DATA PROTECTION POLICY

Date Reviewed	**February 2026**	**Next Review Date**	**March 2027**
Consultation	**Data Management Panel**	**Reviewed By**	**Data & Performance Manager**
EIA	**N/A**	**Responsible Officer**	**Head of Corporate Services**
DPIA	**Complete**	**Approval By**	**Executive Team**

1. Purpose

The Data Protection Act 2018 (DPA18) and the United Kingdom General Data Protection Regulations (UK-GDPR) provide individuals with the right to know what personal and sensitive (special category) information is held about them and how it is processed and protected. It also sets out requirements for organisations to adhere to, when collecting and processing personal data.

This Data Protection Policy sets out how Black Country Housing Group (BCHG) protects the personal data it collects and processes as an organisation, in compliance with the Data Protection Act 2018; UK GDPR, and has been updated to reflect amendments introduced by the Data (Use and Access) Act 2025 (DUAA), which updated the UK-GDPR, Data Protection Act 2018 and PECR. This policy provides clear guidance on employee obligations; the Groups obligations as Data Controller; and individuals rights, in relation to their personal data.

2. Scope

This Policy applies to all personal data processed by BCHG and compliance with this policy is mandatory for all employees. Related policies, procedures and guidelines are available to help colleagues implement the Policy. Any breach of this policy and the related mandatory data protection eLearning training provided to all employees, may result in disciplinary action.

3. Definitions

'Employee' refers to all BCHG employees, including permanent, fixed term, temporary, Board Members, secondees, third party representatives, agency workers, volunteers, apprentices, and agents.

'Personal Data' is any information which relates to a living individual who can be or may be identified from that information (directly or indirectly), from that data alone or in combination with other identifiers we possess or can access for example:

- A person's name, address (postal and email) or date of birth
- A statement of fact and/or any expression/opinion communicated about an individual's actions or behaviour
- Minutes of meetings and reports which refer to an individual
- Emails, file notes, handwritten notes, sticky notes in relation to an individual
- Individual identifiable CCTV Footage
- Lettings, Sales and Employment application forms
- Care Support Plans and Housing Files
- Spreadsheets and/or databases with any list of individuals set up by code, tenancy number, NI (National Insurance) number etc. (this list is not exhaustive)

'Special Category Data' is any information relating to an individual's:

- Ethnicity
- Gender
- Religious or Other Beliefs
- Membership of a trade Union
- Sexual Orientation
- Physical or mental health conditions
- Offences committed or alleged to have been committed by that individual
- Biometric or genetic data

A **'Data Subject'** is an identified or identifiable living individual who is the subject of personal data. The provisions set out in the DPA 18, and UK GDPR do not apply to records of the deceased. Requests for personal data on deceased individuals may be covered by the Access to Health Records Act 1990. Employees should process such requests on a case-by-case basis and always consult with their manager before making a disclosure. If unsure, please consult with the Data Protection Officer (DPO).

'Data Controller' is the natural or legal person, public authority, agency, or other body which, alone or jointly determines the purposes and means of the processing of personal data. This is Black Country Housing Group in relation to the personal data of our customers and employees unless processing data as a Data Processor.

'Data Processor' is a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller. Any suppliers or agents which whom we share personal data will be Data Processor's and we may be a Data Processor on behalf of other public bodies, organisations, or partners we process personal data for.

4. Related Policies & Procedures

Data Retention and Disposal Policy
Data Protection Guidance & Procedures
Personal Data Breach Procedure
Portable Media Policy
Backup System Policy
Mobile Device Policy

Internet & Email Usage Policy	Transparency Policy (web statement)
Network Security Policy	CCTV Policy

5. Data Protection

Data Protection applies to all personal and sensitive (special category) personal data, processed and/or stored electronically[1] and manually (paper based) files.[2] It aims to protect and promote the rights of individuals, ('Data Subjects') and BCHG (the 'data controller').

Personal data may only be processed provided one of the following is met:

- The individual has given their explicit consent to the processing;
- It is necessary for the performance of a contract with the individual;
- It is required under a legal obligation;
- It is necessary to protect the vital interests of the individual;
- It is to carry out public functions; or
- It is necessary to pursue the legitimate interests of BCHG or certain third parties (unless this is prejudicial to the interests of the individual, determined by a Legitimate Interests Assessment)

Special category data may only be processed provided:

- The individual has given their explicit consent;
- The individual has already made the information public;
- It is to protect the vital interests of the individual or other individuals;
- It is necessary for the purposes of, or in connection with legal proceedings or for obtaining legal advice and for the administration of justice or any enactment, function of the Crown;
- It is for medical purposes and is undertaken by a health professional; or
- It is necessary for the purposes of exercising or performing any right or obligation as Data Controller in connection with employment.

Data Protection Principles

There are 7 Principles under the DPA18 and UK-GDPR which BCHG employees must ensure they abide by when processing personal data:

---

[1] This list is not exhaustive: Desktop PC's, Laptops, Tablets, and Mobile Phones.

[2] Manual records are paper based and structured, accessible and form part of a relevant filing system (filed by subject, reference dividers or content), where individuals can be identified, and personal data easily accessed without the need to trawl through a file.

Lawfulness, Fairness and Transparency Personal Data shall be obtained and processed fairly, lawfully and transparently.

Purpose Limitation Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data Minimisation Personal Data shall be adequate, reliant, and limited to only what is necessary for the purpose for which it is obtained.

Accuracy Personal Data shall be accurate and, where necessary, kept up to date.

Storage Limitation Personal Data shall not be kept in a form which permits identification of data subjects for longer than necessary for the purposes for which the data is processed.

Security, Integrity, and Confidentiality Personal Data (manual and electronic) must be processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Accountability Principle The Group are responsible for and must be able to demonstrate compliance with the data protection principles listed above. (Accountability)

BCHG has implemented adequate resources and controls to ensure compliance including:

- Appointing a suitably qualified Data Protection Officer (DPO) and Data Management Panel, accountable for data privacy.
- Implementing Privacy by Design when processing personal data and completing DPIAs (Data Protection Impact Assessments) where processing presents an elevated risk to rights and freedoms of Data Subjects.
- Integrating data protection into internal documents including this Policy, related Policies, privacy guidelines and Privacy Notices.
- Regularly training employees on data protection and data protection matters including, for example: Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches.
- Maintaining a record of training attendance by employees.
- Regularly testing the privacy measures implemented; and
- Conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

BCHG will ensure governance, training and DPIA processes incorporate DUAA requirements, particularly in relation to legitimate interests, research processing, automated decisions and international transfers.

All employees must follow these Principles and maintain data security by protecting the confidentiality, integrity, and availability of the personal data, defined as:

- **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users can access the personal data when they need it for authorised purposed.

Employee Obligations

Employees will not gain access to information that is not necessary to hold, know or process. All information which is held will be relevant and accurate for the purpose for which it is required, the information will not be kept for longer than necessary and will be kept secure.

Employees will ensure that all personal or special category personal information is anonymised or pseudonymised, where appropriate e.g., for equality and diversity reporting.

Employees who manage and process personal or special category personal information will ensure that it is kept secure and where necessary, confidential.

Employees are responsible for notifying their line manager or the DPO, if they believe or suspect that a conflict with this policy has occurred or may occur. This includes notification of any actual or suspected data breach.

Where employees do not comply with this policy, BCHG may also consider acting in accordance with our disciplinary processes. Where it is found that an employee has knowingly (with intent) and maliciously breached our data protection and security policies, guidance and/or the legislation, BCHG and the ICO (Information Commissioners Office) will also consider taking direct legal action against the employee, such as where a data breach has been found to have caused any actual or potential distress to our residents or employees.

Data Controller (BCHG) Obligations

BCHG will follow the Code of Practice issued by the ICO when developing policies and procedures in relation to data protection compliance.

When contracting out services, that involves the processing of personal data, to third parties ('data processors[3]') BCHG will ensure that Data Processing clauses and/or Data Sharing Agreements, where BCHG is the Data Controller, clearly outlines the roles and responsibilities of both the Data Controller and the Data Processor.

Where BCHG engages in research activities, DUAA provisions on broad consent and disproportionate effort will apply, ensuring alternative public notice is provided.

BCHG will adhere to and follow the 7 Principles of the DPA18 and UK-GDPR and the Privacy and Electronic Communications Regulations (PECR) when conducting surveys, marketing activities etc. And where the organisation collects, processes, stores, and records personal data.

BCHG will assess all international transfers under the updated DUAA rules, including any impacts arising from future adequacy decisions.

Where BCHG operates public-facing websites, we will adopt DUAA aligned cookie categorisation, allowing certain analysis/functionality cookies to be set without explicit consent where permitted.

BCHG will conduct DPIAs where processing personal data may result in a substantial risk to data subjects or where we are processing information that related to many individuals. BCHG will conduct Legitimate Interest Assessments where it considers that it relies on Legitimate Interests as defined in the DPA 18 and UK-GDPR, to process data. However, under DUAA, certain processing activities qualify as Recognised Legitimate Interests and may not require a full Legitimate Interests Assessment, for example: fraud prevention; public safety; certain marketing/security uses). BCHG will rely on these bases only where applicable and document decisions accordingly.

BCHG will ensure all staff are provided with data protection training and promote awareness of the organisation's data protection and information security policies, procedures, and processes.

Individuals ('Data Subjects') Rights

BCHG acknowledges individuals (data subjects) rights when it comes to how we handle their data.
These include rights to:

- Withdraw consent to processing at any time.

[3] 'Data Processor' in relation to personal data, means any person (other than an employee of the Data Controller) who processes data on behalf of the Data Controller.

- Receive certain information about the data controller's processing activities.
- Request access to their personal data that we hold.
- Prevent our use of their personal data for direct marketing purposes.
- Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed; or to rectify inaccurate data; or to complete incomplete data.
- Restrict processing in specific circumstances.
- Challenge processing which has been justified based on our legitimate interests or in the public interest.
- Object to decisions based solely on Automated Processing.
- Prevent processing that is likely to cause damage or distress to the data subject or anyone else.
- Be notified of a personal data breach which is likely to cause damage or distress to the data subject.
- Make a complaint to the supervisory authority (ICO); and
- In limited circumstances, receive or ask for personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

Colleagues must verify the identity of an individual requesting data under any of the rights listed above where necessary (do not allow third parties to persuade you into disclosing personal data without proper authorisation).

BCHG recognises that individuals have the right to make a request to obtain a copy of their personal information, if held on our system and files. These rights are known as 'data subject access'. A formal procedure needs to be followed in relation to this matter, therefore please refer to BCHG's Data Subject Access Request Procedure, for more detailed guidance. Under DUAA, BCHG will apply updated SAR exemptions (e.g., vexatious or excessive requests) and maintain DUAA-aligned record-keeping to evidence decisions.

BCHG recognises that individuals have the right to prevent data processing where it is causing them damage or distress. BCHG may use automated decision-making where legally permitted under DUAA. Where used, BCHG will provide clear notice, allow individuals to challenge decisions, and offer human review.

BCHG will only share information in accordance with the provisions set out in the DPA18 and where applicable, BCHG will inform individuals of the identity of third parties to whom we may share, disclose, or be required to pass on information to, whilst accounting for any exemptions which may apply under the legislation.
DUAA strengthens requirements for handling complaints and clarifies how individuals exercise rights regarding automated decisions. BCHG will maintain DUAA-aligned procedures and provide enhanced transparency.

Each Corporate Department, Care Home and Retirement Living Scheme is responsible for the personal data which it collects and processes. This responsibility extends to personal data that is processed by any third parties on behalf of BCHG.

BCHG recognises and understands the consequences of failure to comply with the requirements of the DPA 18 may result in:

- Criminal and/or civil action
- Fines and damages
- Personal (e.g., employee) accountability and liability
- Suspension/withdrawal of the right to process personal data by the ICO
- Loss of confidence in the integrity of BCHG's systems and processes
- Irreparable damage to BCHG's reputation

Record Keeping

BCHG must keep and maintain accurate corporate records reflecting our processing including records of data subjects' consents and procedures for obtaining consents. These records should include, at the very least, the name and contact details of the Data Controller, the Information Asset Owner and the DPO. It should also include clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place. This is recorded in the BCHG Data Asset Register which is reviewed annually.

Training and Auditing

BCHG are required to ensure all employees have undergone mandatory data privacy related training to enable them to comply with data privacy laws. The Group also regularly monitor our systems and processes to assess compliance. All employees must regularly review all the systems and processes within their remit to ensure they comply with this Policy and check that adequate information governance controls and resources are in place to ensure proper use and protection of personal data. Members of the Data Management Panel should complete data Control Returns as part of the Data Security Framework to confirm the data integrity and data access checks that have been carried out on the systems they are responsible for.

Privacy by Design and Data Protection Impact Assessments (DPIAs)

BCHG are required to implement Privacy by Design measures when processing personal data by implementing appropriate technical and organisation measures in an effective manner, to ensure compliance with the data protection principles. Colleagues must assess what Privacy by Design measures can be implemented on all programs/systems/processes that process personal data. This can be achieved on most

projects by conducting a DPIA which helps consider, the nature, scope, context, and purposes of processing; and the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing. The DPIA template and completed DPIA's are available to colleagues on the Intranet and can be submitted to the Data Management Panel for review and consultation.

Colleagues should seek support/input from the DPO, when implementing major system or business change programs involving the processing of personal data including:

- Use of innovative technologies (programs, systems, or processes), or changing technologies (programs, systems, or processes).
- Large scale processing of sensitive data; and large scale, systematic monitoring of a publicly accessible area.
- A description of the processing, its purposes and the data controller's legitimate interests of appropriate.
- An assessment of the necessity and proportionality of the processing in relation to its purpose.
- An assessment of the risk to individuals; and
- The risk mitigation in place and demonstration of compliance.

Sharing, Processing and Retaining Information

Access to personal data will be limited to colleagues with a professional need to access the information to fulfil their role. Generally, BCHG should not share personal data with third parties unless certain safeguards and contractual arrangements have been put into place.

Personal data may be shared with third parties, such as BCHG service providers or partners if:

- A fully executed data sharing agreement or written contract that contains GDPR approved third party clauses has been obtained.
- They have a need to know the information for the purposes of providing the service or fulfilling a duty.
- Sharing the Personal Data complies with the Privacy Notice provided to the data subject and, if required, the data subject's consent has been obtained.
- The third party has agreed to comply with the required data security standard, policies and procedures and put adequate security measures in place.
- The transfer complies with any applicable cross border transfer restrictions.

Where other data controllers request personal information about a customer or employees, we will only share this data where a lawful basis has been established through legislative or regulatory requirements or a valid Data Sharing Agreement is in place. We will assess the request and must consider the purpose of the request and whether the

data sharing objective can be reached by other means e.g. anonymisation etc. Colleagues should consider asking the requester to complete a Data Protection Act Access Request Form, which sets out the information we require to assess and where applicable, comply with the request. Where there is a legitimate, lawful basis for disclosure of personal data to the third party we will:

- verify the identity of the requester.
- only share information that is accurate and up to date to the best of our knowledge;
- ensure that any information is disclosed securely;
- record data sharing requests and decisions made in response to them in the Data Sharing Log.

Examples of where personal data information might be shared without prior consent include:

- Where BCHG has a statutory duty to disclose information, e.g., tax office, council tax office.
- Where the police are investigating a criminal matter.
- Information of a non-personal nature may be released. Personal information or requests to search premises must not be agreed without prior legal authority.
- Where public health or national security issues are involved (The Public Interest Disclosure Act 1998).
- When housing benefit is paid direct, BCHG has a duty to provide certain information, e.g., commencement of tenancy date, changes in rent and service charge etc.
- Where information relating to tenancy dates is requested in respect of statutory services such as gas and electricity supplies.

Personal Data Breach

A data breach can occur in many ways, for example:

- Theft or accidental loss of personal data
- A deliberate attack on the organisation's systems
- The unauthorised use of personal data by a staff member
- Mistakenly sending personal data to an unintended recipient
- Accidentally sharing your screen (when third party personal data is visible) during a video call.

The legislation requires BCHG to notify any reportable Personal Data Breaches to the ICO and, in certain instances, to the Data Subject within 72 hours of becoming aware of the breach. If colleagues know or suspect a Personal Data Breach has occurred, do not attempt to investigate the matter yourself, immediately contact the Data Protection Officer (DPO) and follow the Personal Data Breach Procedure. Colleagues should preserve all evidence relating to the potential Personal Data Breach.

The penalties for breaching the Act can be severe as the ICO has regulatory powers to:

- Impose monetary penalties of up to, £17.5 million, or 4% of total worldwide annual turnover, whichever is the higher (dependent upon the severity of the data breach).
- Issue an undertaking or enforcement Notice requiring an organisation to take remedial action and update procedures and train staff; and/or
- Criminally prosecute organisations and in some circumstance's individuals or employees of the organisation.

If personal information has been lost, stolen, or otherwise dealt with in contravention of this Policy, it must immediately be reported to BCHGs Data Protection Officer (data@bchg.co.uk). This will allow for the appropriate reporting to the ICO and expedient mitigating actions to be carried out.

Data Protection Officer (DPO)

The DPO is responsible for overseeing this Policy and, as applicable, developing related policies and privacy guidelines. The post is held by Sharon Woods, Head of Corporate Services and Company Secretary, data@bchg.co.uk.

Please contact the DPO with any questions or concerns about this Policy, data protection and security, or if concerned this Policy is not being or has not been followed. Always contact the DPO in the following circumstances:

- You are unsure of the lawful basis which you are relying on to process personal data.
- you need to rely on consent and/or need to capture explicit consent.
- you need to draft Privacy Notices or Fair Processing Notices.
- you are unsure about the retention period for the Personal Data being Processed.
- you are unsure about security or other measures you need to implement to protect personal data.
- there has been a Personal Data Breach;
- you need any assistance dealing with any rights invoked by a data subject.
- whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use personal data for purposes others than what it was collected for.
- you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;
- you need help complying with applicable law when carrying out direct marketing activities; or
- you need help with any contracts in relation to sharing Personal Data with third parties.