Data Protection Policy

For Employees

Date of Approval: May 2025

Policy Author: Governance & Risk Manager

Policy Lead: Governance & Risk Manager

Date of next review: May 2027

You are advised that a printed version may not be the latest available version. The latest version, which supersedes all previous versions, is available on the Brighter Places Policy Index Sheet. Those to whom this policy applies, are responsible for familiarising themselves with the latest version and for always complying with the policy requirements.

Should colleagues require any reasonable adjustment to allow for engagement with this document please contact the policy lead

Contents

1. Policy Statement / Purpose 3
2. Brighter Places use of personal data 4
3. Data Protection legal framework 4
4. Definitions 4
5. Data Protection Principles 5
6. Lawful basis for processing 6
7. Consent 7
8. Individuals Rights 8
10. Transparency and Accessibility 10
11. Accountability 10
12. Assessing the possible impact of data processing 10
13. Data sharing 10
14. Data retention 11
15. Data risks, breaches and security 11
16. Monitoring of legal compliance 12
17. Data accuracy 12
18. Changes to this policy 12
Appendix i. Responsibilities for Employees regarding Data Protection 14
Appendix ii. Accompanying Documents 17

1. Policy Statement / Purpose

Brighter Places is committed to protecting individuals' personal information. We must:

- Comply with the UK General Data Protection Regulation (the UK-GDPR), the Data Protection Act and any other current data protection law and implement best practice
- Protect the rights and freedoms of those whose personal data we collect and use
- Be open and transparent in the way we collect, use, share, store and delete personal data
- Have appropriate technical and organisational processes and safeguards in place to ensure the security of the personal data we hold.

This Policy describes the basis on which we process any personal data we collect directly from individuals or that is provided to us from other sources. It sets out our obligations regarding data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

Employees

This Policy applies to all individuals who use personal data on behalf of Brighter Places including employees, volunteers, involved residents and Board & Committee members of Brighter Places itself and our subsidiary company, Bristol Living Limited. This extends to others we work with under contract such as managing agents who may have their own policy but should be aware of ours and adhere to the principles.

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

This Policy does not form part of any employee's contract of employment and may be amended at any time. However, the law takes precedence.

Customers

Questions about how we use personal data should be directed to our Data Protection Officer as follows:
E-mail: dataprotection@brighterplaces.co.uk
Post: Data Protection Officer, Brighter Places, Eden House, Eastgate Office Park, Eastgate Road, Bristol. BS5 6XX.

2. Brighter Places use of personal data

Brighter Places needs to gather and use certain information about individuals in order to be able to provide its services. We collect and process personal data about our customers, suppliers, business contacts, employees, and other people the organisation has a relationship with or may need to contact. There are also situations where we have a legal duty to supply information such as safeguarding or assisting with a criminal investigation.

3. Data Protection legal framework

We are committed to ensuring that we comply with the requirements of the data protection laws in force in England and Wales at any time. These laws include the Data Protection Act 1998 and the UK General Data Protection Regulation (UK GDPR). We are committed to complying with any formal written guidance published by the Information Commissioner's Office (ICO).

The laws apply to personal data, defined as information from which a living individual either can, or potentially can, be identified. This is information about individuals stored in electronic form, including audio and video, or in hard copy (where such information either is, or is intended to be, stored in a relevant filing system).

4. Definitions

Personal data

Any information relating to an identified or identifiable natural person. This is someone 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. This can be on piece of information or two or more sets of anonymised data that when used together can identify an individual for example could be someone's place of work and job title.

NB: This definition includes still photographs and video images and audio recordings where individuals could be identified.

Special category data *(previously called 'sensitive personal data')*

Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. There are specific rules for processing this kind of data, which Brighter Places observes.

Criminal offence data

Brighter Places only collects and processes this category of data when it is clearly in the public interest to do so or when required to carry out our duties as a housing provider (for example the housing of schedule 1 offenders) It can only be gathered and processed under certain conditions that Brighter Places has satisfied.

Data Controller

Brighter Places decides how and why data is used. Brighter Places is the legal Data Controller for the personal information it gathers and stores and is responsible for the data when it is processing it and when the data is processed by other organisations on its behalf.

Data Processor

A data processor is a third party acting under contract with Brighter Places, who must act as required by Brighter Places in relation to the personal data we share with them for specific purposes.

Conditions for processing

Data controllers must have a lawful basis for processing personal data. Data Protection law sets out six lawful basis for processing and we must choose whichever is most appropriate. There are additional conditions for processing special category and criminal offence data.

Information asset

A record of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles. Brighter Places' holds a ROPA (Records of Processing Activities) which is our record of the personal data we collect and how it is used.

Information Commissioners Office (ICO)

The ICO is the supervisory body for data protection in the UK.

5. Data Protection Principles

Under the UK GDPR there are 7 data protection principles. The principles require those using personal data to ensure that it is:

1. Used in a way which it lawful, fair and transparent
2. Only collected for a specified, explicit and legitimate purpose
3. Adequate, relevant and limited to what is necessary for the processing purpose

4. Accurate and up to date
5. Kept in a form which allows identification of individuals for no longer than necessary
6. Kept securely to prevent unauthorised processing, accidental loss, destruction or damage by using appropriate technical or organisational measures.
7. Accountability – Brighter Places is accountable for the personal data we hold, how we use it and how we keep it secure.

6. Lawful basis for processing

The first data protection principle requires Brighter Places to ensure that we have a lawful basis for any processing of personal data. There are six lawful bases prescribed in the UK GDPR:

- **Contract** - our use of an individual's personal data is necessary in order for us to perform a contract between us and that individual which may include, for example, a tenancy agreement, or to take steps to enter into that agreement with an individual

- **Legal obligation** - We are required to process personal data as a result of a legal obligation placed on us

- **Vital interests** - the processing is necessary to protect someone's life.

- **Public task** - the processing is necessary for performing a task in the public interest or exercising official authority.

- **Legitimate Interests** - the processing is necessary for the legitimate interests of the data controller or a third party, unless those interests are overridden by the rights and freedoms of the individual.

- **Consent** - The individual has provided their consent for us to use their data for a particular purpose

When there's a contract in place with the individual
In most instances, Brighter Places only use personal data insofar as it is necessary for us to perform the contract between us and the individual. For example, a tenancy contract or a contract of employment.

Where the use of an individual's person's personal data is necessary for us to perform a contract with that person, we do not need their consent. In order to lawfully use special category personal data, we must satisfy additional Data Protection Act 2018 conditions.

The lawful basis on which Brighter Places shall rely on relation to any personal data, special category and criminal offence data must be documented in our ROPA (records of processing activities). If an employee is unsure about the lawful basis for any data processing, they should consult the Data Protection Officer. Personal data should only be used for the purpose for which it was originally collected, or a new purpose which is compatible with the existing purpose. If a new use is proposed for the data a Data Protection Impact Assessment (DPIA) will be considered if this is likely to result in a "high risk" situation.

7. Consent

At Brighter places we only use consent in specific circumstances when other lawful bases are not appropriate. Our lawful basis for processing is clearly set out in our privacy statements. For example, we would not require consent when someone provides their name and other evidence when gaining one of our homes, also we do not need consent in order to fulfil a contract and provide a service to customers. Examples of when we may use consent is gathering medical data, marketing materials etc.

To gather consent, we must clearly state what we want to use their data for and individuals must actively indicate that they are providing their consent. They may decline or object at any time. Silence does not confirm consent. Pre-ticking the boxes is not considered valid consent.

Evidence of consent must be retained and completed consent forms must be stored securely in Brighter Places' filing system

Individuals can withdraw their consent at any time by contacting the Brighter Places' Data Protection Officer or discussing with a member of staff who can make arrangements to withdraw consent. Where this has been actioned, we will record this, and the action taken.

8. Individuals Rights

The UK GDPR provides individuals with prescribed rights relating to the use of their personal data. As an organisation, we must not infringe those rights. If you receive one of these requests, please pass it on the Data Protection Officer immediately.

The right of access & Data Subject Access Requests (DSAR)

Individuals have the right to request a copy of the personal data we hold about them and the purposes for which we are using it. We have one month to respond to the request.

All individuals whose personal data is held by Brighter Places have the right to submit Subject Access Requests about how we control and process their information, and to exercise their rights as listed above. This could be customers or stakeholders, tenants or employees.

- **Customer:** All Subject Access Requests should be sent to Brighter Places' Data Protection Officer.
- **Employee:** When an employee has received, or considers they might have received, a Subject Access Request, they should contact the Data Protection Officer and follow the relevant Brighter Places process to respond to the request.

The right to be informed

- Individuals have the right to ask Brighter Place's purposes for processing their personal data, how long Brighter Places will retain that data, and who it may be shared with.
- This information is provided in Brighter Places' Privacy Notices which are on the website

The right to erasure

- Individuals have the right to have personal data erased, also known as 'the right to be forgotten'
- An individual may ask that the personal information Brighter Places holds about them is deleted or removed and that any third parties who process or use data also comply with the request
- There may be some restrictions to this where its part of our contract to provide a service or legal requirements. This will be in line with the guidance and data retention.

The right to rectification

- Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete

The right to data portability

- Individuals have the right to data to obtain and reuse their personal data for their own purposes across different services; to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

The right to object

- Individuals have the right to object to the processing of their personal data in certain circumstances.
- This is usually applicable to activities such as direct marketing, for example, the newsletters Brighter Places occasionally sends to its leaseholders and tenants.
- All Brighter Places' e-mail newsletters contain an 'unsubscribe' link.

The right to restrict processing

- Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, organisations are permitted to store the personal data, but not use it
- We reserve the right in some cases to continue to use personal data if we are legally obliged to and/or where we consider processing to be necessary and can claim a lawful basis or legitimate interest for doing so.

Rights in relation to automated decision making and profiling

- Individuals have the right to object to automated individual decision-making (deciding solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual).
- Brighter Places does not carry out automated decision making or profile data.
- Where required, reasonable adjustments will be considered to support colleagues to engage with this policy. Please speak to the policy owner for assistance.

10. Transparency and Accessibility

The first data protection principle requires us to be transparent in relation to how we collect and use personal data.

We provide accessible information to individuals about how we will use their personal data in our Privacy Notices, made available at the point they first give us their details (online and offline). These are all regularly reviewed and updated.

The relevant version can be found on our website at https://www.brighterplaces.co.uk/privacy-notices-and-gdpr/, these must be given to every individual when they provide their personal information to us. and all Privacy Notices must be updated if new categories of information are collected and processed or shared in different ways in the future.

11. Accountability

We are required to maintain records of all our data processing activities in a Record of Processing Activity. This is contributed to by teams across Brighter Places and overseen by the Data Protection Officer.

12. Assessing the possible impact of data processing

Data Protection laws require us to consider the data protection implications of any project or process, both at the beginning and throughout the life of any processing. A Data Processing Impact Assessment (DPIA) is to be carried out and logged for high risk data processing activities i.e. those which may have a high risk to individuals..

A DPIA is used to assess the impact the processing of personal data will have on individuals.

13. Data sharing

Where personal data is shared with a third party organisation, either regularly or for one off projects, consideration is given to whether a Data Processing Agreement or a data sharing agreement is appropriate in the circumstances. Those agreements completed are recorded.

Conditions outlining compliance with the UK GDPR is a standard requirement for any data processing agreement, contract or data sharing agreement with employees, contractors and third-party organisations. In order to share personal data with any third

party we must have a lawful basis for doing to. Our reasons for sharing personal data are clearly set out in our Privacy Notices.

In limited circumstances such as in in the interests of crime prevention and detection as requested by the Police or other law enforcement or legal organisations, we may disclose personal data to an organisation without informing the individual beforehand. Under such circumstances, we ensure the request is lawful and legitimate and seek guidance from the Data Protection Officer.

Personal data which could pose a risk to individuals must be shared using an appropriately secure method, e.g. an encrypted email or secure online portal. General emails to customers are not encrypted nor are general emails.

If we are made aware of any personal data is to be shared outside the European Economic Area the Data Protection Officer must be contacted so that appropriate assessments can be made.

14. Data retention

Brighter Places retains personal data for specific reasons and for fixed periods of time as outlined in our Data Retention Schedule, with any exceptions noted and the reasons for keeping longer than good practice.

15. Data risks, breaches and security

Brighter Places' employees and third parties who process personal data on Brighter Places' behalf must report actual or potential data protection compliance failures and breaches to the Data Protection Officer immediately, as soon as they are discovered. In the case of a serious breach, we the Data Protection Officer inform the ICO and any affected individuals as soon as possible.

This policy helps to protect Brighter Places from data security risks including:

- **Data breach** e.g. if data is lost, for example a lost or stolen mobile device or a paper file. If a database containing personal information or special category data is lost, stolen or hacked. In fact, any unauthorised loss of personal data.
- **Risk of fines** if the organisation is deemed to have acted illegally or negligently by the ICO.

In the event of a potential data breach, Brighter Places:

- Immediately investigate and take any remedial actions

- Maintain a register of data breaches and near misses
- In the case of a significant breach, notify the ICO within 72 hours.

16. Monitoring of legal compliance

Brighter Places is committed to ensuring that it is always compliant with current Data Protection legislation. In line with the UK GDPR, Data Protection audits are carried out, either by external providers or by Brighter Places' Data Protection Officer, at regular intervals and included in our forward plan with the internal auditors which is agreed annually but the Audit & Risk Committee.

17. Data accuracy

Employees - Changes to personal information, such as contact details, must be kept up to date, and inaccuracies must be corrected as soon as they are discovered.

Tenants - Tenants and others can update the personal information Brighter Places holds using the My Tenancy online portal.

Data is regularly reviewed and updated if it is found to be out of date. If, in line with the Data Retention Schedule, if it is no longer required, it is deleted and disposed of securely. This includes both electronic and hard copy files.

18. Changes to this policy

This policy will be reviewed every two years or following any changes or updates in relevant legislation, whichever is the sooner.

19. Roles & responsibilities

Activities	Board	CEO	Finance Director	ARC	Exec	M'gers	All staff	Gov
Owner of the policy			x					
Monitoring & review of the policy				x				x

Activities	Board	CEO	Finance Director	ARC	Exec	M'gers	All staff	Gov
Approval of changes to the policy				x				
Responsible for policy implementation			x					x
Addressing issues in the implementation of the policy			x					x
Version control of live policy								x
Training of colleagues						x	x	x

Appendix i.

Responsibilities for Employees regarding Data Protection

Responsibilities

The Board and Executive Team are responsible for establishing and maintaining a control environment that promotes overall compliance, including approval of this Policy and any significant amendments or updates made to it.

All employees, involved residents, main contractors and Board & Committee Members are responsible for ensuring, whilst undertaking their roles, that they do so in compliance with this Policy, the UK GDPR and other Data Protection laws. They also have responsibility to report actual or potential personal data breaches or near misses to the Data Protection Officer.

Members of staff who gather, record and process personal information are responsible for working with the Governance & Risk team to ensure our ROPA is up to date, which should be reviewed and, where necessary, updated on a regular basis. The Register shows what data assets are held, who this data is shared with, who has access and why, checks that their use of the information is compliant, records any possible risks and risk management activity and monitors retention and destruction of data sets in line with Brighter Places' Data Retention Schedule.

The Head of IT & Data is responsible for ensuring all systems, services and equipment used for storing data meet acceptable security standards; making sure that regular checks are performed through scans and penetration testing etc. to ensure security hardware and software is functioning properly; and evaluating any third-party services the company is considering using to store or process data.

The HR Manager, along with the Data Protection Officer, is responsible for the provision of data protection training.

The Data Protection Officer is responsible for handling data protection questions from employees, involved residents and tenants. They also provide guidance on the interpretation and implementation of the UK-GDPR and Data Protection law; are responsible for reviewing and updating Brighter Places' GDPR and data protection policies and procedures; and oversee responses to Data Subject Access Requests or any other enquiries or complaints relating to Brighter Places' data controller and data processor activities.

The Events and Communications Co-ordinator, working with the Data Protection Officer, is responsible for addressing data protection queries from journalists or media outlets. They also ensure that e-mails and postal communications contain

Data Protection statements and wording as required and work with other staff to ensure all communications and newsletters are compliant.

Staff and Personal Data

Staff handling personal data on behalf of Brighter Places are required to comply with the following obligations at all times. This should be read alongside our Digital Security and Compliance Policy. Failure to comply with this Policy and the associated processes and procedures may result in disciplinary action up to and including dismissal without notice:

- Access to personal data must be strictly limited to those who need it for their work on behalf of Brighter Places
- Employees must keep all personal data secure, by taking sensible precautions and following the guidelines below
- Strong passwords must be used for Brighter Places IT Equipment and must meet the requirements set out in the Digital Security and Compliance Policy . They should never be shared
- Personal data must not be disclosed to unauthorised people, either within the company or externally
- Employees must not leave paper, printouts or files where unauthorised people can see them, e.g. on desks, in meeting rooms or on a shared printer
- Brighter Places operates a clear desk policy. Any paper documentation or files must not be left on desks and kept in lockable drawers or cabinets
- Access to securely stored and archived records containing personal data is only permitted based on business needs and imperatives
- Computer screens must be locked whenever they are left unattended
- Printouts containing personal data must be placed into the confidential waste bins provided and disposed of securely when they are no longer required
- Employees must not save copies of personal data to their own home computers or Brighter Places devices' c drives
- Personal data must not be sent by standard email, as this form of communication is not secure. Data must be encrypted/password before transferring it electronically

- Standard reports (spreadsheets) must be data minimised to remove personally identifiable information and only be made available to those who need them for their work.
- Staff should be aware of the use of CCTV and audio recording in reception areas and tenant meeting rooms and adhere to guidance set out in the CCTV policy and Data processing assessment.
- Data Protection and cyber security training is provided within the company induction programme and on an ongoing basis. Please speak to the Data Protection Officer or HR for more details

Advice and support for employees

Employees should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection. Staff should ensure they report any possible breaches, near misses or concerns as soon as possible.

Appendix ii.

Accompanying Documents

This Policy summarises Brighter Places' approach to legal compliance and best practice in the organisation's use of personal information. The following accompanying documents should also be noted:

- Data Breach/ Near Miss Procedure
- Subject Access Request guidance
- Record of Processing Activity
- Legitimate Interest Assessment for CCTV
- Data Retention Schedule
- Data Processing template

Also:

- Data Subject Access Request Register
- Data Processing Register
- Data Breach /Incident Register
- Clear Desk Procedure
- Home working
- Digital Security & Compliance policy
- Privacy Statements

TRANSLATIONS

If English is not your first language and you need a translation, we can get one for you.

ALBANIAN

Nëse anglishtja nuk është gjuha juaj amtare dhe keni nevojë për një përkthim, ne mund t'ua sigurojmë atë.

BENGALI

ইংরেজী আপনার মাতৃভাষা না হলে এবং আপনার কোন অনুবাদের প্রয়োজন হলে আমরা তা প্রদান করতে সক্ষম।

CHINESE

如果英文不是您的第一語言，而您需要翻譯的話，我們可以爲您安排。

GUJARATI

જો તમારી પહેલી ભાષા અંગ્રેજી ન હોય અને તમને ભાષાંતરની જરૂર હોય તો અમે તમને તે આપી શકીએ છીએ.

HINDI

यदि अँग्रेज़ी आप की पहली भाषा नहीं है और आप को अनुवाद की आवश्यकता है तो यह हम आपको प्रदान कर सकते हैं

KURDISH

Heke îngilîzî zimanê we yê yekem nîne û pêwîstîya we bi wergêr heye, em dikarin yekî ji we re bibînin

POLISH

Jeżeli język angielski nie jest Twoim językiem ojczystym i wymagasz tłumaczenia, możemy to zapewnić.

PORTUGUESE

Se o Inglês não é a sua língua materna e precisa de uma tradução, nós podemos obtê-la.

PUNJABI

ਜੇਕਰ ਇੰਗਲਿਸ਼ ਤੁਹਾਡੀ ਪਹਿਲੀ ਭਾਸ਼ਾ ਨਹੀਂ ਅਤੇ ਤੁਹਾਨੂੰ ਦੁਭਾਸ਼ੀਏ ਦੀ ਜ਼ਰੂਰਤ ਹੈ ਤਾਂ ਤੁਹਾਡੇ ਲਈ ਅਸੀਂ ਇਸਦਾ ਪ੍ਰਬੰਧ ਕਰ ਸਕਦੇ ਹਾਂ।

SOMALI

Haddii Ingiriisku aanu ahayn afkaaga kowaad oo aad u baahan tahay turjumaad, annagaa kuu samayn karra.

URDU

اگر انگریزی آپ کی پہلی زبان نہیں ہے اور آپ کو ترجمہ کی ضرورت ہے تو ہم آپ کے لئے فراہم کر سکتے ہیں۔

VIETNAMESE

Nếu quí vị không thao Anh văn và cần bản dịch, chúng tôi sẽ giúp quí vị một bản.