Data Protection Policy

Applicable to:

☒ All Brighter Places, previous Solon, and previous UC customers

☐ Previous Solon customers only

☐ Previous UC customers only

☒ All Brighter Places, previous Solon, and previous UC colleagues

☐ Previous Solon colleagues only

☐ Previous UC colleagues only

Date adopted by Brighter Places:	February 2022
Date of previous full review:	April 2018
Date of next review:	**February 2025**

Author/Policy owner: Data Protection Officer

Brighter Places

Data Protection Policy for Employees

Introduction

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

- 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, involved residents and Board members of Brighter Places itself and our subsidiary company, Bristol Living Limited.

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.

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.

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.

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 or in hard copy (where such information either is, or is intended to be, stored in a relevant filing system).

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.

NB: This definition includes still photographs and video images where individuals can be clearly 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. 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 – third parties must act as required by the Brighter Places in relation to shared personal data.

Conditions for processing - Data controllers must have a legal basis for processing data. Data Protection law sets out the legal basis for processing. There are additional conditions for processing special category and criminal offence data.

Information asset - A body 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' Information Asset Register is a summary of the personal information Brighter Places holds and processes.

Information Commissioners Office (ICO) - The ICO is the supervisory body for data protection in the UK.

Data Protection principles

Under the UK- GDPR there are 6 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.

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:

- The individual has provided their consent for us to use their data for a particular purpose
- 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
- We are required to process personal data as a result of a legal obligation placed on us
- Unless another lawful basis applies, we only use personal data insofar as it is necessary for us to perform the contract between us and the individual
- Where the use of a 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 and criminal offence data, we must satisfy additional lawful bases.

Employees - The lawful basis on which Brighter Places shall rely in relation to any personal data, special category and criminal offence data must be documented in our Information Asset Register. If an employee is unsure about the legal basis for any data processing, they should consult the Data Protection Officer. Data should only be used for the purpose for which it was originally collected. If a new use is proposed for the data a Data Protection Impact Assessment (DPIA) must be made to ensure that the proposed purpose is necessary and whether it is compatible with the original purpose.

Consent

Consent under Data Protection law must be sought for processing all forms of personal information, including images. The way consent is captured must be specific and clear.

Individuals must actively indicate that they are providing their consent. Silence that presumes consent is not acceptable, and forms that show pre-ticked boxes are not compliant.

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

Individuals can withdraw their consent at any time by contacting the Brighter Places' Data Protection Officer.

However, if the withdrawal of consent will affect how Brighter Places provides its services, this should be made clear so that the withdrawal is made based on complete knowledge of the possible implications.

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.

- *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 share with
    - This information is provided in Brighter Places' Privacy Notices which are on the website or available for the Data Protection Officer
- *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
    - The right to erasure applies in specific circumstances:
    - the personal data is no longer necessary for the purpose for which we originally collected or processed it
    - Brighter Places are relying on consent as its lawful basis for holding the data, and the individual withdraws their consent
    - Brighter Places are relying on legitimate interests as it's basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing
    - Brighter Places are processing the personal data for direct marketing purposes and the individual objects to that processing
    - Brighter Places has processed the personal data unlawfully in breach of the UK-GDPR and Data Protection law
    - Brighter Places have to erase the data to comply with a legal obligation
    - if the data relates to a child under 13 and their parent, guardian or carer withdraws consent
- *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.

Subject Access Requests

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.

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.

Transparency and accessibility

The first data protection principle requires us to be transparent in relation to how we use personal data. This includes being transparent both with the individuals whose personal data we process and with the ICO.

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). We currently have different versions for Leaseholders, Tenants, Employees and Job Applicants, which are all regularly reviewed and updated.

The relevant version must be given to every individual when they provide their personal information to us. Further versions will be created for other new groups in the future and all Privacy Notices must be updated if new categories of information are collected and processed, or shared in different ways in the future.

We also publish a more general Privacy Notice for the public on the Brighter Places website.

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.

Estimating 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 every data processing activity. A DPIA is used to work out the impact the processing of personal data will have on individuals. It is required by law when the use of personal data is likely to result in a high risk to individuals.

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 sharing agreement and/or non-disclosure agreement is appropriate in the circumstances. Those agreements completed are recorded.

Conditions outlining compliance with the UK-GDPR and Data Protection law is a standard requirement for any data sharing agreement, contract or non- disclosure 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 legitimate, and seek guidance from the Data Protection Officer.

Personal data must always be shared using an appropriately secure method, e.g. an encrypted email or secure online portal.

We do not transfer any personal data outside the European Economic Area unless our Data Protection Officer has confirmed that such a data transfer is lawful and appropriate in the circumstances.

Data retention

Brighter Places retains personal data for specific reasons and for fixed periods of time as outlined in our Data Retention Schedule.

Data risks, breaches and security

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

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

- **Breaches of confidentiality** – personal information being shared or made public in contravention of the UK-GDPR and Data Protection law
- **Reputational Damage** – e.g. if data is lost, for example from a mobile device or a paper file; if a database containing personal information or special category data is hacked
- **Risk of fines** – if the organisation is deemed to have acted illegally or negligently by the ICO.

In the event of a data breach, Brighter Places:

- Immediately investigate and take any remedial actions

- Maintain a register of data breaches
- In the case of a serious breach, notify the ICO within 72 hours

Monitoring of legal compliance

Brighter Places is committed to ensuring that it is always compliant with current Data Protection legislation. In line with the advice of the UK-GDPR, Data Protection audits are carried out, either by external providers or by Brighter Places' Data Protection Officer, at regular intervals and by an external provider at least every 5 years.

Data quality

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

Employees - Changes to 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.

Changes to this Policy

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

Appendix 1 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.

Brighter Places also has in place a Data Protection Governance group, comprised of employees led by the Data Protection Officer, to monitor data protection issues and legal compliance.

All employees, involved residents, and Board Members are responsible for ensuring, whilst undertaking their roles, that they do so in compliance with this Policy, the UK-GDPR and Data Protection law. They also have responsibility to report actual or potential data security breaches to the Data Protection Officer.

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 Subject Access Requests or any other enquiries or complaints relating to Brighter Places' data controller and data processor activities.

The Finance Director 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.

Members of staff who gather, record and process personal information are responsible for updating the Information Asset Register, 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.

Working with the Data Protection Officer, the Events and Communications Co-ordinator 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. 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 PCs and laptops and changed regularly in line the IT policies. 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 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.
- Data Protection 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.

Appendix 2 - 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 Procedure
- Subject Access Request and Rights of an Individual Policies and Procedures
- Information Asset Register
- Record of Processing Activity
- Legitimate Interest Assessment
- Legitimate Interest Statement
- Data Retention Schedule
- Data Sharing Policy and Guidance
- Data Protection Impact Assessment Procedure

Also:

- Subject Access Request Register
- Data Sharing Register
- Data Processor Register
- Data Breach Register
- Clear Desk Policy
- IT Security Policy