



DATA PROTECTION, PRIVACY AND INFORMATION GOVERNANCE POLICY

Responsible information • secure systems • trusted partnerships

PURPOSE

To ensure NEWPOINT handles personal information lawfully, fairly, transparently and securely throughout property sourcing, housing management, employment and partnership delivery.

Document owner	Applies to	Review
NEWPOINT Housing Group	Directors, staff, contractors, systems and partners	At least annually and after material change

1. Commitment, scope and status

NEWPOINT depends on accurate and trusted information to acquire properties, manage agreements, coordinate repairs and support residents. We collect only what is needed, explain how it is used, restrict access and keep a clear record of important decisions.

This policy applies to

- Resident, household, applicant, landlord, agent, contractor, employee and partner information.
- The NEWPOINT CRM, email, cloud storage, mobile devices, paper records, photographs, call notes and exported reports.
- Information received directly or from councils, prime contractors, landlords, advisers and service providers.
- All stages from collection and use through sharing, correction, retention and secure deletion.

Core commitments

Principle	NEWPOINT standard
Lawful and fair	Identify and record the purpose and lawful basis before use.
Transparent	Give clear privacy information and avoid unexpected uses.
Limited	Collect the minimum information needed for the stated purpose.
Accurate	Correct material errors and keep operational records current.
Secure	Use appropriate technical and organisational safeguards.
Accountable	Record decisions, ownership, incidents and assurance activity.

POLICY, NOT A PRIVACY NOTICE

This internal policy sets the control framework. NEWPOINT must also issue suitable privacy notices to the people whose information it handles.

2. Legal framework and governance roles

NEWPOINT's primary framework is the UK GDPR and Data Protection Act 2018, as amended. Other duties may also apply, including confidentiality, employment, housing, safeguarding, contract and electronic-marketing rules.

Role	Responsibility
Controller	Decides why and how personal information is used; usually NEWPOINT for its own operations.
Joint controller	Shares purposes and decisions with another controller; responsibilities must be agreed transparently.
Processor	Handles information only on documented controller instructions and under an appropriate contract.
Data subject	The identified or identifiable person the information relates to.
Information lead	Maintains records, coordinates rights and incidents, advises on risk and monitors controls.
System owner	Controls configuration, authorised users, security, backups, changes and supplier assurance.

MAP EACH RELATIONSHIP

A council, prime contractor or landlord is not automatically NEWPOINT's processor or controller. Confirm the factual role for each data flow and record it in the contract or data-sharing arrangement.

3. Data protection principles

Principle	Operational question
Lawfulness, fairness and transparency	Can we explain the purpose, basis and effect honestly to the person?
Purpose limitation	Is this use compatible with the reason the information was collected?
Data minimisation	Do we need every field, attachment, photograph and note?
Accuracy	What source, verification, review or correction control is appropriate?
Storage limitation	What event or date ends the need to retain it?
Integrity and confidentiality	Who needs access and what security matches the risk?
Accountability	What evidence shows we considered and met these requirements?

Before collecting a new field

- Name the specific business or legal purpose and information owner.
- Identify the lawful basis and any additional condition for sensitive information.
- Set access, sharing and retention rules before the field goes live.
- Update the privacy notice and processing record where required.

JUST IN CASE IS NOT A PURPOSE

Do not collect information merely because it may be useful later. A defined and necessary use must exist now.

4. Information held and lawful basis

Typical information	Typical purpose / basis to confirm
Landlord identity, ownership, bank and agreement data	Property offer, due diligence, payment and contract administration.
Resident identity, contact, occupancy and service records	Housing/service delivery, agreement administration and legal obligations.
Repairs, inspections, photographs and access notes	Property safety, contract performance, legal duties and legitimate operational interests.
Council or partner referrals and updates	Contracted service, public-authority instructions or legitimate interests, depending on roles.
Staff and contractor records	Employment/engagement contract, legal obligations and management interests.
Complaints, incidents and legal files	Service resolution, legal obligations, legitimate interests and legal claims.

Lawful-basis control

The lawful basis is chosen for the purpose—not for convenience—and documented before processing. Where legitimate interests is used, NEWPOINT records necessity, the interest pursued and the balancing of individual rights. Consent is used only where it is genuinely optional, specific, informed and easy to withdraw.

DO NOT ASSUME CONTRACT

A contract basis covers processing necessary to perform or enter a contract with that person. It does not automatically cover every useful activity or data sharing connected with a property.

5. Special category and criminal-offence information

Health, disability, racial or ethnic origin, religious or philosophical beliefs, trade-union membership, genetics, biometrics used for identification, sex life and sexual orientation require enhanced protection. Criminal-offence information has separate restrictive rules.

Control	Minimum requirement
Purpose	Clear, specific and necessary use—not a general vulnerability label.
Legal condition	Article 6 basis plus an Article 9 condition; or the applicable criminal-data authority and safeguards.
Policy document	Maintain an appropriate policy document where the selected statutory condition requires one.
Minimisation	Record the practical service need rather than unnecessary diagnosis or history.
Access	Need-to-know roles, restricted fields and no uncontrolled exports.
Sharing	Minimum information, lawful authority, safe channel and recorded recipient.
Review	Remove or update sensitive detail when the need changes.

Housing example

Where a resident needs an access or communication adjustment, the operational record should normally state the adjustment and safe contact method. Detailed medical evidence should be held separately and only where necessary.

HIGHER RISK, HIGHER CONTROL

Large-scale sensitive processing, profiling or use that determines access to a service may require a data protection impact assessment before launch.

6. Privacy information and collection

Collection point	Required action
Property enquiry / offer	Explain landlord and agent data use, verification, advisers, partners and retention.
Resident onboarding	Provide the relevant resident privacy information through an accessible channel.
Council / partner referral	Check what the person was told and give NEWPOINT information where required.
Employee / contractor start	Issue workforce or supplier privacy information before routine processing.
Website / CRM form	Use a short collection message linked to the full notice; avoid pre-ticked marketing choices.
CCTV or monitoring	Use prominent notice and complete necessity, proportionality and retention checks.

Privacy notice content

- Controller identity and contact route; purposes; lawful bases; and legitimate interests where relevant.
- Categories and sources where information was not obtained directly; recipients; transfers; retention approach and rights.
- Whether information is required and the consequences of not providing it; automated decision information where applicable.

PLAIN AND TIMELY

Privacy information must be concise, understandable and available when information is collected—or within the applicable timeframe when received from another source.

7. CRM, email, devices and record quality

Control	NEWPOINT practice
CRM access	Named accounts, role-based permissions, multi-factor authentication where available and prompt leaver removal.
Case notes	Factual, relevant, dated and respectful; distinguish observation, report and decision.
Attachments	Use approved folders/records, consistent names and no unnecessary duplicate copies.
Email	Check recipients and attachments; use links or approved secure transfer for sensitive material.
Mobile use	Screen lock, supported software, no shared logins and prompt reporting of loss or compromise.
Exports	Business need, authorised recipient, secure location and deletion after the task.
Accuracy	Record source, correction, disputed information and material decision history.

Recording standard

- Write as if the person may read the record later.
- Do not use speculation, humour, discriminatory labels or unnecessary personal detail.
- Do not put passwords, identity-document numbers or sensitive histories into free-text notes unless specifically designed and necessary.

CRM IS THE CONTROLLED RECORD

Avoid shadow spreadsheets, personal notebooks and messaging threads becoming the only evidence of a property or resident decision.

8. Sharing with councils, partners and suppliers

Five checks before sharing

Check	Question
Purpose	Why is the disclosure necessary and compatible with the original purpose?
Authority	What lawful basis, legal power, duty, contract or consent supports it?
Minimum	Which exact fields or documents does the recipient need?
Recipient and channel	Have identity, address, access and transmission security been verified?
Record	Can we show what was shared, with whom, when and why?

Agreements and processors

Routine or high-risk sharing should be covered by a proportionate data-sharing arrangement describing roles, purposes, datasets, lawful bases, security, rights, incidents, retention and review. Processors must have a compliant written contract, suitable safeguards and approval controls for subprocessors.

Safeguarding and emergencies

Data protection law does not prevent necessary and proportionate information sharing to protect a person. Staff should record the risk, authority, information shared and reasoning, and seek advice when time allows.

NO WHOLE-FILE DEFAULT

A request from a council, landlord or partner does not automatically justify sending the complete case file.

9. Individual rights and requests

Right / request	Response control
Be informed	Provide clear privacy information and explain significant changes.
Access	Recognise verbal or written subject access requests; verify proportionately; search relevant systems and protect others' information.
Rectification	Correct inaccurate data and complete incomplete material information.
Erasure / restriction	Assess the right, legal exceptions, retention duties and downstream recipients.
Object	Review direct marketing immediately and assess other objections against the applicable basis.
Portability	Provide eligible information in a structured, commonly used, machine-readable format.
Automated decisions	Provide required safeguards and meaningful human review where the rules apply.

Simple handling route

- Log immediately and send to the information lead; do not require a special form.
- Clarify scope and identity only where necessary; calculate the statutory deadline and preserve relevant data.
- Record searches, redactions, exemptions, decisions and delivery.

ONE CALENDAR MONTH

Most rights requests must be answered without undue delay and normally within one calendar month. Any extension or refusal requires a lawful reason and timely explanation.

10. Security and personal data breaches

Security baseline

- Least-privilege access; unique credentials; multi-factor authentication; prompt access review and removal.
- Supported and updated devices, secure configuration, encryption and tested backup/recovery arrangements.
- Verified recipients, secure disposal, clear-desk controls and confidential conversations.
- Supplier due diligence, contractual security requirements and incident cooperation.

If information is lost, sent incorrectly or accessed without authority

Step	Action
1. Contain	Recall, revoke links, isolate devices/accounts and ask unintended recipients to secure or delete.
2. Report	Tell the information lead immediately—do not investigate alone or hide an error.
3. Preserve	Keep messages, logs, affected records and a timeline.
4. Assess	Identify people, data, cause, likely harm, scale and containment.
5. Notify	Decide promptly whether ICO and affected-person notification is legally required.
6. Improve	Record the decision, corrective action, owner and completion evidence.

72-HOUR CLOCK

Where an ICO report is required, it must be made without undue delay and, where feasible, within 72 hours of awareness. Internal reporting must therefore be immediate.

11. Retention, disposal and business continuity

NEWPOINT will maintain an approved retention schedule by record category and business event. Retention periods reflect purpose, law, contract, limitation, safeguarding, insurance and partner requirements—not unlimited storage.

Record lifecycle	Control
Create	Assign record category, owner and secure location.
Active	Keep complete, accurate, accessible to authorised users and protected from alteration.
Review trigger	Use end of agreement, case closure, employment end, complaint resolution or another defined event.
Legal hold	Suspend normal deletion where litigation, investigation, complaint, audit or safeguarding requires preservation.
Dispose	Securely delete digital copies and destroy paper; include exports and working copies.
Evidence	Maintain deletion or disposal evidence proportionate to risk.

Continuity

- Back up critical controlled records and periodically test restoration.
- Document how essential property, safety and resident information remains available during an outage.
- Do not use uncontrolled personal accounts as an emergency archive.

RETENTION SCHEDULE REQUIRED

Before adoption, NEWPOINT must approve its record categories and actual periods. This policy deliberately does not invent universal periods that may conflict with contracts or legal advice.

12. Privacy by design, suppliers and change

Change trigger	Required review
New CRM module or field	Purpose, basis, notice, access, retention, export and deletion controls.
New council / prime contract	Controller roles, instructions, sharing schedule, rights, incidents and end-of-contract return/deletion.
Monitoring, scoring or automation	Necessity, fairness, explainability, human review and DPIA screening.
New supplier / cloud service	Security, location/transfers, subprocessors, contract, exit and assurance.
Large data import or migration	Accuracy, minimisation, mapping, test data, rollback and deletion of temporary copies.
New sensitive-data use	Article 9/10 conditions, appropriate policy document and DPIA screening.

DPIA route

- Describe the proposed processing, purposes, parties, technologies and data flows.
- Assess necessity, proportionality and risks to people—not only risk to NEWPOINT.
- Identify safeguards, residual risk, owners and approval before processing begins.
- Consult the ICO where legally required high residual risk cannot be reduced.

DESIGN BEFORE DEPLOYMENT

Privacy controls must be included while a system, contract or process can still be changed—not added after live data is collected.

13. Accountability, training and quick-reference card

Owner	Key responsibility
Directors	Approve risk appetite, resources, policy and high-risk residual decisions.
Information lead	Maintain governance records; coordinate rights, incidents, DPIAs and advice.
Managers	Control access, record quality, sharing and staff compliance.
All workers	Use approved systems, minimise data and report requests or incidents immediately.
System owners	Security, users, backups, changes, suppliers and assurance evidence.
Contractors / processors	Follow documented requirements and notify incidents without delay.

Quick-reference: stop and check

Situation	Action now
Email sent to the wrong person	Contain if possible and report immediately.
Someone asks for their records	Log as a possible rights request; do not insist on special wording.
Partner asks for a full file	Clarify purpose and share only what is necessary and authorised.
Sensitive detail appears in a note	Restrict access; assess necessity; correct or remove appropriately.
New CRM field is proposed	Complete purpose, lawful-basis, notice, access and retention review first.
Device or account may be compromised	Disconnect/secure where safe and report immediately.
Unsure whether sharing is permitted	Pause unless urgent safety requires proportionate action; seek advice.

NEVER DELAY INCIDENT REPORTING

Fast reporting protects people, preserves evidence and gives NEWPOINT the best chance to meet legal deadlines.

14. Assurance, document control and sources

Minimum assurance

- Annual processing-record, privacy-notice, retention and access-permission review.
- Quarterly incident, rights-request, overdue action and high-risk supplier review during scale-up.
- Training at induction and refresher training proportionate to role and risk.
- Periodic CRM case-note, export, sharing and leaver-access sampling.

Version	Date	Owner	Review
1.0	August 2026	NEWPOINT Housing Group	August 2027 or earlier trigger

Authoritative framework

- **GOV.UK — The UK's data protection legislation**

<https://www.gov.uk/data-protection/the-data-protection-act>

- **ICO — Guide to lawful basis**

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>

- **ICO — Data protection principles**

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/>

- **ICO — Special category data**

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/>

- **ICO — Individual rights**

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/>

- **ICO — Personal data breaches**

<https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>

CONTROL NOTE

Before formal adoption, confirm NEWPOINT's controller/processor map, privacy notices, lawful-basis record, named information lead, ICO registration/fee position, retention schedule, processor contracts, international transfers, incident contacts and appropriate policy document requirements.