

T3 Residential Limited

Data Protection Policy

1 Introduction

1.1 T3 Residential Limited ("**T3 Residential**") is committed to keeping all personal information collected from individuals or service users (data subjects) safe, as required by the General Data Protection Regulation ("**UK GDPR**") and Data Protection Act 2018 ("**DPA18**"). This applies whether the data is collected on paper, stored in a computer database, or recorded via other means. T3 Residential has put in place safeguards to ensure data compliance.

1.2 This policy applies to board members, all staff including all employees, workers, consultants, vendors or any other third parties acting on behalf of T3 Residential.

2 Legal and Regulatory Responsibilities (not exhaustive)

2.1 This policy complies with relevant legislative and regulatory requirements set out in the following:

- UK GDPR; and
- DPA18.

2.2 In line with DPA18, T3 Residential will register as a data controller on the Public Register of Data Controllers maintained by the Information Commissioners Office ("**ICO**").

3 Policy

3.1 This policy sets out the responsibilities for processing personal data and explains residents' rights to access their information. It also describes the procedures for complying with all statutory and regulatory requirements.

3.2 It ensures that individuals whose information is held can fully exercise their rights under the law, including:

- The right to be informed about data processing;
- The right to access their personal information;
- The right to correct or rectify inaccurate data;
- The right to have their data erased ("the right to be forgotten");
- The right to restrict or suppress the processing of their personal data;
- The right to data portability, enabling individuals to obtain and reuse their data;
- The right to object to certain types of processing; and
- The right to request the restriction or suppression of their personal data.

3.3 To keep data secure, T3 Residential will:

- Implement appropriate technical and organisational measures to protect personal information;
- Follow the DPA18 in cases of data loss, corruption, or compromise;
- Provide training to all employees T3 who process personal data to ensure that they understand their responsibilities to uphold good data protection practices and comply with legislation;
- Ensure that no personal data will be removed from T3 Residential systems or premises except for legitimate business purposes;
- Ensure board members, staff, vendors, and third parties acting on behalf of T3 Residential are aware of their responsibilities to protect any personal data that they may remove from T3 systems or premises for legitimate business purposes;

- Provide guidance to staff on the approach and principles to sharing personal data;
- Make staff and board members aware that breaches of this policy may result in disciplinary action;
- Regularly audit how personal information is held, managed, and used;
- Allow individuals to request modification, erasure, reduction, or correction of data in our database; and
- Ensure there is an appointed Data Protection Officer/Manager to ensure internal compliance with data protection legislation and advise on our obligations and be a point of contact for data subjects.

4 Special Categories

4.1 Previously known as sensitive personal data, this is data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data (where used for ID purposes);
- Health; and
- Sexual orientation or concerning a person's sex life

4.2 In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law. Any such consent will need to clearly identify what the relevant data being captured is, why it is being processed and to whom it will be disclosed.

4.3 When processing this data, we will identify a lawful basis under Article 6 of the UK GDPR and a separate condition under Article 9. Where we do not have a lawful basis, the data will not be processed.

5 Criminal Offence Data

5.1 We will only process criminal offence data if we can identify a specific condition for processing in Schedule 1 of the DPA18. We will not keep a comprehensive register of convictions.

5.2 We will determine the condition for processing criminal offence data, or identify our official authority for the processing, before we begin the processing, and we will document this.

6 Monitoring and Performance

6.1 The board is responsible for ensuring compliance with legislative changes to data protection legislation and regulatory requirements. T3 Residential will continually review data protection law to ensure ongoing compliance.

7 Policy Commitment

7.1 T3 Residential will ensure protection of personal data is a primary consideration by completing Data Protection Impact Assessments, as appropriate

- 7.2 Limit access to personal information to those team members/entities whose legitimate business needs require the information
- 7.3 T3 Residential will comply with the principles of data protection, ensuring that personal information is:
- Processed fairly and lawfully;
 - Obtained and used for specific, limited purposes, and not processed in ways incompatible with those purposes;
 - Accurate and kept up to date, and that inaccurate personal data is erased or corrected;
 - retained only as long as necessary and in compliance with our retention and disposal schedule;
 - Processed within legal and ethical boundaries;
 - Processed in accordance with the rights of data subjects under GDPR;
 - Kept secure by the data controller, who must prevent unauthorised or unlawful processing, accidental loss, destruction, or damage;
 - Not transferred to countries or territories without adequate protection as required by the DPA18; and
 - Not communicated informally.

8 Data Breach

- 8.1 In the case of a member of staff becoming aware of a personal data breach they will:
- Report any data breach immediately to the IT team;
 - Comply with all IT requirements including, but not limited to:
 - Password protection protocol
 - Compliance with firewall protection
 - Security updates
- 8.2 Both residents and staff are encouraged to contact data.protection@getliving.com in the event of a data breach in order to be directed on next steps.
- 8.3 Any breach of data storage or unauthorised access will be reported to the appropriate authorities and to the affected individuals no later than 72 hours after being made aware of the breach.
- 8.4 Team members may contact the Data Protection Manager with any concerns or questions regarding data.
- 8.5 Any breach of this policy may result in disciplinary action, up to and including termination.

9 Subject Access Request

- 9.1 Individuals may make a subject access request to obtain their personal data held by T3 Residential. All staff will be trained on identifying subject access requests and ensuring they are sent to the appropriate officer to action.
- 9.2 T3 Residential will comply with the requirements detailed by the ICO when responding to these requests.

10 Marketing

- 10.1 Prior to sending marketing information to anyone:
- Use only T3 Residential approved systems and processes to send marketing information
 - Marketing information should be approved for release by the Managing Agents, Regional Director in all circumstances

11 **Equality, Diversity and Inclusion**

- 11.1 T3 Residential will treat all individuals fairly and justly in accordance with the Equality Act 2010 when handling information requests.

12 **Policy Review**

- 12.1 The board is responsible for ensuring this policy is kept up to date, implemented within the organisation and monitored and evaluated.
- 12.2 The policy will be reviewed every two years or more frequently as a result of an incident occurring, feedback obtained, internal/external audits and change in legislation or regulation. This process ensures the policy continues to be appropriate, adequate and effective.

13 **Background Documents**

- 13.1 This policy should be read in accordance with the following policy documents:
- ICT/Data Management Policy;
 - Equality and Diversity Policy;
 - Complaints Policy; and
 - Privacy Notice.

December 2025

Current version	Data approved	Date for Review	Document Owner	Date change log updated
1.0	December 2025	December 2026	Linnzie Wallace	n/a