Data Management Framework

White Paper 1.0

Contributors: Bolton at Home, ForHousing, Great Places, Johnnie Johnson Housing, One Manchester, Peaks & Plains Housing Trust, Rochdale Boroughwide Housing, Stockport Homes Group, and Wythenshawe Community Housing Group.

Greater Manchester Housing Providers

gmhp

CONTENTS

1.0 Introduction

Greater Manchester Housing Providers (GMHP) are using their combined strength to ensure that everyone in the City Region can live in a quality home that they can afford.

The Data and Information Governance (IG) Working Group has identified a need to create a standard set of principles relating to effective data management, in order to achieve the GMHP objectives.

Through our working group, we have co-designed and authored this White Paper, so that Registered Providers (RP's) within Social Housing can adopt a standard Data Management Framework (DMF). The intention is for RP's to utilise the DMF, to tailor it to the RP's native language and to sell it to their respective organisations as a way to transform the way they manage data.

1.1 Our purpose

The collective aim across the Housing Sector is to provide outstanding homes, services and value for residents. We can only achieve this if we know our customers, understand our stock conditions and have a solid understanding of what works and doesn't work when things go wrong.

In order to achieve this collective vision and maintain the GMHP principles, we need robust data to help us make the right decisions, which allow us to realise our ambitions. The purpose of this White Paper is to embed data at the heart of our organisations and in every decision we make.

1.2 How data supports our purpose

Everything we do must start and end with the customer in mind. We exist for them. To allow us to deliver all of our goals and aspirations, we need to invest in our data and realise that it is our most valuable material asset.

Our knowledge and experience of our customers enables us to make good solid decisions. If we can back this up with a strong evidence base, we stand a stronger chance of delivering our GMHP vision quicker and more accurately. We generate understanding of our customers and a true insight into their needs by having a solid foundation of good quality data upon which to build our services.

1.3 Our challenge

We are data rich and insight poor.

Data is often seen as a by-product of our business processes and not enough effort is made to integrate and translate it. This causes data to be unstructured, unmanaged and poorly utilised. This is where we are as a sector, which is not unique to Housing.

This White Paper will outline how we manage our data moving forward, the organisational structure we need to adopt and the governance framework we need to succeed.

1.4 Outline of this White Paper

This White Paper provides the foundation for achieving our vision for data. It defines the relationships between data and how we operate as a business. It outlines the outcomes we aim to achieve from successful implementation of the DMF, and the capabilities and culture we need to develop to realise these outcomes.

This White Paper will outline:

- How we will identify our data needs
- The benefits our data assets bring
- The gaps in our existing data
- The way we cleanse data
- How we store our data
- Our data architecture
- The governance framework
- The organisational structure.

1.5 Embedding data in our business

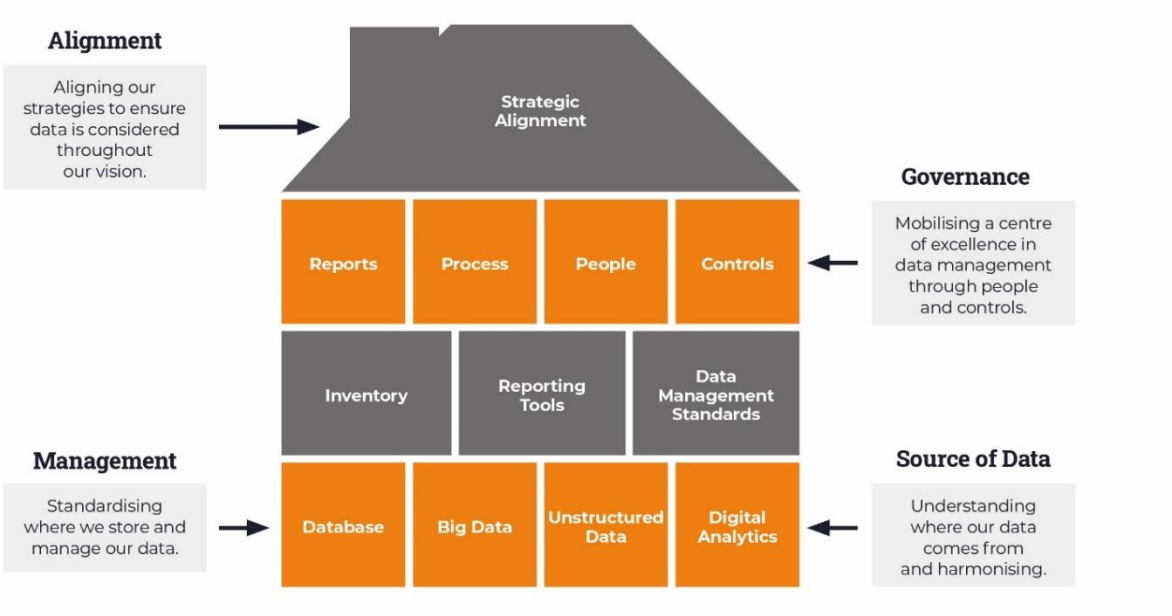
This White Paper will inform the development and implementation programme, projects and changes which will require investment and key decisions, including changes to our IT infrastructure.

Our data will inform the development of new products and services and operational planning, decision-making and general delivery across the business. More specifically, the DMF provides the foundation for the development and implementation of a range of underpinning data and information policies and procedures. It outlines how we should work and treat our data, with the aim to create a consistent sectoral approach to data management across the region.

In this endeavour we will be guided by, and inform, the development of the Greater Manchester (GM) Information Strategy (see section 2.1).

2.0 The Data Management Framework

The Data Management Framework



2.1 Strategic alignment

There are two main approaches to aligning data with existing strategies:

1. Creating a singular standalone strategy, which sits alongside existing strategies.
2. Creating a data consideration component to merge and embed in existing strategies.

The benefit of having a standalone strategy is that organisations are then encouraged to take the subject matter more seriously. It acknowledges that our data management sits alongside our other strategic ambitions, in order to enable and maintain those aspirations.

Depending on the size and scale of our strategies, organisations may wish to embed a component within them to acknowledge that data has a role to play – essentially creating a golden thread throughout the organisation, with data a key component of our strategies.

As we have set out above, our work to create a DMF for Greater Manchester is aligned with the vision set out in the GM Information Strategy:

> We will create a better information ecosystem that realises the full potential of information; manages, shares, and uses information responsibly; helps to tackle our most serious challenges; and supports Greater Manchester's wider ambitions.
>
> *Information Strategy Delivery Plan: consultation on delivery plan priorities, p. 2*

This White Paper has been structured to enable GM Housing Providers to meet these strategic aims and outcomes, employing a continuous improvement process to review, develop and improve the DMF over time. We have set out the benefits of this approach in section 3 below.

2.2 Links to Business Insight Strategies

The DMF should be the foundation of any business insight strategy for the city region. In order to produce insight and predictive analytics we must have good quality, available, up to date and accessible data. Common examples include: corporate development of Key Performance Indicators (KPI's) and related metrics, service standards, 360 degree view of customer and property to support the development of a trusted record of business decisions. This supports the vision we are striving to deliver for our customers and will be based on accurate, data driven information.

The desire to move away from making reactive decisions to predictive decision making requires a significant cultural shift and a willingness to rethink the ways things have always been done. Identifying the particular barriers we face and planning how to overcome these barriers is key to the delivery of insight, as the case study below illustrates.

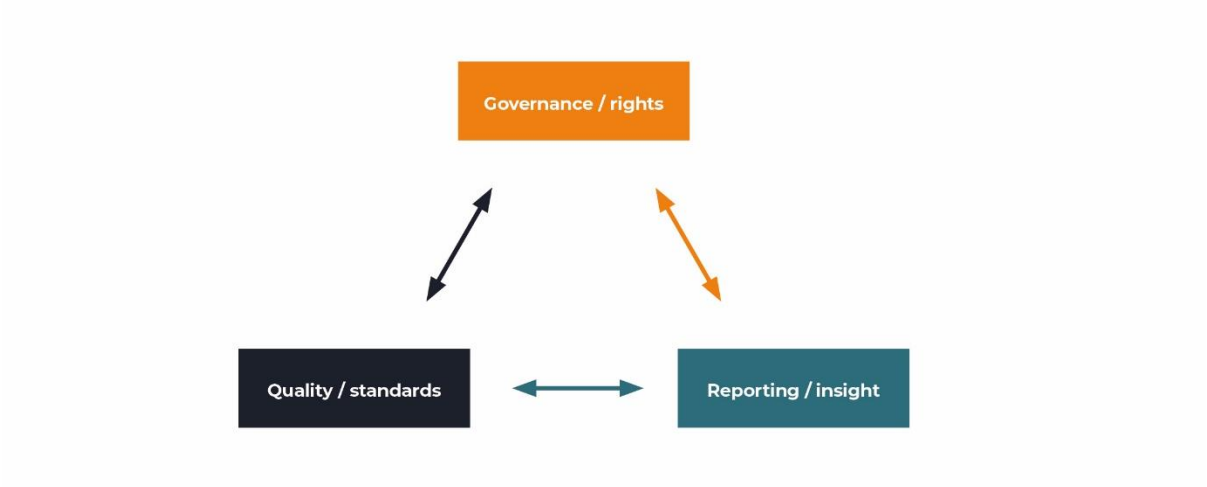
Case study – How ForHousing developed Tenant Lifecycle Management

ForHousing have recently introduced their Tenant 360 Power BI dashboard. The dashboard provides real time data into a tenant's journey, from the very start of their tenancy. This includes visibility of the issues tenants are dealing with so that front-line services can develop a more proactive approach to tenancy management. Through this approach ForHousing will achieve the following outcomes:

- real-time response to tenant needs
- improved data visibility, eliminating data silos
- better understanding of service demand
- a full picture of how users move through stages of their relationship with ForHousing.
- clarity on which channels and actions bring the most value to customers
- increased tenant satisfaction
- reduction in complaints.

3.0 How good data management benefits everyone

Data management comprises of three core capabilities, which we discuss in more detail later in this document:



By developing and implementing policies that support all three of these capabilities, Greater Manchester's social housing providers can ensure that they use and apply good quality data to inform their decision making. Good data management underpins business processes, automation and technology to ensure that data is stored, protected and can be exploited according to its value. Data quality factors include: accuracy, validity, reliability, timeliness, relevance and completeness. Housing providers should measure and report these factors to their data management and/or audit and risk committees to ensure that the data is fit for their primary and subsequent purposes.

3.1 Benefits for the organisation

RPs are uniquely placed as both community service providers and landlords to understand customers' needs better. By collecting, storing and using data in an accurate and timely manner, they can provide those services 'right first time'. This approach speeds up the time taken to respond to and resolve enquiries and requests, reduces demand failure and increases the organisation's ability to make Value for Money decisions. At the same time, good data management practices demonstrate accountability and increases trust in the organisation's capability to steward data responsibly, improving its reputation with customers, partners, regulators and the wider community.

3.2 Benefits for the customer

Customers can reap numerous benefits of good data management. The first of these is the tangible benefits associated with getting better services, such as repairs being completed correctly and on time. There are less tangible but still critical benefits to using data better to support tenants and leaseholders, such as maintaining accurate profiling data to tailor financial inclusion products for specific population segments.

An increased level of trust in their housing provider's data handling practices should in time lead to a reduction in service complaints or requests to check and rectify poorly collected data. Providers may want to regularly consult their customer committee and panels about how they should manage their information, for instance through a Data Protection Impact Assessment (DPIA) process. If tenants perceive that their landlord is handling their information correctly, they will potentially respond more positively to the Tenant Satisfaction Measures, relating to: listening to their views, keeping them informed about the things that matters to them, and treating them fairly (TP06 – TP08). RPs could also include questions about data management as an additional part of their Tenant Perception Surveys.

3.3 Benefits for the community

Finally, if RPs improve their data management and quality control processes, they can increase their understanding of, and support for, the communities they serve. The symbiotic relationship between coherent datasets and cohesive communities can be seen in providers' day-to-day operations, such as maintaining secure and lawful lists of involved residents for consultation and engagement activities. It can also be witnessed in the organisation's partnership role with other statutory and supporting agencies, through better information sharing to support vulnerable individuals and families. And it enables the provider to have a deeper awareness of the needs of its future customers and residents, increasing its ability to generate accurate demographic insights to inform its corporate planning.

4.0 Governance

Governance defines the management controls we will use to ensure that our organisations strive toward delivery of our data strategies. Data Governance is essential to support our organisations to achieve their vision and goals for data. Embedding good data governance will help our organisations to effectively manage, utilise, and safeguard data throughout its lifecycle from creation to deletion.

Data Governance is about ensuring that our policies and principles in relation to data are implemented and upheld, in order to proactively manage risk to individuals and the organisation.

Diagnostic tools such as low-cost data maturity assessments are also useful and can provide a useful starting point to assess key areas of focus. Socitm Advisory's ten-point maturity model looks at data management holistically and is often used as a starting point to craft a data strategy, to build organisational maturity and to identify key areas of focus to inform the roadmap for change.

4.1 Roles and Responsibilities

All data domains (e.g. Customer, Property, etc) will have defined ownership and accountability recorded in the Data Catalogue. These roles are ultimately responsible for the data we manage at each stage of the information lifecycle.

Role	Owner / Sponsor	Purpose
(Data) Controller	Housing Provider or Group of Providers	The RP as a whole is classed as the data controller. It may also operate as a joint controller of a shared set of data; for instance, with Greater Manchester Fire and Rescue Service (GMFRS), or as a Processor for another Controller; for example, where it provides a repairs service to a neighbouring provider.
Data Protection Officer	Head of Information Governance (or similar)	Aligning the data management framework to existing governance, policies and procedures.
Data Leader	Head of Data (or similar)	The Head of Service who oversees the day-to-day management of data, and ensures that the organisation can derive value from them. The role should also be able to implement an ethical approach to the way the organisation handles data.
Data Manager	Data & Insight Manager (or similar)	The person who manages the data insights / business intelligence function with the business.
Data Owners*	Assistant Director / Head of Service / Service Manager	The group of people who individually have responsibility for the various elements that make up the organisation's data catalogue
Data Users*	Team managers / leaders, colleagues (and potentially some involved residents)	The group of people who work within teams, projects and partnerships to collect, store, use and share the elements of the organisation's data catalogue.
Data Champion	Director of Technology / Resources (or similar)	Data Champions can be drawn from across the organisation and are often trained to help teams implement the data management framework, acting as first responders for data queries and issues. The Executive member (Director) is accountable for the implementation and adherence of the framework.

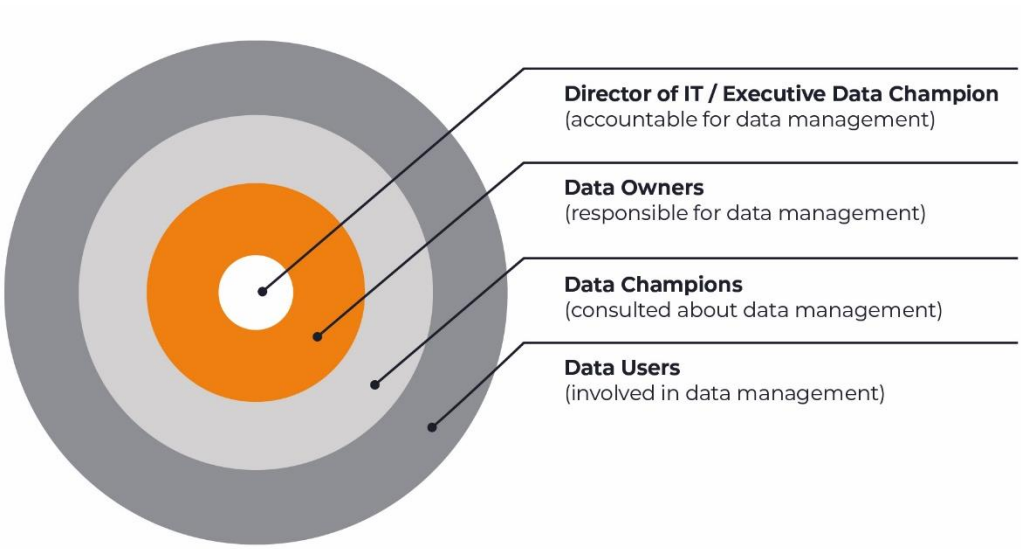
*See data management Responsible, accountable, consulted and informed (RACI) diagram below

Deriving value from data doesn't happen instantly. For it to work, you need complete buy-in at all levels of the business. This means everyone must reimagine how they collect, share, and use data.

It means that the group responsible for data governance, including those responsible for data security, privacy, and internal audit, must challenge the business to think critically about what it's trying to accomplish with its data.
The business must work together to:

1. Embrace new data architectures, processes, and ownership structures
2. Embed effective internal controls into organisational processes and technologies to better safeguard key data assets
3. Understand and, ultimately, operationalise the importance of data privacy and security
4. Learn to value transparency and ethics
5. Be attuned to both the risks and advantages of using emerging technologies like AI.

Data management RACI (Responsible, Accountable, Consulted, Informed/Involved) model



The RACI model above describes the relationship between different types of data roles within an organisation. To implement this model, GMHP will need to design and deliver a stakeholder engagement plan. They should consider how to identify and engage a wide range of internal and external customers in the strategy's development. Stakeholders should receive regular updates on implementation progress, as well as information on the agreed decision-making structures.

This collaborative approach delivers more than an opportunity for us to capitalise on data as an asset. It also ensures customers' interests are constantly protected and at the forefront of everything that we do.

4.2 Training and supporting our people

Our people are at the heart of the business. We aim to support our workforce to unlock the power of their data assets by engendering more understanding within the business about how data can be used to improve operational performance, evaluate options and make better sustainable decisions.

It is essential that everyone who works for the organisation understands their responsibilities for maintaining the integrity and quality of our data assets, complying with data legislation and regulations, and keeping the data assets safe and secure.

The principal roles to be assigned for each data domain held by the RP are:

- Data owner – make decisions about their data and are accountable for the quality of it.
- Data steward – nominated by the Data owner and provided with delegated authority for day-to-day operations.
- Data producers – create the data
- Data consumers – use the data. They need to have clear requirements for what the data needs to look like for them to be able to use it.

An information-skilled workforce is vital to our regional ambitions. Regular, relevant and up to date training is vital to develop our colleagues' confidence in using and applying data in their daily roles. At the same time, it embeds accountability by enabling policies and procedures to be understood and put into practice.

Colleagues and contractors should receive frequent information security awareness training as well as being subject to suitable confidentiality and security obligations in their contracts of employment.

4.3 Reports

RPs should aim to create a reporting suite or repository, along with a glossary outlining what the report is intended for and the associated controls and assurance for the report.

The repository should be split by department and team level to help outline the breadth and scope of reporting across the business.

The glossary should outline the following:

- The report title
- A description of the report
- When the report was created
- The author of the report
- The format the report is created in
- The source of the data being captured
- The level of sensitivity associated with the data contained – mapped against a risk or DPIA register
- The intended purpose of the report
- The audience the report is shared with
- Any associated dependencies attributed to the report and data contained.

5.0 Accountability and Risk Management

Accountability is one of the key principles enshrined in Article 5 (2) of the UK General Data Protection Act (UK GDPR). It is a vital pre-condition for customers' trust in their housing provider, because it requires controllers to demonstrate how they comply with the data protection framework and uphold information rights under the law.

As the Information Commissioner's Office (ICO) says, "Accountability is not about ticking boxes."

The ICO states that an ability to identify, assess and manage privacy risks is a crucial element of delivering a risk-based approach to accountability:

> "Understanding the risks of the way you use personal data specifically is central to creating an appropriate and proportionate privacy management framework." This means that as a complex organisation, you will need to take a risk-based approach to demonstrating compliance. Accountability enables you to implement "appropriate and effective policies, procedures and measures [which are] proportionate to the risks, which can vary depending on the amount of data being handled or transferred, its sensitivity and the technology you use."

Through enhanced scrutiny of our technology and processes, and better identification and management of risk, we can therefore provide accountability to our customers, board, partners and regulators.

The responsibility for managing risk should not lie solely with the Data Protection Officer (DPO) / Information Governance team. Good data governance starts with the belief that we are the custodians of our customers' personal information, and are all entrusted with stewarding it appropriately.

This belief drives fully accountable providers to transform the data culture of their organisation's so that ownership of data risk shifts to the senior managers and their teams are responsible for processing personal data in order to deliver better, more personalised services.

Before any new data-driven project is initiated, the risks to tenants, leaseholders, colleagues and the wider public should be identified and explored. By considering these risks early in the design stage, customers voices are heard and their expectations about how we will use their data will be met. As a result, they are able to exercise their rights over their information at each stage in the data journey.

To embed the risk-based approach successfully, senior leaders need to equip their workforce to develop a privacy management programme, and train staff to use the policies and products it covers successfully.
The ICO's Accountability Framework is useful for those responsible for putting appropriate technical and organisational measures required under Article 32 (often referred to as controls) in place to demonstrate GDPR compliance.

5.1 Organisational controls

Some of the key controls which should form the backbone of a responsible provider's privacy management programme are briefly described below:

Policies, procedures and training	The DMF should be developed in line with strategic business planning for data protection and information governance, which the highest level of management endorses. Operational procedures and guidance should be made available and accessible to operatives and front-line staff and they should understand how they should handle data in their role as a result.
Data minimisation and restriction	Article 5 (1) (c) of the UK GDPR states that all personal data that you hold should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual, which can support this principle.
Record of Processing and lawful bases	Creating a Record of Processing Activities (ROPA), as required by Article 30 of the UK GDPR, will help services to update and regularly review these data maps, ensuring that data is appropriately minimised (see above). Your ROPA should document the lawful basis you have selected for each record of processing, including how customer consents are managed, the conditions selected for processing any special category data (SCD) and the outcomes of legitimate impact assessments (LIAs) where you have chosen to rely on the organisation's legitimate interests to process the data.
Risk and Data Protection Impact Assessments (DPIAs)	A Data Protection Impact Assessment (DPIA) is a key risk management tool as it allows teams to identify, manage, consult on and reduce data risks in new or modified projects and services.

	Article 35 of the UK GDPR requires organisations to carry out a DPIA for high-risk processing activities, and under Article 36 they must report any high risks that cannot be managed to the ICO.
Contracts and Data sharing	Third party contractor relationships can often create weak links in an organisation's data management armour. Supply chain security can be improved through tools such as vendor onboarding questionnaires to provide due diligence on suppliers, and Data Processing Agreements (DPAs). Similarly, it is good practice to have written data sharing agreements when controllers share personal data, and document all sharing decisions, using a DPIA or other review process to assess the lawfulness, benefits and risks of the sharing activity.
Transparency and rights	Transparency promotes individual choice and control, enables better decision-making and improves trust in your organisation and its partners. To maintain transparency of your processing activities, Articles 13 and 14 of the UK GDPR require organisations to inform individuals through privacy notices and statements about their data rights and all staff are aware of how to identify and deal with both verbal and written requests.
Incident management and Breach monitoring	A personal data breach can have a range of adverse effects on individuals, as well as serious repercussions for organisations, their employees and customers, such as financial penalties, reputational damage, loss of business and disciplinary action. You should have procedures in place to make sure that you detect, investigate manage and appropriately record and communicate personal data incidents and breaches.

Case study – creating ownership and accountability for data at Peaks and Plains

Following an internal review Peaks and Plains Housing Trust (PPHT) undertook a comprehensive evaluation of all compliance activity under the heading of Foundations. Focussing on all areas of compliance, including the five "fatal risk areas", Foundations involved a root and branch evaluation of all aspects of the service provision instigating a series of projects across three phases named: Is it right?; Make it right!; and Keep it right!

Central to the programme, and especially the "Keep it right!" phase, was the need for effective Data Governance and Data Management and at the core of this was the concept of CRUD. CRUD is a simple model of data across its life cycle (based on the acronym: Create, Retrieve, Update, Delete) which proved invaluable for:

- Identifying the key activities taken to deliver a service (e.g. the steps needed in the servicing of gas components)
- Establishing the life cycle of the data required (e.g. from installation to disposal)
- Assigning who was responsible for doing what at each step of the process
- Establishing what essential data was required by the users of that information
- Identifying the gaps in knowledge and holes in the process (e.g. poor documentation)
- Identifying where data quality reporting was required.

The CRUD model was an easy to grasp concept that proved powerful in exposing flaws in data dependent processes. CRUD has subsequently begun to be used across all processes that involve data (i.e. all processes) as the principles apply generically.

5.2 Information and Cyber Security

To ensure that the information they process is securely held and appropriately shared, providers should develop a rolling programme of internal information audits of the compliance of its *people, processes and technology*. These should be informed by the standards set out in the organisation's information security management framework.

The UK's National Cyber Strategy (2022) describes a world ever more connected than before. Cyber, or online, technology offers huge opportunities to transform the way we work, communicate and engage with people. However, it notes that organisations need to build cyber security resilience into operations due to the "unprecedented complexity, instability and risk" these technologies bring.

While organisations should create an information security framework which is suitable for their own business, they can also adopt internationally recognised standards, including

- ISO 27001 (and ISO 27701 for international privacy management standards),
- the Cyber Essentials and Cyber Essentials Plus standard which is backed by the UK Government,
- and the NIST framework which originated in the United States.

RPs can sign up to HACT's Housing Data Standards to create a *golden thread* of property information to ensure data consistency across their estate. If providers share information with health and care partners, they could also choose to sign-up to the NHS Data Security and Protection Toolkit, an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's ten data security standards. The National Cyber Security Centre (NCSC) provides useful advice and guidance on implementing and promoting cyber security measures.

Performing risk assessments is also at the heart of an organisation's information security management framework. A common approach to performing a risk assessment may include identifying the scope of protection, identifying the assets and how they are used by the organisation, identifying potential threats and vulnerabilities, measuring the risk of each of these threats and identifying and implementing suitable controls for each risk.

Pseudonymisation and encryption are specified in Article 32 as two examples of measures that may be appropriate for you to implement to minimise or restrict processing to reduce the risks posed to individual. However, these controls should be appropriately managed, as incorrect selection of cryptographic technologies or the poor management of keys can create their own vulnerabilities.

6.0 Records management

Information security supports good data governance, and is itself a legal requirement under Article 32 of the UK GDPR. It is vital for an organisation to have a robust information security framework in place in order to protect the confidentiality, integrity and availability of its systems and data from both internal and external threats and vulnerabilities. Good record management supports good governance, as well as improving the accessibility of information and the effective deployment of an organisation's resources. Whilst there is already extensive guidance on accountability measures that support good record management, specific tasks the organisation should consider include:

- setting up an information asset register (IAR) that records assets, systems and applications used for processing or storing personal data across the organisation;
- creating an appropriate retention schedule outlining storage periods for all personal data, which you review regularly;
- limiting access to personal data to authorised staff only and regularly review users' access rights; and
- classifying types of data depending on their sensitivity, including who has access to that data and how long the data needs to be retained.

6.1 Data Management Standards

Data quality issues will be resolved as close to the point of production or source of the issue as possible rather than at consumption. Producing robust data is an integral part of our operational, performance management, and governance arrangements. The business recognises that there are several key characteristics of good quality data, and we will seek to ensure that our data meets these criteria.

- **Accurate**: Data should be sufficiently accurate for its intended purposes. Accuracy is most likely to be secured if data is captured as close to the point of activity as possible. Data should be captured once only, although it may have multiple uses. The importance of the uses for the data must be balanced with the costs and effort of collection.
- **Valid**: Data should be recorded in an agreed format and, where possible, comply with recognised national and sector standards (e.g. HACT)
- **Reliable**: Data should reflect stable and consistent data collection processes across the business
- **Timely**: Data should be available within a reasonable time period and frequently enough to support information needs
- **Relevant**: Data captured should be relevant to the purposes for which it is used. The Information Asset Register will ensure that Data Privacy concerns are regularly reviewed

- **Complete**: All data should be captured, in accordance with the definitions, or based on the information needs of the RP and data collection processes matched to these requirements. Effective monitoring of missing, incomplete, or invalid records will provide an indication of data quality.

6.2 Inventory

The data inventory is a comprehensive catalogue of data assets held by the RP. This is sometimes known as a Data or Information Asset register. A well-maintained register should include up-to-date and detailed information regarding who owns the data and the systems it's held in, as well as the source of the data within the organisation. This will provide the backbone of the organisation's risk assessment framework, thereby enabling Data Owners to have oversight of risks identified through Data Protection Impact Assessments (DPIAs).

All data domains (e.g. customer, property, etc) will have defined ownership and accountability recorded in the Data Inventory.

6.3 Reporting tools

There are a number of reporting tools on the market and each RP will need to weigh up what is best for their own requirements.

Whatever reporting tool chosen should enable:

- Easy self-serve reporting across the business
- Clear way to manage and audit access to sensitive data
- Easy to understand visualisation of data
- Integrate with other systems
- Allow reporting to be viewed across devices and not just desktop.

It is important to consider the organisation of reports within the reporting system. Reports need to be consistently managed and administered, but also easy for users to find and access the reporting they need.

7.0 Data Architecture and Quality

7.1 Sources of data

Determining which sources of data to include in our data architecture will be specific to each RP, but examples include line of business systems (Housing Management System (HMS), Asset management, finance, HR etc), structured data such as SharePoint, Electronic Discovery Reference Model (EDRM) and unstructured data held in spreadsheets, network drive content, email. All sources need to be fully understood and assigned a data owner to ensure data protection, quality and integrity are maintained.

Master Data Management processes could be used to consolidate multiple system data - identifying issues for upstream action - and to populate downstream data usage. Most important data items should be actioned with a weekly data quality report published. This process allows RPs to identify where data issues are being surfaced for investigation and action, including end user training.

7.2 Filling the gaps in our existing data

There may be gaps in data held by the RP in systems such as asset data, accurate householder information, contact/ social preferences. Work should be done with specific departments and customers to fill these gaps in data. Reporting should be set up to identify missing data so that these gaps can be rectified in a timely manner where possible.

Where the gaps in data cannot be filled through internal work or updating customer information it may be prudent to explore where external sources of data might be used to fill these gaps. This may be through publicly available sources such as the census data or by working with external data companies to match survey data on household composition and spend.

Case study – Getting to know WCHG's customers better

The 'Customer Segmentation' project is part of Wythenshawe Community Housing Group (WCHG)'s Customer Experience workstream. It supports Corporate Plan outcomes linked to the Living Well and Smarter Business themes.

This innovative work will help WCHG to

- Understand more about their current tenants and highlight areas of data quality;
- Gain insight into their use of services outside of the Group such as digital skills;
- Build a model of segmentation that can be used as lens to review all working practices;
- Provide a framework in which to trial 'nudge' communications; and
- Improve the Group's overall offer to tenants.

In July 2021, customer facing teams across the Group came together to consider some of the risks of personalising our services by creating a 'customer segmentation model'. The Group developed two use cases to prioritise the development of this model. By starting with the least risky use case, the group can learn from this experience and build a business case for more complex use cases in future phases:

Use case 1 – "Providing you with the right services first time"	**Use case 2 – "Helping you manage your affairs in difficult times"**
Low-medium risk (all relevant risks to be identified and managed through the DPIA process). We will proceed with profiling activity against this use case, once we have balanced the risks and benefits to customers, or put an informed consent mechanism in place.	Medium – high risk activity (some aspects of the processing may create high risks for individuals which must be reduced before proceeding). We will delay profiling activity against this use case until the group has had more time to consider and manage these risks.

Having completed the DPIA for use case 1 to balance privacy rights with the benefits of tailored services, the project team will continue to engage WCHG's Customer Experience Committee on the next steps for this work. The Strategic Information Committee will oversee the risk management process as the focus of the project shifts to more complex profiling uses.

7.3. Data Quality and Assurance

The business should aim to conduct a regular internal audit on data quality and assurance, to ensure that the DMF is being followed. These audits should be conducted at the very least once a year, but if significant work is needed to improve the quality and management of data in your organisation, it may be prudent to conduct this on a bi-annual (6 monthly) basis.

The day-to-day management of data should be quality assessed by the central Data Team/Function, by working with business owners to assess the quality of data being captured, ratify any anomalies with reporting and ensure colleagues are aware of their responsibilities with data management.

Organisation-wide assurance for data management and quality should be led by a group whose role it is to:

- Oversee the implementation of the Data Strategy
- Champion the benefits of the Data Strategy
- Ensure the elements of the strategy are adopted consistently through the organisation
- Monitor the adherence of the organisation to the data policies and principles
- Own and govern maintenance of the Data Model and Data Catalogue.

7.4 How we store our data – our data architecture

The organisation's data architecture defines the corporate model for the data assets we use to operate our business, including a catalogue to show where data are stored and how they flow through the organisation.

The Open Group Architecture Framework (TOGAF) is a framework for assisting in the acceptance, production, use and maintenance of enterprise architecture and attempts to address the problem of business and IT alignment. The four domains of the standard are:

- **Business Architecture**: defines the business strategy, governance, organisation and key business processes.
- **Data Architecture**: describes the structure of an organisation's logical and physical data assets and data management resources.
- **Application Architecture**: provides a blue print for applications tied to core business processes.
- **Technology Architecture**: describes the logical software and hardware capabilities required (including IT infrastructure, networks, comms etc.)

The TOGAF standard is a comprehensive methodology whose core concepts and building blocks will be applicable to every RP; however, its more prescriptive elements should definitely be tailored to the individual organisation.

Other architecture frameworks include Zachman; FEAF; DoDAF, however, the consensus appears to be that they each have their strengths and weaknesses and should be used with caution.

8.0 Conclusion

The premise of this white paper is that the challenge RPs in Greater Manchester face is not the collection of more and more data. As the Greater Manchester Information Strategy sets out, the real challenge is to join up and make sense of the data we already have.

This is no easy task. However, we believe that a Data Management Framework for the city region can support RPs to build a fit for purpose information ecosystem in three key ways:

- First, the Framework equips providers to define the relationships between different data roles and ensure that each party has clearer responsibilities over their data elements

- Second, the Framework sketches out possible pathways for streamlining data management approaches to create sharper insights that deliver more efficient decision making

- Third, we contend that a more accountable organisation which is able to rely on well managed data to make informed decisions is one that can provide highly effective services to its customers.

We hope that this document will be the first iteration of many, as GMHP continues to mature its data culture. The final message we wish to leave readers is therefore to consider your current data maturity position and use the appropriate tools and resources we have shared here to create your own blueprint for realising the full potential of your data.