The BCHA Group

Data Protection Policy

SUBJECT: Data Protection Policy	**Policy No:** 900	**HCA Regulatory Code:** QAF
SECTIONS: All Departments	**Draft Issued:** 20th April 2018 **Approved:** 24th April 2018	
REVIEWED BY: Strategy & Governance Department	**Effective Date:** 15th May 2018	**Review Date:** 15th May 2019

CONTENTS

Go to contents

Go to contents

1.0 Policy Statement

1.1 Bournemouth Churches Housing Association (BCHA) collects personal information to effectively carry out its everyday business functions and activities and to provide the services connected with its mission. Such data is collected from employees, customers and suppliers and includes (but is not limited to), names, addresses, email addresses, dates of birth as well as other information such as health and social care data. In addition, BCHA may be required to collect and use certain types of personal information to comply with the requirements of law and/or regulation.

1.2 BCHA is committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR), UK data protection laws and any other relevant the data protection laws and codes of conduct (referred to in this policy as **"data protection law"**).

1.3 This policy supports compliance with data protection law through five key objectives (see section 5). It is concerned with the storage and processing of all personal information help by the organisation and the fair and lawful processing of that data. This policy recognises that personal information is confidential and loss or unauthorised access or disclosure is unlawful and a serious matter.

2.0 Purpose

2.1 The purpose of this policy is to ensure that BCHA meets its legal, statutory and regulatory requirements under data protection law and to ensure that all personal and special category information is processed compliantly and in data subjects' best interests.

3.0 Scope

3.1 This policy applies to all staff within BCHA (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with BCHA in the UK or overseas). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3.2 For the purposes of this policy, "BCHA" will be taken to mean BCHA and/or its subsidiaries and "Organisation means BCHA and/or its subsidiaries.

3.1 Definitions

3.1.1 **"Biometric data"** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

3.1.2 **"Binding Corporate Rules"** means personal data protection policies which are adhered to by BCHA for transfers of personal data to a controller or processor in one or more third countries or to an international organisation.

3.1.3 **"Consent"** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

3.1.4 **"Cross Border Processing"** means processing of personal data which:

- takes place in more than one Member State of the EU; or
- which substantially affects or is likely to affect data subjects in more than one Member State of the EU.

3.1.5 **"Data controller"** means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by UK or EU Member State law, the controller or the specific criteria for its nomination may be provided for by UK or EU Member State law.

3.1.6 **"Data processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

3.1.7 **"Data protection law"** means for the purposes of this document, the collective description of the GDPR, Data Protection legislation and any other relevant laws that BCHA must comply with.

3.1.8 **"Data subject"** means an individual who is the subject of personal data and who may be identifiable by that data.

3.1.9 **"GDPR"** means the General Data Protection Regulation (EU) (2016/679).

3.1.10 **"Genetic data"** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

3.1.11 **"Personal data"** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.1.12 **"Processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as:

- Collection
- Recording
- Organisation

Go to contents

- Structuring
- Storage
- Adaptation or alteration
- Retrieval
- Consultation
- Use
- Disclosure by transmission
- Dissemination (or otherwise making available)
- Alignment or combination
- Restriction
- Erasure or destruction

3.1.13 **"Profiling"** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

3.1.14 **"Recipient"** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with UK or EU Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

3.1.15 **"Supervisory Authority"** means an independent public authority which is established by a Member State of the EU. In the UK, this is the Information Commissioner's Office (ICO).

3.1.16 **"Third Party"** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

4.0 Data Protection Context

4.1 UK Data Protection Law & the GDPR

4.1.1 The General Data Protection Regulation (GDPR) applies to all EU Member States from 25th May 2018. The Data Protection Act 2018 implements the GDPR into UK law together with any clarifying or additional provisions.

4.2 The Information Commissioner's Office (ICO)

4.2.1 The Information Commissioners Office (ICO) is an independent regulator which reports directly to Parliament and whose role it is to uphold information rights in the public interest. The legislation it has oversight of includes:

- General Data Protection Regulation and Data Protection Act 2018
- The Privacy and Electronic Communication Regulations 2003
- Freedom of Information Act 2000

Go to contents

- The Environmental Information Regulations 2004

4.2.2 BCHA is registered with ICO and appears on the Data Protection Register as a controller of personal information. BCHA's Data Protection Registration Number is **Z5985815**.

4.3 The GDPR Principles

4.3.1 The GDPR has 7 main principles regarding processing personal data as follows:

1) **Lawful, fair and transparent:** Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2) **Purpose limitation:** Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3) **Data minimisation:** Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4) **Accuracy:** Data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5) **Storage limitation:** Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods if the personal data is to be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

6) **Integrity and confidentiality:** Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7) **Accountability:** Data controllers must show how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

4.4 Types of Personal Data

4.4.1 **Personal data** is defined within section 3.1.

Go to contents

4.4.2 **Special category data** relates to personal data which is more sensitive than personal data and needs more protection so as not to put data subjects at risk, for example unlawful discrimination. This type of data will include:

> "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

4.4.3 **Criminal Offence Data** relates to personal information about criminal convictions or offences.

4.4.4 Processing special category data and criminal offence data requires organisations to identify specific legal basis in addition to the processing of personal data.

5.0 Objectives

5.1 BCHA is committed to ensuring that all personal data processed by the organisation is done so in accordance with data protection law and its principles, along with other associated regulations and codes of conduct issued by the ICO or other relevant body. BCHA will ensure the safe, secure, ethical and transparent processing of all personal data, using appropriate measures to enable data subjects to exercise their rights.

5.2 BCHA has developed **5 objectives** to meet its data protection obligations and to ensure continued compliance with its legal and regulatory obligations:

1) **Protect the rights of the individual**:
   i. BCHA will protect the rights of individuals with regards to the processing of their personal information.
   ii. Personal data will only be processed when the lawfulness of processing requirements have been met.
   iii. BCHA will only process special category data in accordance with Data Protection law.

2) **Develop and adhere to a comprehensive set of Data Protection policies, procedures and audit plans:**
   i. BCHA will develop, implement and maintain a data protection policy and supporting policies and procedures to comply with data protection law.
   ii. BCHA will develop and document appropriate technical and organisational measures and controls for personal data security.

3) **Regularly monitor data protection matters in the organisation:**
   i. All business functions and processes carried out by BCHA will be monitored for compliance with data protection laws periodically.
   ii. BCHA will monitor, review and identify gaps in compliance before they become a risk, implementing mitigating actions where necessary.

Go to contents

4) **Train staff and establish clear reporting lines:**
   i. All staff will be competent and knowledgeable about their obligations and will be provided with training in data protection law and principles, how these apply to their specific role and BCHA overall and how to escalate concerns or incidents as a matter of urgency.
   ii. Staff will be made aware of their own rights under data protection law and will be provided with the Article 13/14 information disclosures in the form of a Privacy Notice.

5) **Develop and maintain relevant data protection registers:**
   i. BCHA will maintain the following registers: Data Processing, Subject Right Requests, Privacy Notices and Data Breaches.

6.0 Governance

6.1 Accountability & Compliance

6.1.1 The Board of BCHA has ultimately responsibility for compliance with data protection law and the Audit, Risk and Treasury Committee will exercise an oversight role within the organisation on behalf of the Board but reporting matters to the Board, as required.

6.1.2 BCHA will implement adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with data protection law which will be reviewed from time to time.

6.1.3 All managers will be accountable for ensuring ongoing adherence to this policy in their areas at all times.

6.2 Data Protection Officer

6.2.1 Under the GDPR, A **Data Protection Officer (DPO)** must be appointed where:

1) The processing is carried out by a public authority or body (except for courts acting in their judicial capacity)
2) the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
3) the core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

6.2.2 BCHA will appoint a DPO in accordance with point 3 above (see 6.2.1). BCHA will ensure that the DPO has sufficient competence, authority, support and resource to perform the role. For the DPO duties and responsibilities, please refer to our **DPO Responsibilities Policy.**

6.3 Privacy by Design

6.3.1 BCHA will operate a **'Privacy by Design' approach** with the aim of mitigating risks associated with processing personal data through its processes, systems and

activities. BCHA will develop controls and measures (detailed below) as part of this approach.

6.3.2 Data Minimisation

Under the GDPR, data should be **'limited to what is necessary'**. BCHA will only ever obtain, store, process and share the data that is essential for carrying out our services and meeting our legal obligations, and will only retain data for as long as is necessary. Measures to ensure that only the necessary data is collected include:

- Electronic collection (i.e. forms, website, surveys etc.) should only have the fields that are relevant to the purpose of collection and subsequent processing. 'Optional' fields should not be included, as optional denotes that it is not necessary to obtain.
- Physical collection (i.e. face-to-face, telephone etc.) should be supported using internal forms where the required data collection is ascertained using predefined fields. Again, only relevant and necessary data should be collected.
- Service Level Agreements or other bespoke agreements should be in place with third-party controllers who send BCHA personal information (either in our capacity as a controller or processor). These will state that only relevant and necessary data is to be provided.

6.3.3 Pseudonymisation

BCHA will utilise pseudonymisation where appropriate to record and store personal data in a way that ensures it can no longer be attributed to a specific data subject without the use of separate, additional information (personal identifiers).

6.3.4 Encryption

BCHA will utilise encryption as a further risk control measure for securing the personal data that is held. Encryption with a secret key is used to make data indecipherable unless decryption is carried out using the assigned key. BCHA will utilise encryption for transferring personal data to any external party.

6.3.5 Restriction

Selected personal and special category data within BCHA's file structure will be restricted by the DPO and IT manager to ensure that only relevant staff can access the data.

6.3.6 Hard Copy Data

Holding hard copy data presents unique risks in regards to data protection. BCHA will seek to minimise the information it holds as follows:

1) **Collection:**
   BCHA will assess whether it is necessary to collect hard copies of the data in question, and will prioritise digital collection techniques where possible.

2) **Storage:**
   BCHA will ensure that appropriate technical and organisational measures and controls are put in place to protect hard copy data, if collected.

3) **Transmission:**
The secure transmission of hard copy data will be the responsibility of the relevant line manager. When transmitting significant amounts of hard copy data, line managers will work with the DPO.

6.5 Legal Basis for Processing

6.5.1 All of BCHA's personal data processing activities will comply with the GDPR's requirements of lawful processing. BCHA will only carrying out personal data processing activity once an appropriate legal basis for doing so has been identified and established. Under the GDPR, there are **6 stand-alone legal bases for data processing data**:

1) **Consent:** The data subject has given consent to the processing of their personal data for one or more specific purposes.

2) **Contract:** Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

3) **Legal obligation:** Processing is necessary for compliance with a legal obligation to which BCHA is subject.

4) **Vital interest:** Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

5) **Public interest:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in BCHA.

6) **Legitimate interest:** Processing is necessary for the purposes of the legitimate interests pursued by BCHA or by a third party (*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data)*

6.5.2 The legal basis identified and established for each activity of data processing will be documented on the **Processing Activities Register** and in BCHA's Privacy Notices. The legal basis may also be provided to the data subject and ICO due to information disclosure obligations.

6.6 Processing With Consent

6.6.1 Where processing is based on consent:

- Consent requests/forms use plain language and are easy to understand.
- Consent is separate from the other matters and is not a precondition of any service (unless necessary for that service).
- Details will be provided of any third party who will use or rely on the consent.
- Consent is documented, signed, dated and retained on file in each case.
- Withdrawing consent is as easy, clear and straightforward and is available through multiple options, including:
    - Opt-out links in mailings or electronic communications.

Go to contents

  - Opt-out process explanation on website and written communications.
  - Ability to opt-out verbally, in writing or by email.
- For special category data, consent obtained is explicit (stated clearly and in detail, leaving no room for confusion or doubt) with the processing purpose(s) always being specified.

6.6.2 **Child's Consent**

Where processing is based on consent AND the personal data relates to a child who is **below the age of 13 years**, such processing is only carried out by BCHA where consent has been obtained by the holder of parental responsibility over the child.

BCHA will put mechanisms in place to verify the age of any child prior to obtaining consent, and ensure that consent is gained from a parent or guardian. BCHA will review such consents periodically to ensure consent is moved from the parent or guardian to the data subject after the age of 13.

6.7 Processing On Legitimate Interests

6.7.1 Relying on legitimate interests as the grounds for processing personal data is only lawful when such processing is **necessary,** and any controller interests are **not outweighed** by the rights and freedoms of the individual. Legitimate interests cannot be relied upon by public authorities in the performance of their tasks.

6.7.2 The GDPR mandates the documenting of any legitimate interests' assessment and decision; as well recording in the privacy notice any legitimate interests pursued by the controller or by a third party where processing on this legal basis.

6.7.3 Please refer to BCHA's **Legitimate Interests Policy** and **Legitimate Interests Assessment Form** for further guidance on using this legal basis for processing.

6.8 Processing Special Category Data

6.8.1 Where BCHA processes personal information classed as special category data or information relating to criminal convictions, we will do so in accordance with Article 9 and 10 of the GDPR and in compliance with the Data Protection Act 2018 Schedule 1 Parts 1, 2, 3 & 4.

6.8.2 In addition to processing using one of the legal bases described in section 6.5, one of the following conditions must also be met:

- The data subject has given explicit **consent** to the processing
- Processing is necessary in exercising specific rights of the controller or of the data subject in the field of **employment/social security/social protection law**
- Processing is necessary to protect the **vital interests** of the data subject where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its **legitimate activities** by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing relates to personal data which are manifestly made **public** by the data subject

Go to contents

- Processing is necessary for the establishment, exercise or defence of **legal** claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial **public interest**
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of **health or social care or treatment** or the management of health or social care systems and services
- Processing is in the **public interest** in the area of public health
- Processing is necessary for **archiving purposes** in the public interest, scientific or historical research purposes or statistical purposes.

6.9 Processing Personal Data Not Obtained from the Data Subject

6.9.1 Where personal data that has **not been obtained directly from the data subject** is to be processed, BCHA will ensure that the information contained in Article 14 of the GDPR are provided to the data subject within 28 days of our obtaining the personal data. This prescribed information will be contained within the relevant Privacy Notice.

6.9.2 BCHA reserve the right not to provide the data subject with the information if:

- they already have a copy of the relevant Privacy Notice
- the provision of such information proves impossible and/or would involve a disproportionate effort.
- obtaining or disclosure is expressly laid down in UK law to which BCHA is subject and which provides appropriate measures to protect the data subject's legitimate interest.
- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by UK law, including a statutory obligation of secrecy.

6.10 Third-Party Processors

6.10.1 BCHA reserves the right to utilise external organisations for certain data processing activities ("third party processors"). Services for which third party processors may be used include:

- IT Systems and Services
- Legal Services
- Debt Collection Services
- Human Resources
- Payroll
- Hosting or Email Servers
- Direct Marketing/Mailing Services

6.10.2 The protection of data subjects' rights and the security of their personal information is a key priority when choosing a third party processor.

6.10.3 Third party processors will be selected to process personal data on behalf of BCHA subject to:

Go to contents

- **Appropriate due diligence** – the organisation is bona fide and solvent
- **Assessment of capability** – the organisation has data security policies, systems and expertise/accreditations to be able to undertake the required processing
- **Agreement between parties** – processing is subject to a written contract which includes appropriate clauses on data security or a data processing agreement supplemental to the contract will be drawn up outlining the responsibilities of the processor.

6.10.4 Third party processors' performance will be subject to periodic contract monitoring by BCHA.

6.10.5 Under no circumstances will third party processors engage another processor without prior specific authorisation from BCHA, and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

6.10.6 Third Party processors will be required to inform BCHA immediately of any data breaches, non-compliance or inability to carry out their duties as detailed in their contract.

6.10.7 Where necessary, third party processors will be asked to sign a **Data Processor Agreement**, which will be logged on BCHA's **Processor Agreements Register**. This will be at the discretion of the Data Protection Officer.

6.11 Record of Processing Activities

6.11.1 As an organisation with more than 250 employees, BCHA will maintain a register of all processing activities readily available for officers, auditors or the Supervisory Authority upon request. The legal basis identified and established for each activity of data processing will be documented on the **Processing Activities Register** and in BCHA's Privacy Notices. The legal basis may also be provided to the data subject and ICO due to information disclosure obligations.

6.11.2 Acting in the capacity as a controller, BCHA's internal records of processing activities carried out under our responsibility, contain the following information:

- The purposes of the processing
- A description of the categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data has or will be disclosed
- Where applicable, transfers of personal data to a third country or an international organisation
- The envisaged time limits for erasure of the different categories of data
- A general description of the processing security measures

6.11.3 Similarly, in instances where BCHA acts in the capacity as a processor, its internal records of the categories of processing activities carried out on behalf of a controller, contain the following information:

- Details of each controller
- The categories of processing carried out on behalf of each controller
- Where applicable, transfers of personal data to a third country or an international organisation
- A general description of the processing security measures

6.11.4 Where BCHA are processing special category or criminal conviction data, the following will also recorded on the register:

- Which condition is relied on as specified in Sch.1, Pt.1-3 of the Data Protection Act 2018 is being relied upon
- How the processing satisfies Article 6 of the Data Protection law

6.12 Data Retention & Erasure

6.12.1 BCHA will introduce specific procedures and retention periods in order to adhere to the legal requirement to hold and process personal information only for as long as is necessary.

6.12.2 Personal data for which ready access is no longer required (e.g. upon a customer leaving a service) will be properly archived for defined periods. This is important in case of return by a customer to the service or to assist statutory enquiries, for example.

6.12.3 All personal data will be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and prioritises the protection of the personal data.

6.12.4 Refer to BCHA's **Data Retention & Disposal Policy** and BCHA's **Right to Restriction, Objection and Erasure Procedure** for full details on retention, storage, periods and destruction procedures.

6.12.5 For closure of offices, there may be significant amounts of personal data to protect of destroy. Refer to **Office Closure Guidance** on the Intranet.

6.13 System Administrators

6.13.1 System administrators who have complete access to the IT system have a particular responsibility towards system integrity and confidentiality when undertaking their duties given the higher risk to personal data these duties can pose. System administrators are responsible for ensuring appropriate and fit for purpose measures are implemented and maintained to protect the IT system from unauthorised access and ensure robust data security at all times. Any risks or incidents must be reported to the IT Manager and Assistant Director of Finance & IT without delay and agreed measures must be introduced as soon as possible to minimise any risks.

7.0 Data Protection Impact Assessments (DPIA)

7.1 BCHA will ensure that the privacy and confidentiality of personal data collected by the organisation will be upheld and respected whilst being stored and processed. Where

processing is likely to be high risk or cause significant impact to a data subject, BCHA will utilise proportionate methods to map out and assess the risks.

7.2 Where BCHA is considering carrying out processing that utilises new technologies, or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, BCHA will carry out a Data Protection Impact Assessment (DPIA).

7.3 Carrying out DPIAs will enable BCHA to identify the most effective way to comply with its data protection obligations and ensure the highest level of data privacy when processing.

7.4 Refer to BCHA's **DPIA Policy** and **DPIA Form** for further details.

8.0 Data Subject Rights

8.1 The Right to Be Informed & Privacy Notices

8.1.1 Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

8.1.2 BCHA will utilise a Privacy Notice to provide individuals with all the necessary and legal information about how, why and when BCHA process their data, along with their rights and obligations.

8.1.3 Privacy Notices may be used in the form of a document, form, webpage or pop-up, and will be easily accessible, legible and jargon-free. A link to the Privacy Notice will be put on our website and can be provided a physical or digital copy of the Privacy Notice upon request.

8.1.4 The responsibility for signing off and reviewing Privacy Notices rests with the Data Protection Officer. All privacy notices will be recorded on BCHA's **Privacy Notices Register**.

8.2 The Right of Access & Subject Access Requests

8.2.1 Under certain criteria, individuals have the right to access their personal data and supplementary information.

8.2.2 If a data subject asks BCHA to confirm whether it holds and processes personal data concerning that individual, and requests access to such data, BCHA will initially verify the identity of the individual, and assess whether there is sufficient reason to fulfil the request. If the identity of the data subject is confirmed, and the reasoning is appropriate, BCHA will respond via a **Subject Access Request (SAR):**

- BCHA will inform customers of data held about them in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- Subject Access Requests will be completed within 28 days and are provided free of charge. Where the individual makes the request by electronic means,

BCHA will provide the information in a commonly used electronic format, unless an alternative format is requested.

- If the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.
- If BCHA do not comply with a request for data provision, the data subject is informed within 28 days of the reason(s) for the refusal and of their right to lodge a complaint with the ICO.

8.2.3 Subject Access Requests must be passed to the DPO as soon as received and a record of the request will be noted and actioned by the DPO. The request will be recorded on BCHA's **Subject Access & Individual Rights Requests Register**.

8.2.4 Please refer to BCHA's **Right to Access and Rectification Procedure** and BCHA's **Customer Data Request Form** for the further guidelines on how an SAR can be made and how BCHA administers them.

8.3 The Right to Data Portability

8.3.1 Under certain criteria, individuals have the right to obtain and reuse their personal data for their own purposes across different services.

8.3.2 BCHA will provide certain personal information about the data subject to them on request, provided the data subject's identity can be verified and the request meets the requirements of the data protection laws. The DPO will oversee and be responsible for the whole process. Data will be transmitted in a usable and machine-readable format that is easy to disclose and read. In most cases, BCHA will utilise the following formats for the machine-readable data: HTML and CSV.

8.3.3 All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. If the personal data relates to more individuals than the subject requesting the data, this is always without prejudice to the rights and freedoms of the other data subjects.

8.3.4 BCHA will aim to transmit the personal data directly from BCHA to a designated controller, where technically feasible.

8.3.5 All information provided to the data subject are done so free of charge and within 28 days of the request being received. If for any reason this is not possible, BCHA will respond to the data subject with a full explanation within 28 days, outlining the reasons for refusal and of their right to complain to the ICO and to a judicial remedy.

8.4 The Right of Rectification

8.4.1 Under certain criteria, individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.

8.4.2 **Correcting Inaccurate or Incomplete Data**

Where inconsistencies are identified and where the data subject inform us that the data we hold is inaccurate (for example a date of birth), BCHA will take steps to ensure that such inaccuracies are corrected with immediate effect, following any directions from the data subject.

In case of significant error, the DPO will be notified of the data subject's request to amend personal data, and will ensure the appropriate action is taken to rectify the error. Once amended, the DPO will add a statement of actions taken where applicable.

Where notified of inaccurate data by the data subject, BCHA will rectify the error within 28 days and will inform any third party of the rectification if BCHA has disclosed the personal data in question to them. The data subject will be informed of the correction and where applicable, will be provided with the details of any third-party to whom the data has been disclosed.

If for any reason BCHA are unable to act in response to a request for rectification or completion, BCHA will provide a full explanation to the individual within 28 days, and inform them of their right to complain to the ICO or seek legal action.

8.4.3 All requests be passed to the DPO will be recorded on BCHA's **Subject Access & Individual Rights Requests Register**.

8.4.4 Please refer to BCHA's **Right to Access and Rectification Procedure** for the further details.

8.5 The Right of Erasure

8.5.1 Under certain criteria, individuals have the right to request erasure of their personal data (sometimes known as the "right to be forgotten").

8.5.2 **Data Erasure**
BCHA will ensure that personal data which identifies a data subject is kept no longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by BCHA will be categorised when assessed by the information audit and will be either given an erasure date or will be monitored so that it can be destroyed when no longer necessary.

8.5.3 All requests be passed to the DPO will be recorded on BCHA's **Subject Access & Individual Rights Requests Register**.

8.5.4 Please refer to **BCHA's Data Retention & Disposal Policy** or **BCHA's Right of Restriction, Objection and Erasure Procedure** for more details.

8.6 The Right to Restrict Processing

8.6.1 Under certain criteria, individuals have the right to request the restriction or suppression of their personal data.

8.6.2 BCHA will apply restrictions to data processing in the following circumstances:

- Where an individual contests the accuracy of the personal data and BCHA is verifying the accuracy of the personal data and/or making corrections.
- Where an individual has objected to the processing (*where it was necessary for the performance of a public interest task or purpose of legitimate interests*), and BCHA is considering whether we have legitimate grounds to override those of the individual.
- When processing is deemed to have been unlawful, but the data subject requests restriction as opposed to erasure.
- Where BCHA no longer needs the personal data, but the data subject requires the data to establish, exercise or defend a legal claim.

8.6.3 Any restricted data will be removed from the normal flow of information and will be recorded as being restricted. Except from storing the data, restricted data will not be processed in any way.

8.6.4 The DPO will review and authorise all restriction requests and actions, and will retain copies of notifications from and to data subjects and relevant third-parties. Where data is restricted, and BCHA intend to disclose such data to a third-party, BCHA will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

8.6.5 Data subjects who have requested restriction of data will be informed within 28 days of the restriction application, and will be advised of any third-party to whom the data has been disclosed. BCHA will also inform the data subject of any decision to lift a restriction on processing. If for any reason, BCHA are unable to act in response to a request for restriction, BCHA will provide a full explanation to the individual within 28 days, and inform them of their right to complain to the ICO and legal action.

8.6.6 All requests be passed to the DPO will be recorded on BCHA's **Subject Access & Individual Rights Requests Register**.

8.6.7 Please refer to BCHA's **Right of Restriction, Objection and Erasure Procedure** for more details.

8.7 The Right to Object & Automated Decision Making

8.7.1 Under certain criteria, individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

8.7.2 **Automated Decision Making**
Data protection law regarding automated decision making does not currently apply to BCHA's activities.

If in any future circumstance, BCHA uses automated decision-making processes, BCHA will inform the individual and advise them of their rights. BCHA will also ensure

that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

8.7.3 All requests be passed to the DPO will be recorded on BCHA's **Subject Access & Individual Rights Requests Register**.

8.7.4 Please refer to BCHA's **Right of Restriction, Objection and Erasure Procedure** for more details.

9.0 Security & Breach Management

9.1 Alongside BCHA's 'Privacy by Design' approach to protecting data, BCHA will ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. BCHA's **Information Security Policy** provides the measures and controls that will be taken to protect personal information and to ensure its security while used within the organisation.

9.2 Whilst every effort and measure will be taken to reduce the risk of data breaches, BCHA will respond to any concerns or incidents reported in a prompt and with utmost seriousness, and will abide by its legal obligations to make notifications to the ICO, relevant service commissioners and data subjects (where applicable). All data breaches will be recorded on BCHA's **Data Breaches Register**.

9.3 Any staff member who is aware of a data protection concern or incident must report this without delay to their line management and the DPO for investigation. The Whistleblowing Policy may also be used where direct reporting is not possible.

9.4 BCHA will fully cooperate with any ICO investigation and seek to implement any resulting findings, recommendations or requirements.

9.5 Refer to our **Data Breach Policy & Procedures** for further information.

10.0 Data Sharing & Transfers

10.1 Data Sharing Internally

10.1.1 Sharing of personal data within the organisation must be undertaken appropriately and not disclosed carelessly or without a legitimate "need to know". For example, staff data will ordinarily be accessible to Human Resources, line managers and the staff members concerned. No-one else within the Organisation has an automatic right to see confidential staff information.

10.1.2 In general, board reports will never contain personal information and any references to staff or customers will be anonymised. On occasions, this rule may need to be waived if disclosure of data is required to enable the board to fulfil its duties. In these instances, board members must not keep records of personal information they are shown and reports on Board Packs and minutes will be anonymised.

10.1.3 It is expected that staff within a service delivery team will share personal data relating to the customers of that service (and this may need to include relief staff, placements and others working, training or volunteering at the service). However, care must be taken to avoid:

- displaying confidential information which customers or visitors may be able to see
- recording personal data (particularly "special category" data) in general records such as daily logs
- sharing of passwords or other system access keys
- weak physical security for staff convenience
- Printing off or photocopying personal information unnecessarily

10.1.4 Data sharing outside the team environment (but still within the organisation) will be permitted to:

- Facilitate internal audit, monitoring or review
- Facilitate the delivery of corporate services
- Ensure consistency and progression of support when a customer transfers from one BCHA service to another
- Reduce risk of harm

10.2 Data Sharing with External Agencies

10.2.1 Statutory bodies include local authorities, housing benefit departments, social services, the police and health authorities. Non-statutory bodies include banks and telephone companies.

10.2.2 The organisation can disclose **personal data** to third parties where a customer has given their written consent although in certain circumstances the organisation may be able to disclose information without the customers' consent (see 10.4 below). Before disclosing information, staff should ascertain:

- That the request is actually from the organisation making the request
- The identity of the person making the request
- That the request is reasonable, proportionate and relevant

10.2.3 Each time a request is made for information about an individual, a record must be kept of the name of the person and agency who requested the information and reason for the request and whether the information was given. All stages of the request must be recorded.

10.2.4 Personal Information can only be shared with statutory agencies or their authorised agents, **without the consent** of the individual:

- To comply with the law in the prevention or detection of fraud or crime or in connection with legal proceedings (e.g. requests from the Police)
- For tax purposes required by law (e.g. Inland Revenue/Council tax)
- Where there is a clear Health and Safety risk (for example where withholding information might cause a risk to the health and safety of staff,

Go to contents

members of the public etc. or where there is a possibility of self-neglect or serious deterioration in the health or well-being of an individual).

- Where disclosure is a child or vulnerable adult protection matter
- In connection with court proceedings or statutory action to enforce compliance with tenancy conditions (e.g. applications for possession or payment of housing benefit direct)
- Where it is a specific requirement of a service contract with a statutory body

10.2.5 Personal Information can only be shared with non-statutory agencies **without the consent** of the individual:

- When a request has been made for information about a customer being evicted, then relevant factual details only may be given
- To enable contractors or agents to deliver services on behalf of the organisation (the handling of this information must be governed by contract or other written terms)
- To confirm the name of a customer/date of occupancy with gas, electricity, water companies etc.
- Anonymously for bona fide statistical, research or publicity purposes – provided doing so would not identify the individual concerned

10.2.6 In the case of regulators such as Commissioning Bodies or the Regulator Social for Housing, access to Personal Information may only be provided with the written consent of the individual unless an exemption in 10.4 applies (i.e. a statutory or criminal investigation). Organisations requesting must make clear what information they wish to see and this must be assessed against Data Protection law.

10.2.7 The Organisation cannot disclose forwarding addresses to third parties without consent (except in the circumstances outlined in section 10.4). Instead, staff should offer to contact the individual concerned on behalf of the enquirer or forward information to them from the enquirer.

10.2.8 **Statistical Monitoring**
Staff should ensure internal or external statistical reports are appropriately anonymised. Removal of someone's name will not necessarily be sufficient - for example data relating to staffing at a lone working scheme can still identify the person concerned.

10.3 Data Sharing Protocols

10.3.1 BCHA is committed to working in partnership with statutory and other agencies to facilitate effective service delivery to individuals and the wider community. BCHA will actively seek to participate in formal multi-agency Information Sharing Protocols although participation in such arrangements must not conflict with the Organisation's duties under the Data Protection laws.

10.4 Data Transfers

10.4.1 Where data is being transferred from BCHA to another organisation or individual for a legal and necessary purpose (for example, a data processing arrangement), BCHA

will utilise a process that ensures such data is encrypted with a secret key and where possible is also subject to BCHA's data minimisation methods. Alternatively, non-electronic means such as courier may be utilised where appropriate.

10.5 International Data Transfers

10.5.1 BCHA recognises the high-risk nature of disclosing and transferring personal data, and as such, places a high priority on the protection and security of data being transferred. Data transfers within the UK and EU are deemed less of a risk than a third country or an international organisation, due to the data protection laws covering the former and the strict regulations applicable to all EU Member States.

10.5.2 The advice of the Data Protection Officer will be sought for any data transfers outside the UK.

11.0 Audits & Monitoring

11.1 From time to time, BCHA will conduct internal data audits, either directly or through a third party. The aim of internal data audits is to:

- Provide assurance of compliance with the data protection law.
- Ensure that the appropriate policies and procedures are in place, to test their adequacy and effectiveness, and verify they are being followed.
- Detect breaches or potential breaches in compliance.
- Identify risks and assess the mitigating actions in place to minimise such risks.
- Recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data.

11.2 The Data Protection Officer has overall responsibility arranging or conducting data audits and that any recommendations are acted upon.

12.0 Staff Duties & Training

12.1 BCHA will ensure that all staff understand, their duties with respect to data protection law requirements and principles, and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role.

12.2 In particular, staff must:

- Not display or disclose personal data to someone outside the organisation without the consent of the person concerned (except as outlined in Section 6.6)
- Keep personal information securely whilst in their possession and on the premises where they work (either through physical security or proper use of technology security)
- Not attempt to gain personal information they are not authorised to access

- Avoid taking confidential information away from the office in paper form (for example on visits, to meetings or home) without line manager authorisation and appropriate security agreed to protect the data. Any such information (or any information collected whilst out of the office from customer or partner agencies) must be returned to BCHA premises **without delay or be securely shredded**.
- Never download personal data to non-BCHA hardware, software or other media without proper authorisation

Failure to observe these requirements will be deemed as misconduct and will be grounds for disciplinary action.

12.3 BCHA's **Staff Development Policy** details how new and existing employees are trained, appraised and supported.

13.0 Miscellaneous Data Protection Matters

13.1 Publicity Material

13.1.1 Case studies about customers must be completely anonymised before publication. However, if it is desirable to identify an individual in publicity material or media interviews (by name, picture or biographical information), express consent must be obtained beforehand. BCHA's **Media Policy** gives further guidance.

13.1.2 BCHA will aim to ensure that use of material which identifies someone will be subject to the Right to Erasure although measures should also be put in place to time-limit the use of individual-specific material after which material should be taken down or destroyed unless the subject still explicitly consents to its use.

14.0 Responsibilities

14.1 The-appointed **Data Protection Officer (DPO)** will lead on data protection matters for the organisation and act in an advisory capacity to the business and its employees. The DPO's duties are listed in a separate statement of responsibilities.

14.2 All managers are responsible for ensuring data security measures are in place and that this policy is adhered to at all times. Managers also have a responsibility for ensuring their staff are appropriately trained in data protection matters and that this training is refreshed from time to time.

14.3 All staff have a duty to report any risks or concerns about data protection to their line manager without delay or to the Data Protection Officer. Any failure to do so will be considered a serious matter. Staff may consider raising a grievance or using the Whistleblowing Policy where they have believe that raising concerns with line management will not be effective.

14.4 Customers may make complaints at any time about concerns they have about the processing of their personal data by the organisation and these will be dealt with in accordance with the Organisation's Complaints procedure.

15.0 References

POLICY	PGN
Data Breach Policy & Procedures	901
Data Breach Incident Form	901.1
Data Retention & Disposal Policy	902
DPO Responsibilities	903
Right to Access and Rectification Procedure	904
Right to Restriction, Objection and Erasure Procedure	905
Customer Data Request Form	907
Information Security Policy	908
DPIA Policy	909
DPIA Form	909.1
Legitimate Interests Assessment Policy	917
Legitimate Interests Assessment Form	917.1
Data Processor Agreement	
Staff Development Policy	
Media Policy	

REGISTERS
Processing Activities Register
Data Breaches Register
Processor Agreements Register
Subject Access & Individual Rights Requests Register
Privacy Notices Register