General Data Protection Policy

Version 1.0

Date of Last Update: December 2017

Version Control

Note: minor updates increase version number by 0.1; major updates increase version number by 1.0.

Version Number	Sections Amended	Date of update	Approved by
1.0	First version (incorporating GDPR compliance 25th May 2018).	Oct 2017	Board
	Checked and suggested format amendments made by Bevan Brittan Solicitors and adopted.	Dec 2017	

TABLE OF CONTENTS

YARLINGTON HOUSING GROUP'S DATA PROTECTION POLICY

1 POLICY STATEMENT

1.1 Yarlington Housing Group's Data Protection Policy (**The Policy**) sets out our commitment to protecting personal data, how we implement that commitment with regards to the collection and use of personal data and ensures that:

1.1.1 we comply with data protection law and follow good practice;

1.1.2 we protect the rights and freedoms of those whose personal data we use;

1.1.3 we are open and transparent in the way we collect, use, share, store and delete personal data; and

1.1.4 we ensure that we have appropriate technical and organisational safeguards in place to minimise the risk of a data breach.

1.2 The purpose of this Policy is to set out the basis on which we will process any personal data which we collect directly from the individuals to which the data relates or personal data that is provided to us from other sources. This policy sets out our obligations on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

1.3 This Policy applies to all individuals who use personal data on behalf of Yarlington Housing Group (**Yarlington**) including employees, involved residents and board members of Yarlington Housing Group itself and our affiliated companies such as Yarlington Homes Limited, Yarlington Property Management Limited and Inspired to Achieve.

1.4 The Policy applies whenever duties are carried out on behalf of Yarlington. Those using personal data on behalf of the Group are required to be familiar and comply with the Policy's terms.

1.5 This Policy does not form part of any employee's contract of employment and may be amended at any time.

2 OUR USE OF PERSONAL DATA

2.1 Yarlington and our subsidiaries need to gather and use certain information about individuals. The categories of individuals about which we collect and use personal data include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

3 DATA PROTECTION LEGAL FRAMEWORK

3.1 We are committed to ensuring that we comply with the requirements of the data protection laws in force in England and Wales (the Data Protection Laws). The Data Protection Laws include the Data Protection Act 1998, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 as they are in force from time to time. The Data Protection Laws also include any formal written guidance published by the Information Commissioner's Office.

3.2 The Data Protection Laws apply to personal data. Personal data is information from which a living individual either can, or potentially can, be identified. The Data Protection Laws apply to information about individuals which is in electronic form or in hard copy (where such information either is, or is intended to be, stored in a relevant filing system).

4 THE DATA PROTECTION PRINCIPLES

4.1 The data protection principles form the bedrock of the Data Protection Laws and must be complied with at all times when using personal data.

4.2 Under the GDPR there are 6 data protection principles (article 5). The principles require those using personal to ensure that personal data is:

4.2.1 used in a way which is lawful, fair and transparent (***the first data protection principle***);

4.2.2 only collected for a specified, explicit and legitimate purpose (***the second data protection principle***);

4.2.3 adequate, relevant and limited to what is necessary for processing purpose (***the third data protection principle***);

4.2.4 accurate and up to date (***the fourth data protection principle***);

4.2.5 kept in a form which allows identification of individuals for no longer than necessary (***the fifth data protection principle***); and

4.2.6 kept appropriately safe against unauthorised processing, accidental loss, destruction or damage (***the sixth data protection principle***).

5 LAWFUL CONDITION FOR PROCESSING

5.1 The first data protection principle requires us to ensure that we have a lawful basis for any processing of personal data. There are six lawful bases prescribed in Article 6 of the GDPR which include:

5.1.1 the individual has provided their consent for us to use their data for a particular purpose; and

5.1.2 our use of an individual's personal data is necessary in order for us to perform a contract between us and that individual.

5.2 Unless another lawful basis applies, we shall only use the personal data of a customer or an employee as is necessary for us to perform the contract between us and the customer or employee. Where the use of a person's personal data is necessary for us to perform a contract with that person, we do not also need their consent for such use.

5.3 Special categories of personal data (which were previously termed 'sensitive personal data'), includes information relation to a person's: (1) racial or ethnic origin; (2) political opinions; (3) religious beliefs / beliefs of a similar nature; (4) membership of a trade union; (5) physical or mental health; and (6) sexual orientation.

5.4 In order to lawfully use special categories of personal data, we must satisfy an additional lawful basis which is listed in Article 9 of the GDPR. (also see Lawful Processing Guide).

5.5 The lawful basis on which we shall rely in relation to any particular categories of personal data and special categories of personal data shall be documented on our Information Asset & Risk Register.

5.6 We shall inform the individual of the lawful basis on which we shall rely through a privacy notice which has been made available to them.

6 CONSENT

6.1 Where consent is the lawful basis for processing personal data, the consent must be freely given by the individual. If there is an imbalance of power between us and the individual, consent can rarely be

said to be freely given, e.g. there will typically be an imbalance of power between an employer and employee. The provision of consent cannot be a condition for us to provide a service to an individual – that would not be freely given.

6.2 Consent under the GDPR must also be specific – we need to be clear in relation to what we are seeking consent for and it cannot be too wide-ranging. The individual must also take an active step to indicate that they are providing their consent - silence, pre ticked boxes or inactivity does not constitute consent.

6.3 Where we do rely on consent for us to use their personal data for a particular purpose, employees must provide evidence of their consent through a completed consent form in digital or hard copy format. The completed consent form must stored appropriately, Yarlington's CRM and document management system for residents/customers and employees on their files.

6.4 Consent can be withdrawn at any time: Yarlington will provide details of how this can be done on all consent forms, our website and My Yarlington.

7 INDIVIDUALS' RIGHTS

7.1 The Data Protection Laws provide individuals with prescribed rights relating to the use of their personal data. As an organisation, we must not infringe those rights.

7.2 Under GDPR the rights which individuals have over the use of their personal data include the following:

7.2.1 **The right to be informed:** Individuals have a right to be told how we use their personal data.

7.2.2 **The right of access:** individuals have a right to access their personal data which we hold**.**

7.2.3 **The right to rectification:** Where personal data is inaccurate or incomplete, an individual has the right to have that data rectified.

7.2.4 **The right to erasure:** In certain circumstances, an individual can ask that we delete their personal data.

7.2.5 **The right to restrict processing:** Individuals can limit our use of their personal data in certain circumstances.

7.2.6 **The right to data portability:** In certain circumstances, individuals can request that we provide their personal data in a way which can easily be reused by them or other service providers.

7.2.7 **The right to object:** Individuals can, in certain circumstances, object to our use of their personal data.

7.2.8 **The right not to be subject of automated decision:** Individuals can insist that they are not the subject of an automated decision concerning them.

8 SUBJECT ACCESS REQUESTS

8.1 All individuals (employees, residents, board members, contractors etc) who are subject of personal data held by Yarlington have the right to request access to personal information that we hold about them (a subject access request). There are limits to this right such as where the disclosure of such information would unreasonably infringe the data protection rights of a third party.

8.2 Further information about our approach to subject access requests is set out in our Subject Access Procedure.

9 RIGHT TO ERASURE

9.1 A data subject may request that any information held on them is deleted or removed and any third parties who process or use data must also comply with the request.

9.2 The right to erasure only applies in specific circumstances which include:

9.2.1 If the personal data is no longer necessary in relation to the purpose for which it was collected;

9.2.2 We are relying on the individual's consent as the lawful basis for processing personal data;

9.2.3 We are relying on a legitimate interest as the lawful basis for using the personal data and there are no overriding legitimate grounds for the processing;

9.2.4 We are unlawfully using the data.

9.3 Where we are using the personal data lawfully in a manner which is necessary for us to perform a contract between us and the individual, the right to erasure will not apply.

9.4 Please see Lawful Processing Guide for further information.

10 TRANSPARENCY

10.1 The first data protection principle requires us to be transparent in relation to the personal data which we use. This includes being transparent with the individuals whose personal data we process and also being transparent with the Information Commissioner's Office.

Privacy Notices

10.2 We will be transparent and provide accessible information to individuals about how we will use their personal data. This will be done through the provision of privacy notices.

10.3 The information which we are required to provide to individuals in a privacy notice are set out in Articles 13 and 14 of the GDPR and includes the following information:

10.3.1 Our identity and contact details;

10.3.2 The contact details of our Data Protection Officer;

10.3.3 Our purpose for processing the personal data;

10.3.4 Our legal basis for processing the personal data;

10.3.5 Our legitimate interests for using the data (if this is the lawful basis on which we rely);

10.3.6 Any third parties with whom we share the personal data;

10.3.7 Whether we transfer the personal data outside of the European Economic Area, and details of the safeguards for such a transfer (including details of adequacy decision);

10.3.8 the period for which the data will be stored;

10.3.9 description of individual's rights;

10.3.10 the right to withdraw consent (if consent is the lawful basis on which we are relying);

10.3.11 the right to lodge a complaint with the Information Commissioner's Office;

10.3.12 any statutory or contractual requirement which we are relying on to process their personal data;

10.3.13 where the personal data is required to enter into a contract;

10.3.14 any consequences of failing to provide the personal data to us; and

10.3.15 if our use of the data involves any automated decision-making.

10.4 We have created a suite of privacy notices for different categories of individuals which include:

10.4.1 The Employee Privacy Notice;

10.4.2 The Contractor Privacy Notice; and

10.4.3 The Resident & Customer Privacy Notice

10.5 It may be necessary to have tailored notices where extra information is collected, processed and shared, e.g. if extra support is provided to vulnerable residents or where employment advice is provided, etc.

10.6 We shall also publish a Privacy statement on our website which shall set out how personal data relating to individuals is used by us as well as how individuals can exercise their rights under the Data Protection Laws.

11 ACCOUNTABILITY AND DATA MANAGEMENT

DATA PROTECTION BY DESIGN AND DEFAULT

11.1 The GDPR requires us to consider data protection by design and default. This obligation requires us to consider the data protection implications of any project or process both at the point of inception and throughout the life of any processing. Data protection is something which should also be a consideration in relation to everything and anything we do with personal data.

11.2 Those who use personal data on our behalf are required to consider data protection by design and default.

RECORD KEEPING

11.3 Under the GDPR, we are required to maintain records of our data processing activities. Those records shall be created, maintained and held by our Data Protection Officer.

DATA PROTECTION IMPACT ASSESSMENTS

11.4 A DPIA is an essential tool for demonstrating our compliance with the GDPR. It is used to work out the impact which our use of personal data will have on individuals and is required by law if our use of personal data is likely to result in a high risk to individuals.

11.5 Where our use of personal data is likely to create a high risk to individuals, a DPIA should be completed before a new project or operation involving personal data begins.

11.6 To complete the DPIA, we need to: (1) outline the scope of the project; (2) establish the risks to individuals' personal data which arise from the project; (3) consider how we can reduce those risks; and (4) identify the remaining risk once the mitigation steps are in place. If the remaining risk is still high risk, we will need to consult with the Information Commissioner's Office before proceeding.

12 SHARING DATA WITH OTHERS

12.1 In order to share personal data with any third party we must have a lawful basis for doing so. Apart from in limited exceptional services, we will also need to inform the individual about such sharing in advance.

12.2 In limited circumstances, we may disclose personal data to an organisation without first informing the individual beforehand. An example may be where the sharing of data is necessary for the prevention and detection of a crime. Under such circumstances, staff will ensure the request is legitimate, and seek guidance from the Data Protection Officer.

12.3 Where we share personal data with a third party organisation, either regularly or for one off project, we shall consider whether a data sharing agreement and/or non-disclosure agreement is appropriate in the circumstances. If a data sharing agreement is completed, this will be recorded on the Information Asset Register.

CONTRACTS

12.4 All contracts will set out the requirements for compliance with the GDPR and the third party arrangements for ensuring any information shared is retained in line with GDPR. This is particularly relevant where another organisation is processing personal data on our behalf as the GDPR imposes strict requirements in relation to the need to have a written contract in such situations and also the clauses which must be included in such an agreement.

12.5 Compliance with GDPR will also be a standard requirement for any Data Sharing Agreement or Non-Disclosure Agreement. Any data shared will be through an appropriately secure method, e.g. encrypted email or secure portal.

TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE OF THE EEA

12.6 As an organisation, we shall not transfer any personal data outside of the European Economic Area unless our Data Protection Officer has confirmed that such a data transfer is lawful and appropriate in the circumstances.

13 DATA RISKS, BREACHES AND SECURITY

DATA PROTECTION RISKS

13.1 This policy helps to protect Yarlington from some very real data security risks including:

13.1.1 **Breaches of confidentiality –** information being shared or made public inappropriately.

13.1.2 **Reputational Damage -** For instance, the company could suffer if sensitive data was accessed by hackers. Refer to Cyber Security Policy.

13.1.3 **Loss of Customer Trust** - residents no longer volunteer information.

13.1.4 **Need to minimise risk of fines through compliance with this policy, as impact of the maximum fine is a catastrophic risk (i.e. potential loss of over £10m, however likelihood is rare).**

13.2 As part of our commitment to GDPR and risk management, Yarlington will maintain Cyber Essentials accreditation to help limit the cyber risk in relation to potential cyber-related GDPR breaches.

Reporting of data breaches

13.3 Anyone who is using personal data on our behalf is required to report all actual or potential data protection compliance failures and breaches to the Data Protection Officer as soon as they are discovered.

This allows us to:

13.3.1 Investigate and take any required remedial actions if necessary.

13.3.2 Maintain a register which can be monitored and record lessons learned.

13.3.3 Report to Information Security Forum. (Via Security Officer/Head of Business Assurance/DPO or Security Officer/ Head of Information).

13.3.4 Notify the Supervisory Authority (Information Commissioner's Office) in line with the GDPR timescale of 72 hours.

13.4 The Security Breach Guidance contains further information.

13.5 Annex 1 to this Policy sets out further requirements which staff must adhere to when using personal data on behalf of us. **Failure to comply with this policy may result in disciplinary action.**

14 MONITORING AND COMPLIANCE

14.1 Data Protection Audits will take place in line with the GDPR requirements either by external providers or Yarlington's Internal Business Assurance Team at regular appropriate intervals and by an external specialist at least every 5 years.

15 ROLES AND RESPONSIBILITIES

Information Security Forum

15.1 In compliance with the GDPR, and to ensure good information governance, the Information Security Forum has been established to provide ongoing steer, support, monitoring and actions in respect of:

15.1.1 GDPR compliance;

15.1.2 Any breach of the data protection laws (including cyber-attacks) and notification to the Information Commissioner's Office;

15.1.3 Responses to any breach of the data protection laws including mitigation steps and strategies;

15.1.4 Compliance with individuals' rights under the data protection laws;

15.1.5 Maintaining an information asset register;

15.1.6 Identifying significant risks to the protection of personal data;

15.1.7 To oversee the conduct of Data Protection Impact Assessments.

15.2 The Group membership consists of the following posts:

15.2.1 Senior information risk owner (SIRO); ED of Finance & Corporate Services

15.2.2 Security Officer; Head of Business Assurance

15.2.3 Security Officer; Head of Information

15.2.4 IT Security Officer; IT Manager and

15.2.5 Head of Operations & Customer Experience.

15.3 Other individuals may be temporary members of the Group at certain times as required.

Data owners (Information Asset Owners)

15.4 These are the Heads of service and are responsible for ensuring that specific information assets are handled and managed appropriately. Their key responsibilities are:

15.4.1 Lead and foster a culture that values, protects and uses information within the law for public good.

15.4.2 Know what information assets are held, who this information is shared with and for what purpose.

15.4.3 Be responsible for defining who has access and why, and ensure that their use of the asset is monitored if required.

15.4.4 Identify any risks to the asset, and support risk management activity including considering the integrity, availability and confidentiality of the information.

Responsibilities

15.4.5 **The Board and Executive Team** are responsible for establishing and maintaining a control environment that promotes overall compliance. Approval of this policy and any significant amendments or updates made to it.

15.4.6 **All employees, involved residents, and Board Members** are responsible for ensuring, whilst undertaking their roles; they do so in compliance with this policy and the GDPR & Data Protection Bill. They also have responsibility to report actual or potential data security breaches to the Information Security Forum through the Security Officers (Heads of Business Assurance and Information) or Internal Auditor.

15.4.7 **Head of Business Assurance** will act as DPO and be responsible for tasks set out in Articles 38 and 39 of the GDPR to ensure that we remain fully compliant.

15.4.8 **Internal Auditor** is responsible for maintaining Yarlington Housing Group's registration with the ICO and for handling data protection questions from staff and all those covered under this policy. Providing guidance on the GDPR, reviewing and updating Yarlington's policy and overseeing requests from individuals to see the data held on them (SAR).

15.4.9 **Head of Information** is responsible for ensuring all systems, services and equipment used for storing data meet acceptable security standards, and ensuring that regular checks are performed through scans and penetration testing etc. to ensure security hardware and software is functioning properly. Evaluating any third party services the company is considering using to store or process data.

15.4.10 **HR and Learning & Development Team**, along with the DPO, are responsible for the provision of adequate training.

15.4.11 **Data Owners (Heads of)** are responsible for entries and amendments to the Information Asset Register. Also leading and fostering a culture that values, protects and uses data within the law for public good and know what data assets are held, who this data is shared with, know who has access and why, ensure that their use of the asset is monitored if required and identify any risks to the asset, and support risk management activity. They will ensure that their teams are regularly reviewing files held (hard and electronic) including archived files to implement secure disposal in line with the retention timescales applied.

15.4.12 **The Procurement Manager** is responsible for ensuring that all contracts and tender documents are compliant with GDPR and the third party has adequate policy and procedures in place for GDPR.

15.4.13 **The Head of Communications** is responsible for addressing any data protection queries from journalists or media outlets. Where necessary, ensuring that communications such as emails and letters contain the required Data Protection statement along with working with other staff to ensure promotional communications abide by data protection principles.

15.4.14 **Information Security Forum** is responsible for monitoring and ensuring compliance in respect of:

(a) Cyber attacks and data protection breaches;

(b) GDPR;

(c) GDPR Breaches and notification to ICO

(d) Rectifying actions for the above

(e) Subject Access Requests

(f) Requests for erasure

(g) Information asset register

(h) Significant data risks

(i) Privacy Impact Assessments

16 ACCOMPANYING POLCIES

16.1 This Policy is the overarching document for Yarlington's Data Governance Framework. Other documents which form part of this framework are:

16.1.1 The Data Breach Procedure;

16.1.2 The Subject Access Procedure;

16.1.3 The Information Asset Register;

16.1.4 The Data Retention Policy; and

16.1.5 The Information Asset Risk Register.

16.2 Other Policies and Documents to Consider, and that should be read in conjunction with this policy are:

16.2.1 Subject Access Request Register

16.2.2 Tidy Desk / Clear Desk Policy

16.2.3 Security Breach Register

16.2.4 Security Breach Guidelines & Form

16.2.5 Social Media Policy

16.2.6 Secure Encryption Policy

16.2.7 ICT Systems usage Policy

16.2.8 IT – agreeing Access Rights & Changes

17 CHANGES TO THIS POLICY

17.1 This policy will be reviewed every two years or following any changes or updates in relevant legislation.

ANNEX 1: STAFF REQUIREMENTS WHEN HANDLING PERSONAL DATA

Those handling personal data on behalf of Yarlington are required to comply with the following obligations at all times:

1 ACCESS TO PERSONAL DATA

1.1 The only people able to access data covered by this policy should be those who **need it for their work on behalf of Yarlington.**

1.2 When access to confidential information is required, employees need to request it from their line managers and decisions made should be recorded. **Data will not be shared informally**.

1.3 All paper records and files containing personal, sensitive or confidential records about individuals, suppliers and contractors must be held securely in all of our offices and archive facilities (Armoury Road). Access to secure storage is limited to employees who have a business need to do so. Data may only be taken off Yarlington's and subsidiaries premises by employees who have a business need to do so. It must be kept securely at all times.

1.4 When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking. (Refer to ICT Systems Usage policy).

2 KEEPING DATA SECURE

2.1 Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

2.2 **Strong passwords** must be used, changed in line with set IT policies and they should never be shared.

2.3 Personal data **will not be disclosed to unauthorised people**, either within the company or externally.

2.4 Employees will make sure paper, printouts or files are **not left where unauthorised people can see them**, e.g. meeting rooms or on a printer.

2.5 Yarlington operate a **clear desk** policy ensuring that any documentation (paper or files) should not be left out but kept in lockable drawers or cabinets.

2.6 Ensure that **computer screens are locked** whenever they are left unattended.

2.7 Data printouts should be placed into shred it bins provided and disposed of securely when they are no longer required.

2.8 Employees will not save copies of personal data to their own home computers or Yarlington devices c drives.

2.9 Personal data will not be sent by standard email, as this form of communication is not secure. Data must be encrypted before transferring electronically. Please refer to Secure Encryption Policy.

3 DATA MINIMISATION

3.1 Standard reports (spreadsheets) **will be data minimised** to remove personally identifiable information and only be available to those who need them for their work.

4 DATA PROTECTION TRAINING

4.1 Data Protection training is provided within the company induction programme and **the online Data Protection package needs to be completed before access to personal data is given.**

4.2 All employees are required to complete the online Data Protection package every two years.

5 KEEPING DATA UP TO DATE:

5.1 Data will be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of securely. **This includes electronic and hard copy files held at all offices, on schemes and at Armoury Road** (please refer to retention periods found in the Information Asset Register/Retention policy).

5.2 **Data should be kept up to date and accurate with inaccuracies updated as soon as they are discovered**. For example, if a customer can no longer be reached on the recorded telephone number, it should be removed from the database.

5.3 Yarlington has made it easy for data subjects (i.e. customers/residents/other occupants) to update the information it holds on them through My Yarlington (customer portal).

5.4 It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept up to date and accurate as possible. Staff should take the opportunity to ensure data is updated. For instance, by confirming a customer's details whenever they interact with them.

6 SEEKING ADVICE

6.1 Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.