Data Protection Policy

Policy Owner:	Data Protection Officer
Policy Lead:	Executive Director of Finance
Approved by:	Executive Team
Approved date:	July 2024
Next review date:	July 2025

Contents

Purpose and scope of the policy
This policy sets out how, as a responsible custodian of your data, we'll manage, collect and process your personal data in accordance with relevant data protection legislation and regulatory requirements. It applies to you if we collect or process your data – for example, if you're a potential or existing customer or colleague.

1. Policy

1.1 As a responsible custodian of your data, we'll manage, collect and process your **personal data,** including **special category data** (please see definitions section of this policy), in accordance with relevant data protection legislation and regulatory requirements. We'll:

- Be open and honest about our collection and ongoing use of data.
- Only collect data that we need to perform (in accordance with our Equality, Diversity and Inclusion Policy) our roles as a housing association and an employer, or for work that arises from our charitable status – and keep the data for the minimum amount of time necessary to perform these roles.
- Keep information and documentation secure and guard against the accidental loss, corruption or destruction of data that we hold by ensuring that appropriate technical, organisational and security measures are in place (as set out in our Data and Technology policies) in line with Article 5 (1) (f).
- Adhere at all times to the seven data protection principles set out in the Data Protection Act, while taking into account the importance of the individual rights of data subjects:
    - Lawfulness, fairness and transparency
    - Purpose limitation
    - Data minimisation
    - Accuracy
    - Storage limitation
    - Integrity and confidentiality (security)
    - Accountability
- Provide Moat colleagues with appropriate data protection training.

1.2 In relation to processing personal data, we're primarily a data controller. In some circumstances, we and our contractors process personal data as data processors. We'll always identify a valid lawful basis for processing personal data before processing begins, including additional conditions for processing special category data.

1.3 Colleagues who need to process special category data must contact the Data Protection Officer before undertaking any processing, and at least one of the following lawful bases must apply, in line with Article 6 of the UK GDPR:

- The processing is necessary for one or more of the following:
  - to perform a task in the public interest or for an official function
  - for fulfilling a contract or to enter into a contract
  - to comply with the law (excluding contracts)
  - to protect the life of the individual, or another individual
  - for out legitimate interests or the legitimate interest of another party, unless it would undermine your right to privacy
- Consent has been given freely, specifically, informatively and unambiguously – We'll inform you of your absolute right to withdraw consent at any time (Please see the definitions section of this policy for a definition of consent).

1.4 We recognise the legal rights you have in relation to your data and will ensure that appropriate information is provided so that you understand how to exercise your rights, and so that we can respond and deal with these appropriately. These rights include:

- The right to be informed (see below)
- The right of access to personal data (please see section 7 of this policy)
- The right of portability of personal data
- The right of rectification of personal data (please see section 8 of this policy)
- The right of erasure of personal data (please see section 9 of this policy)
- The right to restriction of processing
- The right to object to data processing operations under some circumstances (please see section 10 of this policy)
- The right not to be subject to decisions made by automated processing under some circumstances (please see section 11 of this policy)
- The right of complaint about our processing of personal data and the right to a judicial remedy and compensation.

1.5 We'll inform you about the collection and use of your data in line with the UK General Data Protection Regulation (GDPR) transparency requirement. We'll do this by continuing to ensure that our Privacy Statement is published on our website and that it sets out:

- The types of data we process, the purposes for which we process it and the legal basis for doing this
- How long we keep it, who we share it with and how you can exercise your rights as set out above.

1.6 We'll make every effort to ensure that you're aware of our Privacy Statement and any subsequent updates we make to it before and throughout the time we process your information. We'll do this whenever you share any information with us including when you make an application for a home or a job and when you

sign a tenancy agreement, and we'll proactively engage with you to advise you of any amendments we make to it – We'll keep it under review and, where necessary, update it from time to time to incorporate any new uses of data.

1.7 We'll make every effort to maintain the data we hold by ensuring it's as accurate and up to date as possible. Any data which cannot reasonably be assumed to be accurate and up to date will be treated appropriately through erasure or anonymisation.

1.8 For any instances or new data processing, or a new project that involves the use of personal data, we'll ensure that a Data Protection Impact Assessment is completed. We'll follow the principle of Privacy by Design to build data protection into all of our data processing activities.

1.9 In the event of a personal data breach, unless its unlikely to result in a risk to your rights and freedoms, we'll notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach (Risks to your rights and freedoms can include, but are not limited to, risk of identity theft or fraud, damage to reputation, loss of control over personal data or risk of discrimination). To enable us to do this, it's important that Moat colleagues understand their responsibilities under this Policy and report any data breaches to our Data Protection Officer as soon as possible. The Data Protection Officer will, without undue delay, undertake an assessment of the issue, considering the likelihood and severity of the risk to the data subject's rights and freedoms, and the harm to any individuals affected. We'll cooperate fully with the ICO and any individuals (for example colleagues or customers) at all times throughout this process.

1.10 We operate a zero-tolerance policy towards individuals who deliberately and unlawfully obtain or disclose personal data and will take appropriate and proportionate action where required. We acknowledge that human error can occur and encourage all colleagues to report any and all suspected or actual data breaches. We're committed to implementing learnings to prevent future occurrences.

1.11 Failure to comply may result in disciplinary action that may lead to dismissal, in addition to the possibility of an individual being criminally prosecuted under the GDPR and the DPA and/or liable to pay compensation in any civil action.

2. Data protection training for colleagues

2.1 We'll provide data protection training for colleagues as part of the induction process, and annually thereafter.

2.2 We'll provide more specific training for colleagues with specific roles or in specific departments on an individual basis as required and determined by Data Owners and Data Stewards.

2.3 If actual or suspected data protection issues arise, we'll use these as a learning opportunity for the whole organisation, drawing on lessons learnt from each issue and distributing them to teams to raise awareness and prevent future recurrence.

3. Data Protection Impact Assessments

3.1 We'll adopt a risk-based approach to processing personal data, ensuring that we assess any risks to privacy or to the rights and freedoms of people before commencing, commissioning or changing data processing activities.

3.2 To support this, Data Protection Impact Assessments will be undertaken on any proposed:

- new or revised policy
- new or changing data processing activity
- new or changing system within which data is held
- new or changing data sharing activity.

4. Continuous improvement, audit and compliance checking

4.1 We'll undertake periodic compliance checks to test whether our policies and procedures are being complied with and to test the effectiveness of control measures.

4.2 We'll record these audits and take corrective action where non-conformance is found. Any non-conformance will be reported to the Data Steering Group and any sustained non-conformance will be reported to the Audit and Risk Committee.

5. Record keeping and accountability

5.1 We'll maintain records of processing activities to support our policy of transparency in relation to processing activities that we control, undertake or otherwise commission.

5.2 We'll identify and record information assets, documenting the source of personal data we hold, our legal basis for processing it and who has access. We'll ensure that the register remains accurate by reviewing it on a quarterly basis.

6. Data sharing, disclosure and transfer

6.1 We'll only share personal data with, or otherwise disclose personal data to, other organisations and third parties where there's a legal basis for doing so and the data sharing is necessary for specified purposes. When it is in our legitimate interests, we will share your information with our contractors and partner organisations who deliver services for us (like repairs, satisfaction surveys and market research etc.).

6.2 Where information is processed by third parties on our behalf, or we're sharing information with a third party in order to carry out our duties, we'll ensure that there are UK General Data Protection Regulations (GDPR) compliant clauses

regarding the protection of the data and the security of the information in the contract, or that a supplementary data sharing agreement is in place. Data sharing agreements must be approved by the Data Protection Officer, who will maintain a register of all such agreements.

6.3 We'll provide information to colleagues setting out safe and approved methods of transferring personal data to recipients in our Data Transfer Policy, which must be used for all data transfers. Disciplinary action will be taken against anybody who fails to observe this policy unless approval has been received in writing from the Data Protection Officer.

6.4 In some exceptional circumstances, the law allows us to make certain disclosures as exemptions from GDPR (as set out below) but we won't routinely rely on these exemptions – Each disclosure will be considered on a case-by-case basis and we'll keep suitable documentation recording the reason for the decision.

- to safeguard national security
- the maintenance of effective immigration control
- prevention or detection or crime including the apprehension or prosecution of offenders
- assessment or collection of tax or duty
- discharge of regulatory functions (includes health, safety and welfare of persons at work)

6.5 We'll only transfer personal data to jurisdictions outside of the United Kingdom if it has a recognised and adequate level of protection for data protection purposes. Such a transfer requires the express approval of our named Data Protection Officer.

6.6. We will only release your data to anybody other than you where we have received your authorisation to do so (such as a document that you have signed agreeing for the release of your data to another specified party, or by recorded verbal agreement for a specified purpose), or where an exemption has been identified and applied for the release of that information (for example, where we are legally obliged to provide that information).

7. Your right of access to personal data – Data Subject Access Requests (DSARs)

7.1 You have a legal right to access and receive a copy of your personal data, and other supplementary information by making a subject access request (SAR). You can make a SAR verbally or in writing, including via social media, and a third party can make the request on your behalf.

7.2 We'll consider your SAR fairly and respond within the statutory time limit of one calendar month from receipt of your request. We may extend the time limit by up to a further two months if the request is complex or if we've received a number of requests from you. If we do this, we'll confirm this to you and explain why within one month of receiving your request.

7.3 We'll perform a reasonable search for the requested information, disclose the information securely and provide it in an accessible, concise and intelligible format. We'll retain electronic copies of our responses to SARs for one year to help ensure that we don't duplicate effort in responding to any future requests – These copies will be confidentially destroyed after one year.

7.4 In some circumstances, we may refuse your SAR. Any decision to do so will be taken by our Data Protection Officer. If we decide to refuse your SAR, we will, within one month of receiving your SAR, notify you of our decision and the reason(s) for the decision, your right to make a complaint to the Information Commissioner's Office (ICO) and your right to seek to enforce your right of access to your personal data through the courts. We may refuse to provide the information you've requested if an exemption or restriction applies, or if your request is manifestly unfounded or excessive. Where an exemption applies to the facts of your request (for example, if responding to the request would break another UK law), we may refuse to provide either some or all of the requested information – This decision will be made on a case by case basis.

7.5 In some circumstances, we may make a reasonable charge to respond to your SAR if its manifestly unfounded or excessive – Any decision to do so will be taken by our Data Protection Officer.

7.6 We'll consider your SAR to be manifestly unfounded if it's used to cause disruption to the business – for example if:

- You clearly have no intention to exercise your right – as evidenced, for example, by an offer to withdraw the request if compensation is provided
- Your request is malicious in intent
- Your request explicitly states that you intend to cause disruption
- Your request relates to a personal grudge with a colleague

7.7 We'll consider your SAR to be manifestly excessive if the request itself is unreasonable. This decision will be based on whether the request is proportionate when balanced with the burden or costs involved in dealing with the request, taking into account:

- The nature of the requested information
- The context of the request
- Available resources
- Whether the request is a repeat of a previous request.

8. Your right of rectification of personal data

8.1 If you ask us to rectify (correct) your personal data (for example, if any of the information we hold about you is incorrect or misleading), we'll take reasonable steps to establish whether the data is accurate and to correct it if necessary, taking into account any evidence and arguments to support your request, as well as any steps we've already taken to verify the accuracy of the data prior to

challenge. Where we've shared the information with others, we'll contact them and ask them to correct your data too.

8.2 In some instances, we might need to record the fact that we'd made a mistake and have since rectified it. Recording of opinions within our systems are not generally permitted. If an opinion must be recorded, the record should clearly that that it's an opinion and whose opinion it is.

8.3 In some circumstances, we can apply exemptions, which will be assessed on a case-by-case basis, including whether we deem the request to be manifestly unfounded or excessive. If we conclude that we've undertaken an appropriate level of due diligence in relation to the information and decide not to rectify your data, or that the request is manifestly unfounded or excessive, we'll inform you of this decision and your right to make a complaint to the Information Commissioner's Office (ICO) and your right to seek to enforce your right of rectification of your personal data through the courts. For customers, we'll keep a record of this decision on our Customer Relationship Management (CRM) system.

8.4 Whatever the outcome, we'll respond to you within one calendar month of receiving your request. We may extend the time limit by up to a further two months if the request is complex or if we've received a number of requests from you.

9. Your right of erasure of personal data

9.1 You have the right to request that we erase your personal data from our records if:

- The data is no longer necessary for the purposes for which we originally collected or processed it,
- We're relying on consent as the lawful basis for holding the data, and consent is being withdrawn,
- We're relying on legitimate interest as the basis for processing the data, you object to the processing and there's no overriding legitimate interest reason for us to continue processing it,
- We're processing data for direct marketing purposes, and you object to that processing,
- We've processed the data unlawfully,
- We need to comply with a legal obligation.

10. Your right to object to data processing operations

10.1 We'll notify you of your right to object to direct marketing in our Privacy Statement, which we'll continue to make available on our website and make accessible when you first consent to the marketing. We'll stop processing personal data for direct marketing purposes as soon as we receive an objection, and no later than one calendar month from receiving the objection.

10.2 You have the right to object to processing based on legitimate interests, and we'll stop processing the data unless we can demonstrate compelling legitimate

grounds for the processing which override your interests, rights and freedoms, or to establish, exercise or defend a legal claim.

11. Your rights in relation to automated decision making and profiling

11.1 We'll only profile your data to enable us to tailor the support we provide, for example, to assess the likelihood of your falling into rent arrears. We'll only undertake profiling on data for which the lawful basis for processing is for the performance of a contract between us (for example, our tenancy agreement).

11.2 To make a request for human intervention, or to contest a decision made by automated profiling, please contact our Data Protection Officer, who will assess the request within one calendar month.

12. Your rights in relation to portability of your data

12.1. You have the right to receive copies of the data you have provided to us in a structured data file (in a commonly used and machine-readable format) to transfer to another provider. This applies where we have relied on your consent to use and process your personal data or need to process it in connection with your contract (for example, a tenancy agreement or lease). You can contact our Data Protection Officer to exercise this right.

13. Your right to restrict our processing of your data

13.1. You have the right to request that we limit the way we use your data in some circumstances. This could be because you contest the accuracy of the data and wish to verify it, the data has been processed unlawfully, we no longer need your personal data but you need us to keep it to establish, exercise or defend a legal claim, or you have objected to the processing and we are considering our legitimate grounds to hold it. You can contact our Data Protection Officer to exercise this right.

13.2. To exercise any of your rights, or to make a complaint in relation to the processing of your data, please contact our Data Protection Officer at customer@moat.co.uk or by writing to: Data Protection Officer, Moat, Mariner House, Galleon Boulevard, Crossways, Dartford, Kent DA2 6QE. You also have the right to lodge a complaint with the Information Commissioner's Officer at casework@ico.org.uk, or in writing at: Information Commissioner's Officer, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

14. Cookies

14.1. We collect cookies when you use our website or associated apps so that we can better understand our users' needs and optimise our service and user experience. These websites and apps use cookies and other technologies to collect data on users' behaviour and their devices. We will only ever collect and store pseudonymised user profiles and we and our service providers will never sell any of the data collected.

14.2 The information contained in the data transmitted to Moat is required for the provision of services now and in the future. You can opt out of being tracked by Google Analytics across all websites.

Roles and responsibilities

Moat colleagues (employees), volunteers, casual / temporary workers and contractors:

- Adhere to this policy, the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR) at all times and understand your obligations
- Always process data safely and securely
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay to our Data Protection Officer
- Undertake the required training

Data and Technology Team:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Check and scan security hardware and software regularly to ensure it's functioning properly
- Implement data deletion and/or anonymisation on request or at such time as the retention schedule determines

Data Protection Officer (DPO):

- Keep the Board abreast of Moat's data protection responsibilities, risks and issues
- Ensure that robust data protection policies and procedures are in place and regularly reviewed
- Arrange data protection training and advice for all colleagues (employees) and contractors as necessary
- Provide advice around Moat's data protection responsibilities
- Be the first point of contact with data subjects and the information commissioner
- Be the first point of contact for, and oversee the investigation and conclusion of data related incidents and reporting of these to the appropriate bodies
- Maintain the Record of Processing Activities and Information Asset Register
- Provide advice and oversight of data related documentation and agreements, including but not limited to:
    - Data Sharing Agreements
    - Data Protection Impact Assessments (DPIAs)
    - Non-Disclosure Agreements
    - Legitimate Interest Assessments
    - Contractual clauses in relation to data protection

Chief Executive Officer (CEO):

- Ensure that appropriate mechanisms are in place to support service delivery and continuity.

Data owners:

- Ensure compliance with data protection legislation and good practice in respect of your assigned data asset(s).
- Understand how data is used in the business and how, who has access to it and why
- Understand and address risks to the data and the organisation

Data stewards:

- Day to day compliance and application of good practice in respect of your assigned data asset(s).

Data Steering Group:

- Oversee and monitor the delivery of the Data and Technology Strategy
- Act as a support group for data owners, driving best practice through policy, procedure and training

People Services Team:

- Ensure compliance with data protection in relation to the management of the workforce, including recruitment and retention
- Ensure that adequate training is provided to all colleagues (employees)

Partners and third parties:

Any third party or organisation that is commissioned to process data or receives data from us or is able to access any data which is within our custody is expected to comply with this policy where applicable.

Definitions

Personal Data:
Any information relating to an identified, or identifiable, living individual, such as name, identification number, location data, online identifier or other factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Processing:
Any collection, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying of personal data either via automated or manual means.

Data subject:
The identified or identifiable individual whose personal data is held or processed.

Data controller:
A person or organisation that determines the purposes and means of processing personal data.

Data processor:
A person or organisation, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach:
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data Protection Impact Assessment (DPIA):
An exercise which analyses the risk of a processing activity to Data Subjects. This could include Privacy Impact Assessments or Legitimate Impact Assessments.

Information asset:
Any single entity where personal data is collected and stored in an organised way. This could include spreadsheets, paper and digital folders, cabinets and systems.

Legitimate Interest Assessment (LIA):
A type of DPIA, used specifically when relying on Legitimate Interest as the legal basis for processing.

Criminal data:
Information about an individual that relates to criminal activity, allegations, investigations and proceedings.

Consent: We interpret consent to be defined within the UK General Data Protection Regulation (GDPR) and appreciate that consent won't be valid unless:

- there's a genuine choice of whether or not to give consent
- consent has been explicitly and freely given, and represents a specific, informed and unambiguous indication of your wishes that signifies agreement to the processing of personal data relating to you
- the consent was given through statement made by you or by a clear affirmative action taken by you
- we can demonstrate that you've been fully informed about the data processing to which you've consented and can provide that we've obtained valid consent lawfully
- we provide a mechanism to withdraw consent at any time, ensure that withdrawing consent is as easy as it was to give it, and that you've been informed about how to exercise your right to withdraw consent
- where there's an imbalance of power, any alternative legal basis for processing is valid, necessary, fair and transparent.

Special category data: The UK General Data Protection Regulation (GDPR) defines special category data as:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership
- genetic data
- biometric data (where used for identification purposes)
- data concerning health, a person's sex life or sexual orientation.

Cookies
Cookies are small pieces of information, normally consisting of just letters and numbers, which online services provide when users visit them.

Pseudonymise
A technique that replaces, removes or transforms information that identifies individuals, and keeps that information separate.

Data Subject Access Request (DSAR)
A data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.

Equality, Diversity and Inclusion

This policy will be delivered in accordance with our Equality, Diversity and Inclusion Policy. An Equality Impact Assessment was completed for this policy and considered as part of the approval process.

Data protection

A Data Impact Assessment was completed for this policy and considered as part of the approval process. We're clear that successful implementation of this policy will be dependent on us ensuring that the development and delivery of all our strategies, policies and procedures supports the delivery of this policy.

Related legislation and regulations

- Data Protection Act 2018
- UK General Data Protection Regulations (GDPR)
- Privacy and Electronic Communications Regulations

Related policies and procedures

- Assets and Liabilities Register Policy
- Business Continuity Management Policy
- Equality, Diversity and Inclusion Policy

- Data and Technology Security Policy
- Data and Technology Acceptable Use Policy
- Data and Technology Third Party Access Policy
- Data and Technology Software Standards Policy
- Data Transfer Policy
- Risk Management Policy
- Cookie Policy

Customer engagement
Customers' views were not sought when reviewing this policy.

Document Revision History (Record of any changes made to the policy)		
Date	**Changes approved by**	**Details of changes made**