

PRIVACY AND DATA PROTECTION POLICY

UK GDPR • Data Protection Act 2018 • Data (Use and Access) Act 2025

Organisation	Scott Ford Management Ltd, trading as Scott Castle
Status	Public-facing policy and privacy information
Effective date	14 August 2026
Review date	May 2027, or earlier if the law, guidance or our processing changes

Plain-English summary. We use personal information only where we have a lawful reason, keep it secure, share only what is necessary, retain it only for an appropriate period, and respect the rights of the people whose information we hold. The Data (Use and Access) Act 2025 updates—but does not replace—the UK GDPR and Data Protection Act 2018.

1. Purpose and scope

This policy explains how Scott Ford Management Ltd, trading as Scott Castle (we, us or our), collects, uses, stores, shares and protects personal information. It applies to leaseholders, freeholders, residents, tenants, guarantors, applicants, landlords, directors of client companies, clients, suppliers, contractors, professional advisers, complainants, correspondents and visitors to our office or website.

It also sets the standards our directors, employees and contractors must follow. Separate, more specific notices may apply to employees, job applicants, CCTV, cookies or a particular service. Where a specific notice conflicts with this policy, the more specific notice applies for that processing.

2. Who is responsible for your information

Scott Ford Management Ltd is the data controller for personal information used for its own business purposes. In some property-management arrangements, we may act as a processor on the documented instructions of a client management company, freeholder, landlord or other controller, or the parties may each be separate or joint controllers. The applicable contractual arrangements determine those roles.

Data Protection Lead: Rob Scott

Email: rob@scottcastle.uk

The company—not an individual employee—is the controller where Scott Castle determines why and how personal information is used. Staff must refer data-protection queries, complaints, rights requests and suspected breaches promptly to the Data Protection Lead.

3. Data protection principles

We process personal information in accordance with the following principles:

- lawfully, fairly and transparently;
- for specified, explicit and legitimate purposes, and not incompatibly reused;

- limited to what is adequate, relevant and necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form only for as long as necessary;
- protected by appropriate technical and organisational security; and
- with records that demonstrate our accountability and compliance.

4. Information we collect and where it comes from

Depending on the relationship and service, we may collect the following categories of information:

- identity and contact details, including names, addresses, telephone numbers, email addresses, dates of birth and signatures;
- property, lease, tenancy, ownership, occupancy and company-director information;
- financial and transactional information, including bank details, rent, service-charge, payment and arrears records;
- application, referencing, affordability, identity-verification, right-to-rent, anti-fraud and credit-check information;
- communications, correspondence, call notes, complaints, maintenance reports, inspection records and photographs;
- access, security and visitor information, including keys, access codes, entry records and CCTV images;
- supplier and contractor details, qualifications, insurance, invoices and work records;
- technical information from our website, systems and communications, such as IP address, device, security and audit logs; and
- limited special category or criminal-offence information where genuinely necessary, for example health or vulnerability information needed to make reasonable adjustments, protect someone, manage an emergency, or meet a legal requirement.

We normally obtain information directly from you, but may also receive it from landlords, freeholders, management companies, joint owners, occupiers, referees, letting and property portals, referencing and identity-verification providers, previous agents, contractors, professional advisers, insurers, local authorities, utility providers, emergency services, publicly available registers and other lawful sources.

5. Why we use your information

We only use personal information when we have a lawful reason to do so. The reason will depend on the service we are providing and our relationship with you.

We may use your information for the following purposes:

- **Providing our services:** We use information to manage properties and tenancies, communicate with clients and residents, arrange repairs and inspections, instruct contractors, collect rent or service charges and maintain property records.
- **Entering into or fulfilling a contract:** We may need information to process a tenancy application, prepare an agreement or provide a service directly to you. Where our contract is with another party, such as a management company or freeholder, we will normally rely on legitimate interests instead.
- **Managing properties effectively:** We have a legitimate interest in using information to look after buildings, deal with maintenance and complaints, manage contractors, collect money and protect the interests of our clients, property owners, leaseholders, tenants and residents.
- **Complying with the law:** We may need to use and retain information to meet legal, tax, accounting, safety, property-management, anti-fraud or regulatory requirements.

- **Protecting people and property:** We may use information for CCTV, access control, building safety, emergency repairs, safeguarding concerns and the prevention or investigation of crime.
- **Operating our business securely:** We use information where necessary to maintain our computer systems, backups, financial records, security logs and audit trails.
- **Marketing our services:** If we send promotional information, we will do so only where the law allows it. You can ask us to stop sending marketing at any time.

When we use consent

We do not rely on consent for routine property or tenancy management. This information is normally needed to provide our services, fulfil a contract, comply with the law or manage a property effectively.

Where we do ask for consent, you will have a genuine choice. You may withdraw your consent at any time without affecting anything we lawfully did before it was withdrawn.

Recognised legitimate interests

The Data (Use and Access) Act 2025 introduced a lawful basis called recognised legitimate interests. In limited circumstances, this may allow us to use or share information for specified public-interest purposes, such as preventing crime, safeguarding a vulnerable person or assisting an organisation with an official public function.

We will use this basis only where the relevant legal condition is met and the use of the information is necessary. It does not remove our other data-protection responsibilities.

Special category and criminal-offence information

Where we process more sensitive information, we identify both an Article 6 lawful basis and the additional Article 9 or Data Protection Act 2018 condition required by law. We limit access and apply safeguards appropriate to the risk. We do not routinely seek this information unless it is necessary.

6. Sharing personal information

We share only the minimum information reasonably necessary for a defined purpose and only where there is a lawful basis. Depending on the circumstances, recipients may include:

- landlords, freeholders, management companies, resident-management or right-to-manage companies and their directors;
- tenants, leaseholders, residents, guarantors and authorised representatives where appropriate;
- contractors, surveyors, engineers, cleaners, grounds contractors and other property-service providers;
- referencing, identity, credit, deposit-protection, inventory, payment, accounting, software, hosting, communications and IT-security providers;
- insurers, brokers, loss adjusters, solicitors, accountants, auditors, debt-recovery providers and other professional advisers;
- utility companies, local authorities, regulators, ombudsman/redress schemes, courts, tribunals, police and emergency services; and
- a purchaser, successor or adviser in connection with a lawful sale, transfer or reorganisation of a business or managed property portfolio.

Where a recipient processes information for us, we use appropriate written terms requiring confidentiality, security, assistance with rights and breaches, deletion or return at the end of the service, and use only on our documented instructions. Where the recipient is an independent controller, it has its own legal duties.

Our responsibility does not simply end when information is transferred: we remain accountable for ensuring that our disclosure was lawful, fair, secure and appropriately governed.

A contractor must not use contact, access or property information for any unrelated purpose, disclose it without authority, retain it longer than necessary, or contact an occupier except as required to complete authorised work.

7. International transfers

Some service providers may store or access information outside the United Kingdom. Before making a restricted transfer, we use a lawful transfer mechanism and assess whether the protection is not materially lower than under UK law. This may include UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to approved contractual clauses, or another permitted safeguard. Further information about relevant safeguards is available on request, subject to lawful confidentiality restrictions.

8. Security and access

We apply security measures proportionate to the nature and risk of the information, including role-based access, strong authentication, password controls, encryption where appropriate, firewalls, malware protection, secure backups, audit logging, controlled remote access, staff training, confidentiality requirements, supplier due diligence, physical office security, alarm systems, secure doors/shutters and CCTV.

Access is limited to authorised people who need the information for their work. Staff must not use personal accounts or unauthorised devices or services for company information, and must verify recipients before sending information. Paper records must be stored securely and disposed of confidentially.

9. Retention and deletion

We keep personal information only for as long as necessary for the purpose for which it was collected, including legal, accounting, tax, insurance, limitation, regulatory and dispute requirements. We review and securely delete, anonymise or destroy information when it is no longer required.

Record type	Typical retention approach
Tenancy, client and property-management records	Usually seven years after the relationship or relevant transaction ends, unless a longer or shorter period is justified.
Financial and accounting records	Usually six years after the relevant financial year or transaction, subject to tax, audit and legal requirements.
Unsuccessful applications and referencing	Usually up to 12 months after the application closes, unless needed longer for a complaint, fraud concern or legal claim.
General enquiries and routine messages	Usually up to 12 months, unless moved into an active property, tenancy, complaint or client record.

Record type	Typical retention approach
Email and calendar records	Managed by purpose and retention schedule; relevant messages are retained with the underlying property, tenancy, financial or complaint record rather than kept indefinitely merely because they are email.
CCTV	Normally up to 30 days, unless footage is required for an incident, investigation, complaint or legal claim.
Supplier and contractor records	For the engagement and normally six or seven years afterwards where required for accounts, insurance, claims or contract records.
Rights requests, complaints and breaches	Normally at least six years from closure where needed to demonstrate compliance or manage a legal claim.

These periods are guides, not automatic entitlements to keep every item. Litigation holds, safeguarding, fraud prevention, insurance or regulatory requirements may justify longer retention. Backups are protected and deleted or overwritten through controlled cycles.

10. CCTV and office visitors

CCTV is used for the legitimate interests of protecting people, premises, information and property, and for investigating incidents. Signs are displayed where required. Access to recordings is restricted and disclosure is made only where lawful and necessary. CCTV is not used for unrelated monitoring. Requests for footage are assessed against the rights of other people appearing in it, and redaction may be required.

11. Automated decision-making and profiling

We do not currently make decisions that produce legal or similarly significant effects solely by automated means without meaningful human involvement. Referencing, fraud, identity or credit services may use automated tools to support an assessment, but a person can review relevant decisions where required.

If we introduce significant solely automated decision-making, we will identify a lawful basis, provide the required information and safeguards, allow representations and human intervention where the law requires, and carry out a data protection impact assessment where appropriate. Additional restrictions apply to special category information.

12. Cookies, website forms and communications

Our website and online forms may collect contact details and limited technical information needed to operate, secure and improve the service. We provide separate cookie information where storage or access technologies are used. Consent is obtained for non-essential cookies unless a specific PECR exemption applies. Information submitted through portals or third-party websites may also be processed under that provider's privacy notice.

Our telephone system does not routinely record calls. A property portal or other third-party service may record calls or communications under its own notice. We do not use personal information for unrelated marketing, and every electronic marketing message will include an appropriate method to opt out.

13. Re-use of information and new purposes

Before using information for a new purpose, we assess whether the new use is compatible with the original purpose, whether a new lawful basis is required, and whether updated privacy information must be provided. We document the assessment where appropriate. The 2025 Act treats certain limited re-uses as compatible or provides specific exceptions, but we will still apply necessity, data minimisation, security and all other applicable safeguards.

14. Your rights

Subject to conditions and exemptions in the law, you may have the right to:

- be informed about how your information is used;
- request access to your personal information and supplementary information;
- have inaccurate information corrected and incomplete information completed;
- request erasure in certain circumstances (the right is not absolute);
- request restriction of processing in certain circumstances;
- receive certain information in a structured, commonly used and machine-readable format and transmit it to another controller;
- object to processing based on legitimate interests and object at any time to direct marketing;
- withdraw consent at any time, where consent is the lawful basis, without affecting earlier lawful processing; and
- seek safeguards and human involvement in relation to qualifying automated decisions.

To exercise a right, email rob@scottcastle.uk. We may ask for information reasonably necessary to verify identity and locate the records. We normally respond within one month. The law permits an extension in certain complex cases and allows us to refuse or charge a reasonable fee for requests that meet the statutory threshold. Following the 2025 Act, searches for information in response to an access request must be reasonable and proportionate; this does not reduce our duty to conduct a genuine search and explain our response.

15. Data protection complaints

You may complain if you believe we have used your personal information incorrectly, failed to respect your rights, or handled a request inadequately. Complaints may be made by email to rob@scottcastle.uk or in writing to Scott Ford Management Ltd, trading as Scott Castle, at our published office address. Please describe what happened, the outcome sought and any relevant dates or documents.

We will:

- make it clear and straightforward to raise a complaint and provide reasonable assistance;
- acknowledge a data-protection complaint within 30 days;
- investigate fairly, proportionately and independently of the subject of the complaint where practicable;
- keep you appropriately informed and respond without undue delay;
- tell you the outcome, the reasons, any action taken and your right to complain to the Information Commissioner; and
- record the complaint and outcome so that we can identify trends and demonstrate compliance.

You can also complain to the Information Commissioner's Office (ICO), although the ICO normally expects you to raise the issue with us first. Visit ico.org.uk/make-a-complaint or call 0303 123 1113.

16. Personal data breaches

Staff and contractors must report any suspected loss, unauthorised disclosure, alteration, access, destruction or unavailability of personal information immediately to the Data Protection Lead. We investigate, contain and document incidents, assess risk, and notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of a notifiable breach. Where a breach is likely to result in a high risk to people, we also notify affected individuals without undue delay unless a lawful exception applies.

17. Governance, training and accountability

- Staff receive proportionate data-protection and information-security training and must follow this policy and related procedures.
- We maintain appropriate records of processing, lawful-basis assessments, processor arrangements, retention, rights requests, complaints and breaches.
- We complete data protection impact assessments before high-risk processing and build privacy into new systems and services by design and default.
- Suppliers are selected and monitored with regard to security, privacy, confidentiality, data location and deletion arrangements.
- This policy is reviewed at least annually and sooner when our processing, technology, contracts, legislation or ICO guidance materially changes.

18. Contact and regulatory information

Scott Ford Management Ltd is registered with the Information Commissioner's Office where registration is required. The current registration certificate and reference are available from our office or can be checked through the ICO's register of fee payers.

Data Protection Lead: Rob Scott

Email: rob@scottcastle.uk

This policy is displayed or made available through our website and office and may be provided electronically or in another accessible format on request.

Appendix A — Internal contractor data-handling instruction

The following wording should appear on, or be incorporated into, contractor work orders where personal information is disclosed:

Personal information supplied with this work order is confidential and may be used only to arrange and complete the authorised work. Use only the minimum information necessary; keep it secure; do not disclose it to another person without Scott Castle's authority or another lawful basis; do not use it for marketing or any unrelated purpose; report any loss, misdirection or unauthorised access immediately; and securely delete or return it when no longer required, subject to any legal retention obligation. By accepting the instruction, you agree to comply with applicable data-protection law and your contractual duties.

Appendix B — Principal legal and guidance sources

- [Data \(Use and Access\) Act 2025](#)
- [ICO: What the Data \(Use and Access\) Act means for organisations](#)

- [ICO: Summary of changes to data-protection law](#)
- [ICO: Recognised legitimate interests](#)
- [ICO: Right to be informed](#)
- [ICO: Data sharing and lawful basis](#)

Document owner: Data Protection Lead | Approved by: Directors of Scott Ford Management Ltd |
Version: 2.0 (August 2026)