FIRST CHOICE HOUSING ASSOCIATION LTD

DATA PROTECTION POLICY

1.0 INTRODUCTION AND PRIVACY STATEMENT

1.1 First Choice Housing Association (FCHA) is required to gather certain information about individuals in order to carry out its functions. This can include information on tenants, employees, contractors, stakeholders and others the association may have a relationship with. In addition FCHA may be required by law to collect and use information in order to comply with the requirements of local and central government.

1.2 The Association will take all reasonable steps to ensure compliance with the Data Protection Act 2018 and is registered under the General Data Protection Regulations (GDPR), Number Z464170X. The Director of Corporate Services (DCS) is the appointed Data Protection Controller and is responsible for data handling. This data must be handled and dealt with properly however it is collected, recorded and used, whether it is on paper, in computer records or recorded by other means.

1.3 By providing us with your information you are consenting to us using your information as set out in this policy. Your information will be used to provide you with information and services that you request from us, and for other legitimate business purposes. We may offer you the opportunity to opt in to receiving additional information about our activities or those of our partners and service providers. You may opt out of this at any time by contacting us.

2.0 POLICY STATEMENT

This policy describes how information must be collected, handled and stored to meet the organisation's data protection standards, and to comply with the law.

This policy applies to all FCHA suppliers, contractors and staff (including Board members), and to all data that the organisation holds relating to identifiable, living individuals, even if that information technically falls outside of the GDPR.

The Data Protection Act which became law in May 2018 describes how organisations must collect, handle and store personal and sensitive information. These rules apply whether the information is stored electronically, on paper or on other materials.

3.0 DEFINITIONS

Some helpful definitions are set out below to assist in your understanding of this Policy:

Personal data: means information about a living person who can be identified by that information or together with other information that the Data Controller has or is likely to obtain. This is information that relates to an identifiable living individual,

whether in person, family or business life. You must not share personal data with any third party unless expressly authorised to do so. (See Appendix 5)

Sensitive Personal Data: means certain personal data that is given special status in data protection legislation. Sensitive personal data is personal data consisting of information as to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health conditions, sexual life, medical information, commission or the alleged commission of an offence or the sentence of any Court in such proceedings. Sensitive Personal data can only be collected and processed with that individual's express consent, which would generally require the consent to be written.

Data Subject: means all staff and customers of FCHA

Subject Access Request: means a request made by or on behalf of an individual for the information held about an individual

4.0 RESPONSIBILITIES

All staff are responsible for protecting information located across the association and contained in different file formats and stored on physical devices by ensuring that information is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. A checklist guide has been provided to all staff and is available via the staff intranet. (Appendix 1)

Responsibility for ensuring the effective communication, implementation and operation of this Policy rests with the members of the FCHA Board, the Chief Executive, Company Secretary and the Executive Management Team.

The Director of Corporate Services will

- Take action where there is evidence of a breach and for ensuring records are kept in accordance with the principles of the policy
- Notify the Information Commissioners Office under the GDPR guidelines
- Keeping the Board updated about data protection responsibilities, risks and issues.
- Process Subject Access Requests.
- Take responsibility for the maintenance of the Information Asset Register alongside relevant Executive and Management team responsibilities
- Check and approve contracts or agreements with third parties that may handle the company’s sensitive data.
- Review this and related policies in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handle data protection questions from staff and anyone else covered by this policy.
- Approve any data protection statements attached to communications such as emails and letters.

- Address any data protection queries from journalists or media outlets like newspapers.
- Where necessary, work with other staff to ensure marketing initiatives abide by data protection principles.
- Ensure a privacy notice is clearly available via the associations website

The Director of Finance & ICT will

- Ensure systems, services and equipment used for storing data meet acceptable security standards.
- Perform regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluate any third-party services the company is considering using to store or process data, for instance, cloud computing services.
- Ensure personal sensitive information is kept secure

4.0 GDPR PRINCIPLES –FCHA are committed to following the following principles

1. Lawfulness, fairness and transparency

Transparency: Tell the subject what data processing will be done.
Fair: What is processed must match up with how it has been described
Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)]

2. Purpose limitations

Personal data can only be obtained for "specified, explicit and legitimate purposes"[article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

3. Data minimisation

Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[article 5, clause 1(c)]
i.e. No more than the minimum amount of data should be kept for specific processing.

4. Accuracy

Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)]
Baselining ensures good protection and protection against identity theft. Data

holders should build rectification processes into data management / archiving activities for subject data.

5. Storage limitations

Regulator expects personal data is “kept in a form which permits identification of data subjects for no longer than necessary”. [article 5, clause 1(e)] i.e. Data no longer required should be removed.

6. Integrity and confidentiality

Requires processors to handle data “in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage”. [article 5, clause 1(f)]

As a housing association FCHA is not subject to the Freedom of Information (FoI) Act and there is no statutory obligation for us to respond to requests. We endeavour to provide requested information where we can and where it is readily available

7.0 DATA USE AND SECURITY

7.1 How we handle information is very important. Our customers have entrusted their information with us, and if we were to misuse or lose personal information it could cause serious harm or distress to people. Confidential and sensitive information needs to be kept secure, but it also needs to be available when required. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

7.2 The need to ensure that personal data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All staff should ensure that:

- Any personal data which they hold is kept securely.
- Identity checks are carried out before giving out personal information.
- Data is held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Data is regularly reviewed and updated if it is found to be out of date or no longer required, it is deleted and disposed of.
- Data is not shared informally. When access to confidential information is required, employees may request it from their line managers.
- Personal data is not disclosed either orally or in writing, intentionally or otherwise to any unauthorised third party.
- Where personal data is processed by a third party on behalf of FCHA, there is a written contract between the parties which specifies that the data processor agrees to act on FCHA instructions only, and to abide by the provisions of the GDPR Act in connection with data security.

7.3 All personal information in the form of manual records should be:

- Kept in a locked filing cabinet or drawer
- Care must be taken to ensure that manual records or printouts containing personal data are not left where they can be accessed by unauthorised staff.
- Manual records or printouts containing personal data that are no longer required are shredded and disposed of securely.
- Identifiable images are not used nor personal data uploaded online without the express consent of the individual.
- Personal data is not sent in the body of an email as this form of communication is not secure. Personal data may be attached within an email so long as the attachment is password protected.
- Data is protected by strong passwords that are changed regularly and never shared between employees.
- Data stored on removable media (like a CD or DVD) is kept locked away securely when not being used.
- Data is stored only on designated drives, servers and devices, and should only be uploaded to an approved cloud computing services.
- Data is encrypted before being transferred electronically - the IT team can explain how to send data to authorised external contacts.
- Screens for computers and other devices are always locked when left unattended.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Assistance is sought from the Data Controller If they are unsure about any aspect of data protection.

7.4 Staff working outside of FCHA business premises should take care to avoid extra risks by not discussing sensitive information publically or where it can be overheard, and should be careful about accidentally disclosing data when handling devices in the presence of other people.

All possible steps will be taken to maintain effective security for the whole of the computer system. Access to information stored on computer systems and devices should be appropriately password protected. Staff must take all necessary steps to avoid careless loss of data, particularly when working remotely.

A *staff checklist* is included at *Appendix 1* to act as a guide for staff. Please note the association has a retention policy which link to this policy (O22) to ensure the association complies with the fifth principle.

7.5 Transit of data

Any transit of data must be done so securely in line with appropriate technical and organisational measures to protect shared personal data. In some instances we may transfer personal data to another organisation but still remain responsible for its security. You should:

- always use an appropriate form of transport e.g. secure courier for sensitive paper based personal data and encryption on email, secure file transfer protocol (SFTP) or Virtual Private Network (VPN) for electronic files;
- minimise data being transported;
- log the transfer in and out where appropriate and check to ensure that data is received; and
- employ security measures to safeguard the data in transit such as tamper evident packaging, and storage on encrypted devices.

8. BREACHES

It is the responsibility of all staff (including Board members) to comply with this policy, and to understand their obligation to ensure that they have regard to the six GDPR principles above when accessing, processing or disposing of personal information. Failure to observe the principles within this policy may result in staff incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if employment records are accessed without the requisite authority, the organisation will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

In addition, a failure to comply with this policy could expose the business to enforcement action by the Information Commissioner (which could result in restrictions being imposed on our use of personal data and significant fines), or to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.

Where an individual suffers damage or loss because of unauthorised disclosure, inaccurate or missing data, or the loss or destruction of data in relation to themselves they may seek compensation from the courts. For these reasons, it is important that all staff familiarise themselves with this policy.

Any breach and/or potential breach must be reported immediately to the DCS. Always report lost or missing information immediately as the cost of hiding or ignoring a loss can be far worse.

9.0 SURVEILLANCE AND MONITORING

FCHA has a legitimate interest in monitoring the behaviour of staff and customers who attend offices and may wish to carry out monitoring in order to prevent inappropriate behaviour or to prevent or detect any unlawful act.

Monitoring can take several forms. It can involve e-mail and Internet monitoring, telephone monitoring or monitoring by way of Closed Circuit Television (CCTV). FCHA holds information on the destination and duration of calls made from the the association’s telephone system, and from the use of other IT systems and devices and may use this information if misuse is suspected. In operating this policy individuals must comply with the requirements laid down in FCHA ICT policies and procedures.

10.0 SUBJECT ACCESS REQUEST

All individuals who are the subject of personal data held by FCHA are entitled to ask what information the association holds about them and why, how to gain access to this information, be advised how the information is kept up to date and how the association is meeting its obligations under the GDPR.

If an individual contacts FCHA requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email to donnalloyd-williams@fcha.org.uk or via the *Subject Access Request Form* **(**Appendix 2). Subject Access Requests should be passed immediately to the Data Controller. The Data Controller will provide the relevant data within 28 calendar days of receipt of the request. The Data Controller will always verify the identity of anyone making a subject access request before handing over any information.

Where the provision of information would reveal the identity of a third party, the information may not be provided unless either the consent of that third party is obtained, or the information relating to them can be redacted so as to ensure their identify is not revealed.

Confidential and personal information cannot normally be disclosed to an unauthorised third party, unless a '*consent to disclose*' form (*Appendix 3*) has been received and verified. In certain circumstances, the Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, FCHA will disclose requested data. Where the association is required to share data we will utilise and refer to our Data Sharing Protocol which will clearly set out an agreement with relevant partners about the purpose and data to be shared with the relevant security measures applied. (Appendix 4)

11.0 DATA SHARING

If you share data with another organisation you should reference the ICO data sharing code for detailed guidance which explains the legal process for sharing of personal data. When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) you need to identify the objective that it is meant to achieve.
For FCHA this could be

- sharing of employee data between past and future employers
- Local Authority passing personal data on prospective tenants
- The passing of information about the victim of a crime to a counselling charity;
- Health Board providing information about a prospective tenant
- the police and immigration authorities exchanging information about individuals thought to be involved in serious crime;

How the code can help
Adopting the good practice recommendations in the code will help you to collect and share personal data in a way that is fair, transparent and in line with the rights and

expectations of the people whose information you are sharing. The code will help identify issues you need to consider when deciding whether to share personal data. It should give confidence to share personal data when it is appropriate to do so, but should also give you a clearer idea of when it is not acceptable.
What do we mean by 'data sharing'?
By 'data sharing' we mean the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Data sharing can take the form of:

- a reciprocal exchange of data;
- one or more organisations providing data to a third party
- several organisations pooling information and making it available to each other
- exceptional, one-off disclosures of data in unexpected or emergency situations

Before sharing any personal data you hold, you will need to consider all the legal implications of doing so. Your ability to share information is subject to a number of legal constraints which go beyond the requirements of the GDPR. There may well be other considerations such as specific statutory prohibitions on sharing, copyright restrictions or a duty of confidence that may affect your ability to share personal data. The association has a data processing agreement that it will ask third parties to sign in the event of shared data

12.0 PRIVACY IMPACT ASSESMENTS

A Privacy Impact Assessment is a simple risk assessment that should be carried out at the beginning of a project or service review, or if we are implementing a new idea or want to do things a bit differently. See Appendix 6. This would include

- collecting new information about individuals?
- using information that FCHA already have but for a different purpose?
- contacting individuals in ways they may find intrusive?
- making significant changes to the way you work which could put information about individuals at risk?

Appendix1

Checklist Guide For Staff

- Am I authorised to collect/store/process this personal/sensitive information?
- Do I really need this information about an individual? Do I know what I'm going to use it for?
- Is the information 'ordinary' personal data or is it 'sensitive' personal data?
- If it is sensitive personal data, do I have the data subject's express consent?
- Am I collecting only the personal information need for this particular business
- purpose?
- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- Do I need to obtain explicit consent to hold this information?
- Have I provided an option to opt-out where appropriate?
- Am I satisfied the information is being held securely, whether it's on paper or on computer?
- Am I sure the personal information is accurate and up to date?
- Do I delete/destroy personal information as soon as I have no more need for it? Do I dispose of confidential paper waste securely by shredding?
- Is access to this personal information limited only to those with a strict need to know?
- Do I keep my password secure? Do I change it regularly?
- Do I lock / log off when away from my desk/devices?
- Have I encrypted this personal information that is being taken out of the
- office?
- If I'm asked to pass on personal information, am I clear that I may do so?
- Do I know what to do if somebody tells me they want to see what data the association holds about them?

Appendix 2

Subject Access Request Form

Details of the Data Subject
Full name:
Home Address:
Postcode:
Telephone No:
Email address:
Details of person requesting the information
If you are not a FCHA employee and are acting on behalf of the Data Subject, please supply evidence of your identity (e.g. driving licence, birth certificate, etc.) together with written authority from the Data Subject. Please also confirm the following information:
Your full name
Your home Address:
Your postcode:
Telephone No:
Email address:
Please describe your relationship to the Data Subject that leads you to make this request for information on their behalf:
Please describe the information you seek, together with any other relevant data. This will help to identify your requirements.
Declaration to be completed by all applicants. Please note that any attempt to mislead may result in prosecution I certify that the information given on this application is true. I understand that if I am not a FCHA employee, it may be necessary for FCHA to confirm the Data Subject's identity. Signature: Date: Please return the completed form marked to The Data Controller, First Choice Housing Association Limited, Avon House , 19 Stanwell Road ,Penarth,CF64 2EZ or via email to donnalloyd-williams@fcha.org.uk If applicable, please also enclose: - evidence of your identity - evidence of the data subject's identity (if different from the above)

Appendix 3

Consent to Disclose Information

All staff employed by First Choice Housing Association (FCHA) have a legal duty to keep information about you confidential, and therefore cannot share information about you until you have given permission to do so. If you are prepared for us to share information about you please complete and return this form to FCHA.

Full name:
Address:
Contact number:
Date of birth:
Person / body requesting information:
Brief description of the information to be shared:
Please tell us of any conditions or restrictions you would like to apply:
I hereby consent to the above information being provided, and understand that I can withdraw my consent at any time in writing to FCHA
Signature: Date:

FCHA will not release information about you until we receive your Consent.

APPENDIX 4

Data Sharing Protocol

This data sharing protocol is agreed between First Choice Housing Association Ltd (Partner A)
and ……..(Partner B)
on (*date*) ……..

1. Purposes for processing the data

Common purposes for processing the data:
……
……

Partner A purposes for processing the data (if different):
……
……

Partner B purposes for processing the data (if different):
……
……

2. Data to be shared:

……
……

3. Staff Members

Staff with access to and responsibility for this shared personal data is as follows:
Partner A: ……
Partner B: ……

Data Protection Officers (partner A): ……
Data Protection Officers (partner B): ……

4. Security Measures

The following security measures have been put in place to ensure protection of data:
Partner A:
……
……
……

Partner B:
……
……
……

All partners agree to abide by the principles of the General Data Protection Regulations 2018 and to abide by any other legislation which might pertain to the transfer of personal data.

Subject Access Requests should be directed to First Choice Housing Association Limited for the attention of the Data Controller.

Data subjects have been informed of the collection and processing of their personal data, including who it will be shared with, and have been given the opportunity to object or opt-out.

Sub-contractors and consultants have received copies of this data sharing protocol, and are aware of the relevant policies and procedures of partner institutions.

Partner A:
(*name*) **……**

(signature) **……**

Partner B:
(*name*) **……**
(signature)
……

Appendix 5

How to record decisions on sharing personal information

1.0 This guide describes how to record information sharing decisions, whether you are the requestor or the recipient of a request for personal information and whether the decision is to share or not.

2.0 Why should we record information sharing decisions?

Recording information sharing decisions, including the reasons for the decisions, is necessary under Data Protection Law and General Data Protection Regulation. Without these records it may be difficult to prove that due process was followed if legal action is brought against the association.

3.0 Recording information sharing decisions where you are the decision maker

3.1 When you receive a request or decide it is appropriate to share personal information with another agency or service you must ensure that you record:
• the date and time;
• a summary of the information and the reason for the request;
• the requestor's name, job title, organisation (and telephone number);
• your decision (whether to share or not) and the reasons for this decision.

3.2 If you decide to share information you must also record:

• whether you are sharing with or without consent;
• if sharing without consent, whether the person was informed and, if not, why not;
• who consented to or authorised the information sharing,
• what type of information you shared (but not the content);
• how you shared the information, e.g. email, phone and if appropriate how receipt was confirmed.

Example of recording information sharing decisions can be seen in Appendix 5A

Appendix 6

Assessment

Name of Project / Area of Work	
Commencement date	
Lead Officer	

SECTION 1 – OVERVIEW OF THE PROJECT AND DATA PROTECTION IMPLICATIONS

Answer the following questions and give a brief outline where necessary.

1	**Give a brief description of the project / new way of working**		
2	**Data implications**	**YES**	**NO**
2.1	Will you be collecting information from **new or existing** individuals?		
2.4	Will you be using information already held by FCHA but for a new purpose?		
3.	**Sharing information**	**YES**	**NO**
3.1	Will the project involve sharing information persons / organisations		
4	**Use of Technology**	**YES**	**NO**
4.1	Will you be implementing a new system which will hold personal information?		
4.2	Will you be using different type of technology to collect, process or hold information about individuals?		
5.	**New ways of working**	**YES**	**NO**
5.1	Will you be working in a different way which will have an impact on or change the way you collect, hold or process information about individuals?		
6	**Contacting Individuals / Direct Marketing**	**YES**	**NO**
6.1	Will you be contacting individuals in a way that they may find intrusive or sending marketing material out to individuals		

SECTION 2 – INFORMATION FLOWS

Complete this section if you are:

- Collecting **new personal information** from individuals
- Using information already held by FCHA but for a **different purpose**

7	**Give a brief description of what you will be doing**
8	**List the information you will be collecting, using or sharing.**
9	**Will it include Sensitive personal information? Please List**
10	**Explain the purposes or legal basis for collecting, using or sharing the information**
11	**The information of how many individuals will be collected, used or shared?**
12	**Will individuals know that you are collecting, using or sharing their information for this purpose? Please provide details of how they will be informed.**
13	**Will you need their consent? If so please explain how you will get their consent**
14	**List the systems / methods that will be used to hold or access the information. (system, folders ,drives, Hard Copies)**
15	**How many staff will have access to the information?**
16	**What security is in place to make sure this information is kept safe?**
(you may need to work with IT on this)	
17	**If an individual makes a Subject Access Request will it be easy to obtain copies of the information held?**

SECTION 3 – USE OF TECHNOLOGY

Complete this section if you are **implementing a new system or using new technology**

18	**Describe the new system / technology and the purpose for**

	implementing it
19	**What personal information will be held / accessed on the new system / technology**
20	**Will it include sensitive personal information? Please List**
21	**What security is in place to make sure this information is kept safe?**
(you may need to work with IT on this)	

SECTION 4 – NEW WAY OF WORKING

Complete this section if you are

- Implementing recommendations made following a **service review** or implementing a **new way of working**

22	**Describe the new way of working and the purpose for the change**
23	**What personal information will be affected by this new way of working?**
24	**Does it include sensitive personal information? Please list.**
25	**Do individuals need to know about this new way of working? If so please explain how they will be informed.**
26	**What physical and technological security is in place to make sure that the information in question is kept safe?**
(you may need to work with IT on this)	

SECTION 5 – DIRECT MARKETING

Complete this section if any part of your project involves direct marketing.

27	**Describe the method / methods of direct marketing you will be using and the purpose for doing it**
28	**How many individuals will be contacted?**
29	**Have the individuals consented to being contacted?**
30	**Have you got a process for customers to opt out?**

SECTION 6 – PRIVACY RELATED RISKS

Risk	Severity (H,M,L)	Solution	Result of Solution	Responsible Officer	Status (RAG)

SECTION 7 – SIGN OFF

	Signature	Print Name	Date
Lead Officer			
Data Protection Officer			
Responsible Director			

Appendix 7

Processing Agreement between
First Choice Housing Association Ltd [insert supplier name]

This Data Processing Agreement is to ensure compliance with the General Data Protection Regulation (GDPR) in respect of the processing to be carried out by the Data Processor on behalf of the Data Controller.

WHEREAS:-

1. The Data Controller and the Data Processor (taking the meanings given at B below), have entered into a contract to secure the provision and processing of **personal and/or special categories of personal data** (hereinafter referred to as the 'data') identified in Schedule D of this agreement solely for the purpose of processing **[define the nature and purpose of the processing]** during **[insert start date] until [insert end date].**

B. In consideration of the Contract referred to below, IT IS HEREBY AGREED BETWEEN THE PARTIES IN SCHEDULE A AS FOLLOWS:-

Definitions & Interpretations in this Agreement

a) Data Controller - means First Choice Housing Association Limited ("FCHA") as the organisation who determines the purpose (s) and mean (s) of the processing of personal data;
b) Data Processor - means **[insert supplier name]** as the individual/organisation who will process personal data on behalf of the Data Controller
c) Data Subject - means an identified or identifiable natural person who is the subject of personal data
d) Personal Data - means any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by way of reference to an identifier n the possession of, or is likely to come into the possession of, the Data Controller
e) Special Categories of Personal Data – such has the meaning given by Paragraph 1 within Article 9 of the General Data Protection Regulation
f) Data - means datasets, personal data, and/ or special categories of personal data as defined within the General Data Protection Regulations.
g) Authorised Dataset - means the set of data stipulated at Schedule D.
h) Processing - means any operation or set of operations which is performed on personal data or on sets of personal data, whether or no by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
i) Contract - means the agreement **dated [insert date]** entered into between FCHA and **[insert supplier] for the provision of [insert services to be provided].**
j) Agreement - means this Data Processing Agreement
k) Information Commissioner's Guide to the General Data Protection Regulation (GDPR) - means the online guide published from time to time by the Information Commissioner's Office

2. The Data Processor will process authorised datasets solely for the purpose of administering the Data Controller's **[define the nature and purpose of the processing]** as shown in Schedule D and in accordance with the obligations of the Data Processor, as shown in Schedule B & C, in order to support their obligations set out in the Contract. Such processing may include personal and special categories of personal data, and shall be strictly undertaken in accordance with the warranties and obligations set out below, including the Schedules to this Agreement, and at all

times in accordance with the guiding principles and advice set out in Information Commissioner's Guide to the General Data Protection Regulation (GDPR).

3. The data sets will be provided **electronically via the data controllers email system. No data will be processed outside of the UK without the written permission of the Data Controller and data is not permitted to be processed outside of the EU.**

4. Warranty and Obligations of Data Processor

a) The Data Processor warrants that it has the necessary legal authority in the United Kingdom where it is established for the purpose of controlling the processing of the data and to use it for the purpose(s) set out herein, and to give warranties and fulfil the undertakings set out herein and to enter into this Agreement.

b) The Data Processor will process the data exclusively for purposes and in accordance with the means of processing listed in Schedule D to the exclusion of any other purposes or means of processing.

c) The Data Processor will not enter into any arrangement to process the data outside the United Kingdom without the written permission of the Data Controller. The Data Processor will not use temporary or subcontracted staff or other third parties to carry out its obligations under this Agreement, or the Contract, without prior agreement from the Data Controller. Such consent shall not be unreasonably withheld by the Data Controller. Where the Data Processor is authorised by the Data Controller to use temporary or subcontracted staff or other third parties, the Data Processor will ensure that such staff or organisations are complying with the requirements of this data processing agreement and monitor same.

d) The Data Processor warrants that it has in place security programs and procedures appropriate to the risks presented by the processing, to ensure that unauthorised persons will not have access to the data. Furthermore, that any persons it authorises to have access to the data will be bound by contract or otherwise to respect and maintain the confidentiality and security of the data.

e) The Data Processor warrants that it will comply with the organisational and technical obligations set out in Schedule C and apply them to the processing of the data originally provided or subsequently amended.

f) The Data Processor will ensure all of their staff has undertaken relevant training on data protection and information security, before this Agreement commences, and that such training is maintained on a regular basis to include periodic updates for all staff.

g) The Data Processor will ensure that they only act on the written instructions of the Data Controller

h) The Data processor will ensure that people processing the data are subject to a duty of confidence

i) The Data Processor will take appropriate measures to ensure the security of processing

j) The Data Processor will only engage sub-processors with the prior consent of the Data Controller and under a written contract

k) The Data Processor will assist The Data Controller in providing the subject access and allowing data subjects to exercise their rights under the GDPR

l) The Data Processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data braches and data protection impact assessments

m) The Data Processor will delete or return all personal data to the Data Controller as requested at the end of the contract; and

n) The Data Processor will submit to audits and inspection, provide the Data Controller with whatever information they need to ensure that they are both meeting their Article 28 obligations, and tell the Data Controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state

5. Applicable Law

The parties to this Agreement shall be subject to English law.

6. Rights of Data Subjects

The Data Processor shall notify the Data Controller within 2 working days if it receives a request from a Data Subject for access to that person's Personal Data. The Data Processor shall provide the Data Controller with full co-operation and assistance in relation to any request made by a Data Subject to have access to Personal Data. The Data Processor shall not disclose the Personal Data to any Data Subject or to a third party other than at the request of the Data Controller or as provided for in this Agreement.

7. Suspension of Contract

This agreement can be suspended for 45 working days, if security has been seriously breached. This should be detailed in writing and be evidenced by the Data Processor to the Data Controller. Any suspension will be subject to a risk assessment and a resolution meeting between nominated representatives of the Data Processor and the Data Controller being held. This meeting will take place within 14 working days of the written identification of any breach. The suspension may be lifted when the cause of the breach has been satisfactorily investigated and appropriate measures have been taken to address and resolve the situation. Any such suspension is to be without prejudice to the parties other rights under this Agreement and the Contract.

8. Indemnity

Each party will keep the other indemnified against all reasonable costs, expenses and claims arising out of any breach of this Agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending party, employees, agents or any other person within the control of the offending partner of any data obtained in connection with this Agreement. Such indemnity extends to any sanction imposed by the Information Commissioners Office under its statutory powers.

9. Duration

This Agreement shall commence on its date of signing referred to at point 12 below and shall continue for the duration of the Contract, including any extension given under it, subject to the parties' rights of termination below and in the Contract. It shall automatically terminate on completion or termination of the Contract.

10. Consequences of Termination of the Contract

Either party shall have the right to terminate this Agreement in the event that the Contract is terminated in accordance with the provisions contained.

Either party may terminate this Agreement with immediate effect by giving written notice to the other party in the event that the other party commits a material breach of any term of this Agreement and (if that breach is capable of remedy) fails to remedy that breach within a period of 30 days after being notified to do so

In the event of termination, the Data Processor shall immediately and securely return or transfer, all data in its possession or control provided under this Agreement to the Data Controller, and shall certify in writing that it has done so within 7 days of the transfer, unless this is prohibited by

the national law or regulator of the country in which the Data Processor processes the data. Where this is the case, to the extent allowed under such requirements, the data will be kept confidential and will no longer be processed.

11. Entire Agreement

For the purpose of this Agreement the parties acknowledge that this Agreement and its Schedules represent the entire agreement between the parties relating to the data processing part of the Contract that this Agreement supports.

12. This Agreement is effective from the latest FCHA approved signatory date below for the duration of the Contract it supports

SIGNATORIES:

This Agreement was signed on the date shown below.

Date: _____

FCHA
Authorised signatory

_____ Date: _____

[NAME OF CONSULTANT/CONTRACTOR
Authorised Signatory

SCHEDULES

SCHEDULE A

Data Controller:

FIRST CHOICE HOUSING ASSOCIATION LIMITED
AVON HOUSE , 19 STANWELL ROAD,
PENARTH
CF64 2EZ

Information Commissioner's Office Registration Number: **Z464170X**

Name	Title	Description of Role	Contact Details

Data Processor:

[insert supplier name and address]

[E-MAIL ADDRESS]

Information Commissioner's Office Registration Number: **: [INSERT THE ORGANISATION'S ICO REGISTRATION NUMBER or provide an explanation as to why the organisation has not registered as a Data Controller with the Information Commissioner's Office]**

Name	Title	Description of Role	Contact Details

N.B. If unsure whether organisation is required to register please check on the Information Commissioner's Office website https://ico.org.uk/for-organisations/register/self-assessment/

SCHEDULE B

Purpose of Processing the Personal Data:

[insert supplier name] ("Data Processor") has been contracted by FCHA ("Data Controller") to **[define the nature and purpose of the processing]** during the period **[insert start date] until [insert end date].**

Both personal and special categories of personal data sets are to be processed and the conditions within the GDPR that support this are

1. ***Lawfulness, fairness and transparency***

2. ***Purpose limitations***

3. ***Data minimisation***

4. ***Accuracy***

5. ***Storage limitations***

6. ***Integrity and confidentiality***

Schedule 2 6 (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by third parties to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms of legitimate interests of the data subject

Schedule 3 2 (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

The data sets , (identified in Schedule D of this agreement) will be used solely for the purpose stated in this agreement

SCHEDULE C – Information Security Management Requirements

The Data Processor must be able to demonstrate their commitment to information security. This will include, but is not necessarily limited to, the following best practice requirements:

1. **Organisation of Information Security:**

    a. Documented policies demonstrating the Data Processor's commitment to the management and security of information.
    b. A named single point of contact for data protection matters.

2. **Human Resources (HR) Security**:

    a. Appropriate HR recruitment practices that include: screening and vetting of employees and, where applicable, referral to the Debarring & Vetting Service.
    b. Employment contracts, which include confidentiality statements.
    c. Information security training (and regular refresher sessions) for relevant employees.
    d. Processes to promptly manage termination or changes to roles and responsibilities, including the return of processing facilities and information assets where applicable. For example: the return of IT equipment, portable storage devices, hardcopy records, deletion of IT access rights etc.

3. **Physical & Environmental Security**:

    a. Physical security controls of buildings, offices, and facilities etc in order to protect areas where processing of the Data Controller's information will be take place.
    b. Appropriate measures to protect against damage from fire, flood, explosion, civil unrest and other forms of natural or man-made disaster.
    c. Controls in place to manage access points, (eg delivery and loading areas, reception areas), where unauthorised persons may enter the Data Processor's premises.
    d. The positioning of processing equipment to reduce the risks from environmental threats and hazards and opportunities for unauthorised access. Examples include: the encryption of portable processing equipment, such as laptops; monitors positioned to reduce the risk of being viewed by unauthorised persons; guidance to protect against 'shoulder surfing' when in public places.
    e. Applying security controls to off-site equipment and for home-working. For example: encrypted mobile devices; equipment and media not being left unattended in public places; keeping hardcopy information secure by not storing it with mobile devices; not leaving equipment or information in vehicles etc.
    f. An authorisation process for users to take the Data Controller's information out of the Data Processor's organisation. For example, approval to work from home providing adequate security controls are in place
    g. Processes to ensure devices and physical storage equipment containing sensitive information are checked to ensure that any data belonging to the Data Controller has been removed or securely overwritten/deleted prior to disposal.
    h. Processes in place for the secure return or disposal of hardcopy information belonging to the Data Controller.
    i. Prohibiting the use of cloud storage without prior authorisation from the Data Controller.

4. **Communications & Operational Procedures**:

    a. Documented operational procedures and responsibilities that are implemented and maintained, to ensure the correct and secure processing of the Data Controller's information.
    b. Appropriate contracts and monitoring processes to manage third parties, authorised by the Data Controller, to undertake any processing on the Data Processor's behalf.
    c. Undertaking privacy impact assessments when planning to introduce, amend or remove processing facilities, procedures etc., which may or will impact the processing of the Data Controller's information.
    d. Technical controls to manage computing facilities in order to maintain the integrity, availability and confidentiality of the Data Controller's information covering areas such as: system planning and acceptance; protection against malicious and mobile code; back-up; and network security management.

e. Acceptable use policies when processing the Data Controller's information to safeguard against:

    i. Interception, copying, modification, misrouting and destruction;
    ii. Malicious code that may be transmitted through the use of electronic communications;
    iii. Risks from emailing, printing, scanning, faxing or other means of transporting sensitive information;
    iv. Leaving sensitive information on voice message facilities, answering machines or being sent via text etc.

f. Appropriate controls to protect sensitive information from unauthorised access, misuse or corruption during transportation. For example, by using: authorised couriers, procedures to check the identification of couriers, information encryption; using special delivery etc.
g. Processes in place to monitor and regularly review processing activities and information security events.
h. Prompt reporting of actual breaches of physical or technological security that may or has impacted confidentiality, integrity or availability of the Data Controller's data are immediate reported to the Data Controller.
i. The Data Processor will ensure any actual breaches of the General Data Protection Regulation (GDPR)–and or the terms and conditions of this Agreement that may or has impacted the Data Controller's compliance are immediately reported

5. **Access Control**:

a. Documented physical and logical access control procedures that ensure the processing of the Data Controller's information is only undertaken by authorised personnel, covering areas such as:

    i. Registration and de-registration for granting and revoking access to buildings, information systems and services.
    ii. Promptly reporting to the Data Controller, leavers who had authorised remote access to its systems, including where the access was via a web based application.
    iii. Unique user IDs to enable users to be linked to and held responsible for their actions.
    iv. Password/cryptographic management standards.
    v. The secure allocation and maintenance of passwords.
    vi. Clear desk requirements for papers and removable storage media.
    vii. Inactive computer sessions shutting down after a defined period of inactivity.

6. Management of Information Security Incidents & Improvements

a. Responsibilities and procedures to handle security events and weaknesses effectively are documented and maintained.
b. Processes to comply with the Data Controller's requirements for reporting information security events that have, or may impact, the Data Controller's information.
c. Arrangements to ensure business continuity in the event of major failures to information systems or disasters.

7. Compliance with Legal Requirements

a. Appropriate policies and procedures to ensure:

    i. Compliance with legislation and regulatory requirements that the Data Controller is subject to, in relation to the processing of its information.
    ii. Ensuring the Data Controller's information is protected from loss, damage, destruction and falsification, in accordance with statutory, regulatory (including codes of practice), contractual and business requirements, which includes, but is not limited to:

        1. The Freedom of Information Act 2000

2. General Data Protection Regulation (GDPR)
3. The Environmental Information Regulations 2000

b. Freedom of Information Act 2000

i. The Data Processor acknowledges that the Data Controller may have legal responsibilities to make information available under the Freedom of Information Act 2000.

ii. The Data Processor shall give reasonable assistance to the FCHA Data Controller to comply with the Act.

iii. In particular, the Data Processor shall supply all such information and records (together with reasonable assistance to locate the same) which are needed by the Data Controller to comply with its obligations under the Act in a timely and consistent manner.

iv. The Data Processor acknowledges that the Data Controller shall have the discretion to disclose any information which is the subject of either the Contract or this Agreement to any person who makes a request under the Act and which in the opinion of the Data Controller it has to disclose to discharge its responsibilities under the Act.

v. When exercising its rights under the Act the Data Controller shall consult with the Data Processor and may take account of any reasonably suggestions made by it. The Data Controller shall have regard to use of the exemptions referred to in the Act, and shall apply those which it considers relevant and reasonable in the interests of maintaining commercial confidentiality and/or other valid reasons for exemption from disclosure of requested information

vi. The Data Controller shall not be responsible for any loss damage harm or detriment sustained by the Data Processor, however caused, arising from disclosure of information relating to this Agreement where it has been required by law to disclose that information.

SCHEDULE D-Data sets Covered by this Agreement

[INSERT LIST OF DATA SETS eg, name, address, post code, dob etc, information systems that will be accessed remotely (if applicable) including web based applications]

1.

2.

3.

4.

5.

6.

7.

8.

9.

10.