Bromford.

Data Protection Policy

Be.Secure

Policy Statement & Purpose

This policy, which is part of our overall framework for data protection and information security, explains the Bromford Housing Group's commitment to a "Privacy by Design" approach to personal data. This means that Bromford protects personal data relating to our customers, colleagues and everyone we work with by following good data protection practices and principles.

Our "Privacy by Design" principles are:

- we believe in privacy by default
- we embed privacy into design;
- we believe in visibility and transparency;
- we are committed to end-to-end security;
- we are proactive not reactive, preventative not remedial;
- we won't trade privacy off against other objectives;
- we respect user privacy

These principles help ensure that all personal data is collected, stored, used, shared and disposed of safely and securely, in line with legal requirements and best practice.

This policy; and these principles, help Bromford ensure that personal data relating to our customers, colleagues and other data subjects is:-

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The above sets out Bromford's main responsibilities under data protection law including the UK's General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018 (DPA 2018). Bromford is responsible for, and must be able to demonstrate compliance with the principles relating to the processing of personal data.

Scope

The principles and terms within this policy apply to all personal data processed by Bromford which relates to customers, colleagues and others.

Personal data is defined as any information related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

The UKGDPR's definition of personal data makes it clear that information such as an online identifier – e.g. an IP address – or location data can be personal data. The more expansive definition provides for a wide range of

personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

This Policy covers Bromford Housing Group and its subsidiaries.

Our Privacy by Design Principles

Great data protection practice is about making sure that all the personal data Bromford colleagues come into contact with, through any channels is handled properly throughout its "personal data journey". This means that all information must be collected, stored, used, shared and disposed of appropriately and securely, by following our Privacy by Design Principles:-

Our privacy by design principles	**How do we achieve this?**
We believe in privacy by default Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.	This policy outlines our commitment to Privacy by Design. Our **Information Security Policy,** our **Data Classification Policy** and **information about Data Protection on the Hub** explain how we embed the all the privacy by design principles, including privacy by default.
We embed privacy into design Privacy by Design is embedded into the design and architecture of our IT systems and business practices. It is not bolted on as an add-on, after the fact. As a result privacy is an essential component of the core functionality being delivered. Privacy is integral to our systems processes and practices, without diminishing functionality. Leaders and colleagues must consult the Data Protection Officer when a change to the way we use personal data could introduce new privacy risks in data processing activities. This is possible when new data processing processes, systems or technologies are introduced or when data is bought from third parties.	We carry out a **Data Protection Impact Assessment** (DPIA) before we embark on a new project or introduce a new process. The need to consider if a DPIA is needed is embedded in our procurement processes. This enables us to identify and manage privacy risks inherent in the processing of personal data. They help us avoid the need for costly alterations that otherwise might only be discovered part way through a project and help avoid possible loss of trust and reputational damage. In summary, a DPIA helps minimise privacy risk.
We believe in visibility and transparency Visibility and transparency are essential to establishing accountability and trust. Privacy by Design seeks to assure all stakeholders that whatever the IT system or business process involved, it is in fact, operating according to stated promises and objectives, subject to independent verification by the Data Protection Officer and our auditors.	Our **Privacy Notices** provide visibility and transparency about the data we collect and process. It also explains what we will, and won't, do with personal data. Our **Policy for Processing Special Category & Criminal Offence Data** provides additional transparency around processing of this data.
We're committed to end-to-end security Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire data lifecycle. Strong security measures are essential to privacy, from start to finish. They ensure that data is securely retained, and securely destroyed when no longer required in a timely way. Privacy by Design ensures secure lifecycle management of information, end-to-end.	Our Information Security Policy and Acceptable Use Policy reinforce our commitment to end-to-end security. Our Data & Document Retention Policy and **Data & Document Retention Table** set out clear expectations for data retention.

We are proactive not reactive; preventative not remedial Our Privacy by Design approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Our Privacy by Design approach does not wait for privacy risks to materialise, and it aims to prevent data protection incidents from occurring. In short, Privacy by Design comes before-the-fact, not after.	We have a **Data Protection Compliance Checking Programme** which provides assurance that we are following our policies and procedures. Data protection breaches can and do happen but when they do, we follow our Data Protection Breach Reporting guidance. We will always find out what went wrong and ensure that lessons are learnt.
We won't trade off privacy against other objectives Privacy by Design seeks to accommodate all legitimate interests and objectives in a win-win manner. Privacy by Design avoids unnecessary trade-offs, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.	Our Privacy Notices provide transparency on the legal basis for processing personal data. We avoid relying on consent because of the imbalance of power between Bromford and our customers and colleagues. If we rely on legitimate interest as the legal basis for processing we will ensure that our interests are balanced with those of the data subject. We will do this by carrying out a Legitimate Interests Assessment if necessary.
We respect user privacy Above all, Privacy by Design requires us to keep the interests of the individual uppermost by offering measures such as strong privacy defaults and respect for data subject's rights.	We publish Your data, Your Rights on our website to highlight data subjects' rights to customers, colleagues and others.

Responsibilities

What?

The use of information about people, often described as personal data or personal information, is specifically covered by the Data Protection Act 2018 and the UK General Data Protection Regulations (UKGDPR). It can be information about customers, colleagues, or any other people Bromford has contact with.

Bromford has nominated a Data Protection Officer as described by UKGDPR. The appointment of a Data Protection Officer is not mandatory for the Housing Sector but Bromford sees the role of the Data Protection Officer as important in delivering our Privacy by Design approach and ensuring compliance with data protection law.

Additionally, we process special category and criminal offence data as part of our core business. Our approach to processing this data is set out in our Policy for Processing Special Category & Criminal Offence Data.

Our Privacy Notices and the Lawful Bases for Processing Personal Data

Our privacy notices set out: -

- Contact details for Bromford and our data protection officer;
- The purposes of and lawful basis for our personal data processing;
- The legitimate interests for our personal data processing;
- The recipients, or categories of recipients of the personal data we process;
- Information on transfers of personal data to any third countries;
- Retention periods for personal data;
- Rights available to individuals in respect of our personal data processing including the right to withdraw consent and the right to lodge a complaint with a supervisory authority;
- Details of where individuals are under a contractual obligation to provide personal data;
- Confirmation that Bromford does not use automated decision-making.

Most commonly the lawful basis for our personal data processing is either legitimate interest or performance of a contract (such as a tenancy agreement, lease agreement, contract of employment etc).

Bromford recognises that there can be an imbalance of power between ourselves and our customers and colleagues when we process their personal data. We therefore avoid relying on consent when processing personal where there is a clear imbalance of power which would invalidate consent. A potential customer applying for a home may be in a vulnerable position and may not have many other housing options. This means they may have no real choice but to sign up to our terms.

In these cases, we rely on legitimate interests as the lawful basis for our processing and allow customers, colleagues and others to object to our processing on grounds relating to their particular situation.

Why?

The personal data that our customers and colleagues entrust Bromford with is a valuable asset and we must handle it with respect and keep it secure. The consequences of an incident that results in personal data falling into the wrong hands can include serious harm and distress to individuals whose data is breached and harm to Bromford. Under Data Protection laws the business could be prosecuted and have large fines imposed, as well as suffer reputational damage.

Good data protection practice is an integral part of good customer service.

When?

The policy must be followed in all situations, including whether colleagues are working in the office, at home, in our customer's homes or at any other private or public location.

Who?

Bromford is accountable for; and must be able to demonstrate compliance with responsibilities under UK data protection law.

The Board has overall responsibility for this policy and is committed to Privacy by Design.

The annual declaration signed by members of Bromford's Board includes an acknowledgement of an absolute duty of confidentiality to Bromford. This states that Board members must not disclose to any third party any confidential information which they have obtained because of their position on the board

The Audit & Risk Committee (ARC) will obtain assurances relating to the adequacy and effectiveness of risk, control and governance processes relating to data protection and privacy in Bromford.

The committee will receive reports on Bromford's compliance with the principles of this policy and data protection law.

The Risk & Compliance Forum (RCF) will maintain and monitor proper arrangements for data risk management, ensuring these are effectively developed, implemented, managed, monitored and embedded across Bromford. The Risk & Compliance Forum will ensure that proper arrangements for risk management and internal control are maintained and monitored in Bromford's approach to data protection and privacy. Ensuring these are effectively developed, implemented, managed, monitored and embedded across Bromford.

The Data Governance Group (DGG) will provide oversight to the Executive Board and the Risk and Compliance Forum with regards to Bromford's data estate. The group provides a mechanism to monitor the effectiveness of individual Data Assurance Groups. The group will actively monitor and review all aspects of data, whilst ensuring the alignment of data governance within the context of the strategic direction of the organisation. The group will ensure that data risk management and data protection obligations are championed throughout all aspects of data ownership and management. The group will report monthly on personal data breaches, security incidents, data governance / quality incidents and transformation design requests.

The Information Security & Resilience Team are key stakeholders in Bromford's overall approach to ensuring that data subjects rights are respected. In particular, the Information & Data Management Service will be responsible for ensuring that appropriate technical measures are in place to facilitate compliance with data protection law and the principles in this policy. The team are also responsible for maintaining data quality dashboards and ensuring that data quality errors are rectified by data owners.

Data Owners & Data Stewards Data Owners are generally identified as a director level role that span a broad collection of service areas. They are responsible and accountable for a collection of data assets This extends to ensuring that our use of those data assets complies with data protection law. Data Owners may be supported by Data Stewards who will work with the Security & Resilience Team to help improve management of data quality and drive proactive identification and resolution of issues.

Leaders are responsible for ensuring that all colleagues in their teams understand the Privacy by Design policy statement and principles and the underlying procedures and guidance. Leaders must also ensure their teams understand the need to report data protection incidents to the Data Protection Officer within 24 hours. as part of a commitment to continuously improving standards of data protection and privacy. Leaders should:

- share this Policy and all policies and procedures linked to this Policy, as well as other communications about data protection matters, with their teams;
- make sure their teams complete their training;
- support their teams in reporting possible breaches;
- ensure that Data Protection Impact Assessments (DPIA's) are carried out when changes in the way we operate mean significant changes to the way in which personal data is collected or used or significant impacts on privacy are likely;
- ensure that a Data Processors Agreement (DPA) or Standard Contractual Clauses are in place where we appoint a contractor who will have access to personal data relating to Bromford customers, colleagues or other data subjects;
- design their policies and processes with good data protection principles in mind.

All colleagues are required, via their contract of employment, to abide by procedures designed to protect the confidentiality of information held about customers, other colleagues or others.

The Data Protection Officer is responsible for the following tasks:

- To inform and advise Bromford and colleagues about their obligations to comply with the UKGDPR and other data protection laws;
- To monitor compliance with the UKGDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; training colleagues and conducting compliance audits; and
- To be the first point of contact for supervisory authorities (the Information Commissioner's Office) and for individuals whose data is processed (colleagues, customers etc.).

In particular the Data Protection Officer is responsible for ensuring that appropriate procedures and guidance on our approach to data protection and privacy are available to Board members, leaders and colleagues.

Guidance available on the Hub set out specific guidance including procedures for carrying out DPIA's and procedures for complying with data subject's rights under the UKGDPR.

How?

Colleagues can promote good data protection practice by:

- following this Policy, and linked policies and procedures;
- completing their Data Protection training;
- reporting suspected breaches to the Data Protection Officer; and
- querying anything that looks like poor data protection practice or that they are unsure of.

The Data Protection Officer can provide extra help and advice. The Information Security & Resilience Team can also provide help and advice on technical measures to comply with our data protection principles.

Reference Documents

Additional guidance, related policies and procedures can be found in:

The Bromford Housing Group Privacy Notices Our Data & Document Retention Policy and Retention Table Policy for Processing Special Category & Criminal Offence Data Information Security Policy	Acceptable Use Policy Access Control Policy Third Party Governance Policy Data Classification Policy

And the following articles on the Hub

- Report a Data Protection Breach;
- Subject access requests and other data subject's rights;
- Managing and processing data, and
- Our data protection toolkit

The articles on the Hub includes guidance on DPIA's; DPA's; CCTV; photography & film and sending and sharing information securely.

Legislative Requirements

Bromford's policy is to comply with:

• Data Protection Act 2018; • General Data Protection Regulation 2016	• Privacy & Electronic Communications Regulations 2003 • Human Rights Act 1998

Please note that whilst Bromford is not currently subject to the Freedom of Information Act 2000, new proposals were put forward in the Social Housing White Paper in the Autumn of 2020 that will make it easier for customers to access information regarding their housing associations, which are similar to the requirements under the Freedom of Information Act. For advice please contact the Governance, Risk & Assurance Team.

Assurance Framework

Directors will be asked to provide assurance that key data protection requirements are understood and complied with via the twice-yearly Directors Assurance Statement.

Leaders will be asked to ensure that this policy is communicated to all colleagues in their teams and a copy of the policy will be made available via the Hub. Awareness of our Data Protection & Privacy Policy will be reinforced on a periodic basis via news items, e-learning and other training and team talks.

The Data Protection Officer will provide management and performance information relating to data protection breaches; data subjects' rights; numbers of colleagues who have completed the e-learning module and other measures.

The Data Protection Team's data protection compliance checking programme provides assurance that we meet the principles of UKGDPR by following our policies and procedures.

The Information & Data Security Team maintain Data Quality Dashboards that keep a record of data quality issues and the actions we take to correct these.

The Risk & Compliance Forum provide assurance to the Board and Audit & Risk Committee (ARC) in discharging their responsibilities for ensuring the adequacy and effectiveness of data risk management across Bromford. The group will escalate matters, provide recommendations and regularly report to A&R and/or Board.

ARC is responsible for obtaining assurances relating to the adequacy and effectiveness of risk, control and governance processes relating to data protection. The committee will also review material data protection incidents, risk exposures or control failings.

Our approach to ensuring we comply with data protection law and our data protection principles will be subject to external review on a regular ongoing basis.

Document Details

Owner:	Chris Down – Data Protection Officer
Approved By:	Audit & Risk Committee
Date of Approval:	08/07/2021
Next Review Due:	July 2024
Policy Version:	1.2