectification** — you have the right to request that we correct any inaccurate or incomplete personal data.
- **Right to erasure** — you have the right to request that we delete your personal data in certain circumstances.
- **Right to restrict processing** — you have the right to request that we restrict the processing of your personal data in certain circumstances.

- **Right to data portability** — you have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller, where processing is based on consent or contract and is carried out by automated means.
- **Right to object** — you have the right to object to processing based on legitimate interests (including processing through AI tools and processing by Teambuild personnel) or for direct marketing purposes.
- **Right to withdraw consent** — where processing is based on consent, you have the right to withdraw that consent at any time.
- **Rights in relation to automated decision-making** — you have the right not to be subject to a significant decision based solely on automated processing (that is, a decision with no meaningful human involvement) which produces legal effects or similarly significant effects concerning you. We do not currently carry out any solely automated decision-making.

To exercise any of these rights, please contact our Data Protection Officer at office@braydenkane.com. We will respond to your request within one month. In certain circumstances, we may extend this period by a further two months, in which case we will inform you. Where your request requires us to conduct extensive searches, we may ask you to provide further information to help us locate the data you are seeking, and the one-month response period will pause while we await your clarification.

There is no fee for exercising your rights, unless your request is manifestly unfounded or excessive, in which case we may charge a reasonable fee or refuse to act on the request.

12. Data Protection Complaints

In accordance with section 164A of the Data Protection Act 2018 (as inserted by section 103 of the Data (Use and Access) Act 2025), we operate a formal data protection complaints procedure.

If you believe that we have not handled your personal data in accordance with data protection legislation, you have the right to make a complaint directly to us. You should raise your complaint with us in the first instance before escalating it to the Information Commissioner's Office.

12.1 How to Make a Complaint

You can submit a data protection complaint by any of the following means:

- **Email:** office@braydenkane.com (preferred)
- **Post:** Data Protection Officer, Brayden Kane Ltd, 161 Gloucester Crescent, Wigston, LE18 4YH
- **Telephone or in person:** by arrangement through the contact details above

To help us investigate your complaint efficiently, please include the following where possible:

- Your full name and contact details
- A description of your complaint and the personal data it relates to
- The dates and any reference numbers relevant to the matter
- What outcome you are seeking

You are not required to use any particular form or wording, and we will accept complaints however they are made. If you would prefer not to put your complaint in writing, please contact us to discuss alternative arrangements.

12.2 What Happens Next

Once we receive your complaint, we will:

- Acknowledge your complaint within 30 days of receipt
- Take appropriate steps to investigate your complaint without undue delay, including making appropriate enquiries
- Keep you informed of the progress of our investigation
- Inform you of the outcome of your complaint without undue delay, in plain and accessible language
- Inform you of your right to escalate your complaint to the Information Commissioner's Office if you are not satisfied with the outcome

12.3 The Information Commissioner's Office

If you are not satisfied with our response, you have the right to lodge a complaint with the ICO:

Information Commissioner's Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Telephone: 0303 123 1113

Website: <https://ico.org.uk>

13. Changes to This Notice

We may update this notice from time to time to reflect changes in our processing activities, legal requirements, or regulatory guidance. The current version is always available on our website. Where we make significant changes, we will take reasonable steps to notify you, for example by providing a revised copy of the notice or notifying you by email.

This notice was last updated in April 2026.

BRAYDEN KANE LTD

Part 2

CCTV and ANPR Policy

April 2026

CCTV and ANPR Policy — Version 2.0

1. Purpose

This policy governs the use of closed-circuit television (CCTV) surveillance systems and Automatic Number Plate Recognition (ANPR) technology by Brayden Kane Ltd. It sets out the basis on which these systems are used, how data is managed, the rights of individuals whose data is captured, and the responsibilities of those who operate the systems.

This policy should be read in conjunction with the Fair Processing Notice set out in Part 1 of this document and is compliant with the UK GDPR, as amended by the Data (Use and Access) Act 2025, and the Data Protection Act 2018.

Summary of changes from version 1.0

- Updated section 7 (Access) to reflect that authorised personnel engaged through Teambuild Consultancy Limited may access CCTV and ANPR data, with personnel based in the Philippines processing under the safeguards of an International Data Transfer Agreement.
- Added section 12 cross-referencing the data protection complaints procedure in the Fair Processing Notice.

2. Scope

This policy applies to all CCTV and ANPR systems operated by or on behalf of Brayden Kane Ltd at the following locations:

- Communal areas of residential properties owned and managed by Brayden Kane Ltd (including but not limited to entrance hallways, corridors, stairwells, car parks, and bin storage areas)
- Car parks where ANPR is deployed to manage vehicular access, enforce parking restrictions, and monitor vehicle movements
- The office premises of Brayden Kane Ltd at 161 Gloucester Crescent, Wigston, LE18 4YH

CCTV is not installed within individual residential units. ANPR cameras are directed at vehicle access points and parking areas only.

3. What Data Is Captured

3.1 CCTV

The CCTV systems capture visual images and video footage. Audio recording is not used. CCTV cameras are positioned to cover communal and public areas only and are not directed at private areas such as inside individual residential units, bathrooms, or changing areas.

3.2 ANPR

The ANPR system captures:

- Vehicle registration numbers (number plates)
- Images of vehicles (including the vehicle and its immediate surroundings at the point of capture)

- Date, time, and location of entry to and exit from the car park

Vehicle registration numbers are personal data under the UK GDPR because they can be linked to identifiable individuals through DVLA records.

4. Legal Basis

We process personal data captured by CCTV and ANPR on the following lawful bases:

4.1 Legitimate Interests (Article 6(1)(f))

For the general operation of CCTV and ANPR, we rely on our legitimate interests, which include:

- The prevention and detection of crime (including theft, vandalism, and antisocial behaviour)
- The safety and security of tenants, licensees, staff, visitors, and contractors
- The protection of our property and assets
- The management and security of car parking facilities, including the enforcement of parking restrictions and the prevention of unauthorised use
- The resolution of disputes and the provision of evidence in legal proceedings where necessary

We have conducted a legitimate interests assessment for both CCTV and ANPR to confirm that these interests are not overridden by the rights and freedoms of the individuals whose data is captured. These assessments are reviewed annually.

4.2 Recognised Legitimate Interests (Article 6(1)(ea))

The Data (Use and Access) Act 2025 introduced the lawful basis of “recognised legitimate interests” under Article 6(1)(ea) of the UK GDPR. Where we disclose CCTV or ANPR data to law enforcement agencies for the detection, investigation, or prevention of crime, we rely on this basis. Under Annex 1 to the UK GDPR, processing for these purposes does not require a balancing test, though we must still demonstrate that the processing is necessary.

Where CCTV is deployed in a workplace environment (our office), we have also considered our obligations under employment law and have informed staff accordingly.

5. Signage

Clear and prominent signage is displayed at all locations where CCTV and/or ANPR is in operation. Signage includes:

- The identity of the data controller (Brayden Kane Ltd)
- The purpose of the surveillance (CCTV and/or ANPR as applicable)
- Contact details for enquiries (including how to exercise data subject rights)

ANPR signage is displayed at the entrance to each car park where ANPR is in use, clearly informing drivers that their vehicle registration number will be recorded.

6. Retention

6.1 CCTV Footage

CCTV footage is retained for a maximum of 30 days from the date of recording, after which it is automatically overwritten.

6.2 ANPR Data

ANPR data (including vehicle registration numbers, associated images, and entry/exit timestamps) is retained for a maximum of 30 days from the date of capture, after which it is automatically deleted.

6.3 Extended Retention

CCTV footage or ANPR data may be retained for longer than 30 days in the following circumstances:

- Where an incident has been reported or identified that requires investigation
- Where data is required as evidence in connection with legal proceedings, a police investigation, or an insurance claim
- Where a parking enforcement dispute or appeal is ongoing
- Where a subject access request has been received and the data is being prepared for disclosure

In such cases, the relevant data will be securely extracted and retained separately for as long as necessary for the relevant purpose, and then securely destroyed.

7. Access

Access to CCTV footage and ANPR data is strictly limited to:

- The Data Protection Officer (Brayden Cooper)
- Authorised senior personnel of Brayden Kane Ltd
- **Authorised personnel engaged through Teambuild Consultancy Limited** for the purpose of providing property administration support, including reviewing footage in connection with tenant queries, incident logs, and parking enforcement matters. Such personnel are based in the Philippines and access footage under the safeguards described in section 7.1 below
- Law enforcement agencies, where a lawful request has been made
- Legal advisors, insurers, or other parties as required for the purposes set out in this policy
- Parking enforcement agents, where data is required for the enforcement of parking restrictions

Data will not be disclosed to any other party unless required by law or with the informed consent of the individuals concerned.

All access to CCTV footage and ANPR data is logged, recording the identity of the person accessing the data, the date and time of access, and the reason for access.

7.1 International Access by Teambuild Personnel

Teambuild Consultancy Limited personnel based in the Philippines may access CCTV and ANPR data as part of their property administration duties. Because the Philippines does not currently have a UK adequacy regulation, this access is governed by the following safeguards:

- A written International Data Transfer Agreement (IDTA) issued by the Information Commissioner's Office, between Brayden Kane Ltd and Teambuild Consultancy Limited

- A separate written Data Processing Agreement governing how Teambuild and its personnel handle CCTV and ANPR data
- A documented transfer risk assessment confirming that the level of protection for this data is not materially lower than the UK standard
- Mandatory technical measures including encrypted access, multi-factor authentication, application whitelisting on devices used to access footage, and a prohibition on local download, copying, screenshotting, or further sharing of footage
- A confidentiality undertaking signed by each individual at Teambuild who accesses CCTV or ANPR data
- Access only to footage relevant to the specific task being undertaken, with all access logged in accordance with this policy

8. Subject Access Requests

Individuals who are captured on CCTV footage or whose vehicle registration number has been recorded by ANPR have the right to request access to that data under Article 15 of the UK GDPR.

To make a subject access request, please contact us at office@braydenkane.com and provide:

- Your name and contact details
- The approximate date, time, and location of the footage or ANPR data you are requesting
- For CCTV: a description of yourself (or, where possible, a recent photograph) to help us identify you in the footage
- For ANPR: the vehicle registration number in question

We will respond within one month. In line with the Data (Use and Access) Act 2025, we are required to conduct a reasonable and proportionate search when responding to your request. Where footage also captures other identifiable individuals, we will take reasonable steps to obscure their images before disclosure.

9. Data Protection Complaints

If you wish to raise a concern or complaint about our use of CCTV or ANPR, you may submit a data protection complaint to us using the procedure set out in section 12 of the Fair Processing Notice (Part 1 of this document). We will acknowledge your complaint within 30 days and investigate it without undue delay.

If you are not satisfied with our response, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Telephone: 0303 123 1113 | Website: <https://ico.org.uk>

10. Security

We take the following measures to ensure the security and integrity of our CCTV and ANPR systems:

- Recording equipment is stored in a secure location with restricted physical access

- Access to digital footage and ANPR data is protected by password, multi-factor authentication, and is restricted to authorised personnel
- Devices used to access footage (including those used by Teambuild personnel) have application whitelisting and endpoint protection installed
- Local download, copying, screenshotting, or printing of footage is prohibited save where expressly authorised by the Data Protection Officer
- Where data is transmitted over a network, appropriate encryption and security measures are in place
- Systems are regularly maintained and inspected to ensure they are functioning correctly
- ANPR data is stored securely and separately from other business data where practicable

11. Review

This policy will be reviewed annually, or sooner if there are changes to relevant legislation, ICO guidance, or our CCTV or ANPR systems.

BRAYDEN KANE LTD

Part 3

Cookie Notice

April 2026

Cookie Notice — Version 2.0

1. Introduction

This Cookie Notice explains how Brayden Kane Ltd (“we”, “our”, “us”) uses cookies and similar technologies on our website. It should be read alongside the Fair Processing Notice set out in Part 1 of this document.

Our use of cookies is governed by the Privacy and Electronic Communications Regulations 2003 (PECR), as amended by the Data (Use and Access) Act 2025, and the UK GDPR.

2. What Are Cookies?

Cookies are small text files that are placed on your device (computer, tablet, or mobile phone) when you visit a website. They are widely used to make websites work, improve efficiency, and provide information to the website owner. The term “cookies” in this notice also covers similar technologies such as tracking pixels, web storage, and fingerprinting techniques.

3. The Cookie Rules

Under the Privacy and Electronic Communications Regulations 2003, as amended by the Data (Use and Access) Act 2025 with effect from 5 February 2026, cookies fall into three categories:

3.1 Cookies That Do Not Require Consent (Strictly Necessary)

These cookies are essential for the website to function properly. They include cookies used for security protection, fraud detection, user authentication, and maintaining user selections. These cookies are set without requiring your consent as the website cannot function without them.

3.2 Cookies That Do Not Require Consent But You Can Opt Out

Certain cookies may be set without prior consent, provided we give you clear information and a simple, free way to opt out. These include:

- **Statistical/analytics cookies:** Cookies used for the sole purpose of collecting aggregate statistical information about how visitors use our website, with a view to improving the website. These cookies do not identify, track, or monitor individual users.
- **Appearance/functionality cookies:** Cookies used for the sole purpose of adapting the appearance or functionality of the website to your preferences (such as language or display settings).
- **Software update cookies:** Cookies used to enable the delivery of automatic software updates.
- **Emergency assistance cookies:** Cookies used to detect and respond to security incidents or to provide emergency assistance.

Where we rely on these exemptions, you do not need to consent before the cookies are set, but you can opt out at any time using the methods described in section 5 below. If you opt out, the cookies will no longer be set on your device.

These exemptions apply only where the cookies are used solely for the specified purpose. If a cookie serves more than one purpose (for example, if an analytics cookie also feeds into advertising targeting), it will require your consent.

3.3 Cookies That Still Require Your Consent

Marketing and advertising cookies, and any cookies that are used for purposes beyond those described above (such as behavioural tracking or profiling), continue to require your prior consent. Wix may set marketing cookies that track visitors across websites to enable the display of relevant advertisements. These cookies will only be set if you give your consent through our cookie consent banner.

4. What Cookies Our Website Uses

Our website is hosted on the Wix platform. Wix sets cookies for various purposes including:

- Strictly necessary cookies for core website functionality and security
- Analytics cookies to help us understand how visitors interact with our website (this may include Wix's own analytics and, if enabled, Google Analytics)
- Functional cookies to remember your preferences and settings
- Marketing cookies set by Wix and its advertising partners (consent required)

We are reviewing which of Wix's analytics and functional cookies qualify for the PECR exemptions described above. In the meantime, our cookie consent banner gives you the option to accept or reject non-essential cookies.

5. Your Choices

You can manage your cookie preferences in the following ways:

- Using the cookie settings link on our website (where available) to opt out of analytics and functionality cookies or to withdraw consent for marketing cookies
- Adjusting your browser settings to block or delete cookies
- Using your browser's private or incognito mode

Please note that blocking strictly necessary cookies may prevent our website from functioning properly.

6. PECR Penalties

For transparency, we note that the Data (Use and Access) Act 2025 aligned PECR enforcement penalties with UK GDPR levels. Breaches of cookie and e-marketing rules can attract fines of up to £17.5 million or 4% of worldwide annual turnover. We take our cookie compliance obligations seriously.

7. Third-Party Cookies

As our website is hosted on Wix, some cookies are set by Wix and its partners rather than by us directly. We do not control the cookies set by third parties. For more information about Wix's use of cookies, please refer to Wix's Cookie Policy at <https://www.wix.com/about/cookie-policy>.

8. Changes to This Notice

We may update this Cookie Notice from time to time, particularly as further ICO guidance on the DUAA cookie exemptions is published. Any changes will be posted on our website.

9. Contact Us

If you have any questions about our use of cookies, please contact us at:

Brayden Kane Ltd

161 Gloucester Crescent, Wigston, LE18 4YH

Email: office@braydenkane.com

Last updated: April 2026