Bromford.

Data Protection Policy

Be.Secure

Policy Statement & Purpose

This policy, which is part of our overall framework for 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 and
- 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 UK data protection law which is derived from the EU's General Data Protection Regulation (GDPR). Additionally, 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 GDPR'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 our **Data Protection Toolkit** 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 **Data Protection Impact Assessments** before we embark on a new project or introduce a new process. 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, the Data Protection Impact Assessment 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.
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. This ensures that all data is securely retained, and then securely destroyed when no longer required in a timely fashion. Privacy by Design ensures secure lifecycle management of information, end-to-end.	Our **Information Security Policy,** our **Acceptable Use Policy** and guidance on the **Personal Data Lifecycle** reinforce our commitment to end-to-end security. Our **Data & Document Retention Policy** sets clear timescales 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** 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 General Data Protection Regulations. 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 the GDPR. 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 recognise that we process a significant volume of sensitive data, for example related to our customer's health, as part of our core business.

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 or at any other private or public location.

Who?

Bromford is responsible 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 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 compliance with the principles of this policy data protection law.

The Risk & Compliance Forum 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 Information & Data Management Service 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.

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 encourage the reporting of data protection incidents as part of a commitment to continuously improving standards of data protection and privacy. Leaders should:

- share this Policy and all policies and How To guides linked to this Policy, as well as other communications about Information Governance (IG) matters, with their teams;
- make sure their teams complete their training;
- support their teams in reporting possible breaches;
- and design their policies and processes with good data protection principles in mind.

All colleagues are required, by the Colleague Handbook and / or Code of Conduct 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 GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; train colleagues and conduct 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.

Our data protection toolkit will set out a specific way to carry out a specific duty or activity. These will include a clear desk procedure; procedures for carrying out data protection / privacy impact assessments and procedures for complying with data subject's rights under the GDPR.

How?

Colleagues can promote good data protection practice by:

- following this Policy, and other policies and How To guides linked to this this Policy and other information governance communications;
- 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, part of the Governance, Risk & Assurance Team can provide extra help and advice. The Information & Data Management Service can also provide help and advice on technical measures to comply with our data protection principles.

Reference Documents

Please note: this policy replaces Bromford's Information Governance policy and Bromford's Data Protection Policy. This document is published on our group intranet.

Additional guidance, related policies and procedures:

Bromford Housing Group Privacy Notice
Data & Document Retention Policy
Data Protection Toolkit

The data protection toolkit includes how to guides on the Personal Data Lifestyle; Data Protection Impact Assessments; CCTV; Data Subjects Rights; Sharing Personal Data; Reporting Data Protection Breaches and other topics related to data protection.

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

Please note Bromford is not currently subject to the Freedom of Information Act 2000. For advice please contact the Governance, Risk & Assurance Team.

Assurance Framework

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 Bromford's intraNet sites (OurSpace, Mint and Stick). Awareness of our Data Protection & Privacy Policy will be reinforced on a periodic basis via news items on OurSpace, 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 Corporate & Risk Forum provide assurance to the Board and Audit & Risk Committee (A&R) 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.

A&R 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:	Risk & Compliance Forum
Date of Approval:	12/11/2018
Next Review Due:	May 2020
Policy Version:	1.1