Data Protection Policy

1. Introduction

Hurstleigh Homes needs to gather and use certain information about individuals.

These can include residents, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet our data protection standards – and to comply with the law.

2. Why this policy exists

This data protection policy ensures Hurstleigh Homes:

- Complies with data protection law and follow good practice.
- Protects the rights of staff, residents and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

3. Data Protection Law

The General Data Protection Regulations 2018 as transposed into UK law (UKGDPR) describes how organisations – including us – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The UKGDPR is underpinned by six important principles. These say that personal data must:

- Be processed fairly, lawfully and in a transparent manner.
- Be obtained for specified, explicit and legitimate purposes.
- Be adequate, relevant and limited to what is necessary.
- Be accurate and kept up to date.
- Not be held for any longer than necessary.
- Processed in an appropriate manner to maintain security.

4. People, Risks and Responsibilities

4.1 Policy Scope

This policy applies to:

- The residential home of Hurstleigh Homes.
- The Trustees.
- All staff and volunteers.
- All contractors, suppliers and other people working on behalf of Hurstleigh Homes.

It applies to all data that Hurstleigh Homes holds relating to identifiable individuals, even if that information technically falls outside the GDPR. This can include:

- Names of individuals.
- Postal addresses.
- Email addresses.
- Telephone numbers.
- any other information relating to individuals.

4.2 Data Protection Risks

This policy helps to protect Hurstleigh Homes from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how Hurstleigh Homes uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

4.3 Responsibilities

Everyone who works for or with Hurstleigh Homes has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and other data protection policies.

However, these people have key areas of responsibility:

- The **Trustees** are ultimately responsible for ensuring that Hurstleigh Homes meets its legal obligations. They are also responsible for;
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
  - Approving any data protection processes, policies and statements attached to communications such as emails and letters.
  - Addressing any data protection queries.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- The **Warden,** is responsible for overseeing data protection compliance in the home and with staff.

5. General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from the Warden.

- Hurstleigh Homes will provide training to all staff to help them understand their responsibilities when handling data.
- Staff should keep all data secure, by taking sensible precautions.
- Strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the charity or externally.
- Data should be regularly reviewed and updated if it is found to be out of date, if no longer required, it should be deleted and disposed of.
- Employees should request help from the Warden if they are unsure about any aspect of data protection.

6. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Trustees.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, such as on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from the general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with Hurstleigh Homes' standard backup procedures.
- All servers and computers containing data should be protected by approved security software and a firewall.

7. Data Use

When data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, staff should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.

- Data must be encrypted where possible before being transferred electronically. Our email system has end to end encryption.
- Personal data must not be transferred outside the UK unless approved by the Trustees and only then in accordance with the data transfer requirements pursuant to UKGDPR.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

8. Data Accuracy

The law requires Hurstleigh Homes to take responsible steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort Hurstleigh Homes should be in ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets or documents.
- Staff should take every opportunity to ensure data is updated and kept secure.
- Hurstleigh Homes will help data subjects to update the information Hurstleigh Homes holds about them.
- Data should be updated as inaccuracies are discovered. For instance, if a resident's relative can no longer be reached on their stored telephone number, it should be removed from the database.

9. Subject Access Requests

All individuals who are the subject of personal data held by Hurstleigh Homes are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the charity requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at our email address. We can supply a standard request form, although individuals do not have to use this.

We must provide the relevant data within 30 days.

We will always verify the identity of anyone making a subject access request before handing over any information.

10. Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Hurstleigh Homes will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

11. Providing Information

Hurstleigh Homes aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights.

To these ends, the charity has a privacy statement, setting out how data relating to individuals is used by the company.

Issue No	Description of change	Approval	Date of Issue	Date to review