



**Cottongrass
Homes**

DATA PROTECTION POLICY

Cottongrass Homes Data Protection Policy

1. Introduction

1.1. This Data Protection Policy is the overarching policy for data security and protection for *Cottongrass Homes Limited* (hereafter referred to as "us", "we", or "our").

2. Purpose

2.1. The purpose of the Data Protection Policy is to support the General Data Protection Regulation (2016) ("GDPR"), the Data Protection Act (2018) ("DPA18"), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

2.2. We comply with data protection legislation guided by the six data protection principles. They require that personal data is:

- 2.2.1. processed fairly, lawfully and in a transparent manner.
- 2.2.2. used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- 2.2.3. adequate, relevant, and limited to what is necessary.
- 2.2.4. accurate and, where necessary, up to date.
- 2.2.5. not kept for longer than necessary; and
- 2.2.6. kept safe and secure.

2.3. In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law.

3. Scope

3.1. This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data.

- 3.2. The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person. Pseudonymised personal data is covered by the legislation, however, anonymised data is not providing the anonymisation has not been done in a reversible way.
- 3.3. Some personal data is more sensitive and is afforded more protection this is information related to:
- 3.3.1. Race or ethnic origin;
 - 3.3.2. Political opinions;
 - 3.3.3. Religious or philosophical beliefs;
 - 3.3.4. Trade union membership;
 - 3.3.5. Genetic data;
 - 3.3.6. Biometric ID data;
 - 3.3.7. Health data;
 - 3.3.8. Sexual life and/or sexual orientation; and
 - 3.3.9. Criminal data (convictions and offences)
- 3.4. This policy applies to all children who are or who have been supported in our homes (hereafter referred to as "supported children"), and staff, including temporary staff and contractors whether current s or past.

4. Principles

- 4.1. We are open and transparent with supported children and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012.
- 4.2. We have and maintain policies to ensure compliance with the DPA18, Human Rights Act 1998, the common law duty of confidentiality, the GDPR and all other relevant legislation.
- 4.3. We have and maintain policies for the controlled and appropriate sharing of supported children and staff information with other agencies, taking account all relevant legislation and citizen consent.
- 4.4. Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time. We ensure that it is as easy to withdraw as to give consent.
- 4.5. We undertake regular audits of our compliance with legal requirements.

- 4.6. We acknowledge our accountability in ensuring that personal data shall be:
 - 4.6.1. Processed lawfully, fairly and in a transparent manner;
 - 4.6.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - 4.6.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
 - 4.6.4. Accurate and kept up to date;
 - 4.6.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
 - 4.6.6. Processed in a manner that ensures appropriate security of the personal data.
- 4.7. We uphold the personal data rights outlined in the GDPR;
 - 4.7.1. The right to be informed;
 - 4.7.2. The right of access;
 - 4.7.3. The right to rectification;
 - 4.7.4. The right to erasure;
 - 4.7.5. The right to restrict processing;
 - 4.7.6. The right to data portability;
 - 4.7.7. The right to object;
 - 4.7.8. Rights in relation to automated decision making and profiling.
- 4.8. To ensure that every individual's data rights are respected and that there are the highest levels of data security and protection in our organisation, we have appointed a member of staff to be our Data Security and Protection Lead (Lauren Poole). The Data Security and Protection Lead will report to the other founders of the organisation. Cottongrass Homes will support the Data Security and Protection Lead with the necessary resources to carry out her tasks and ensure that they can maintain expertise.
- 4.9. We require all staff to undertake mandatory training on information governance and security.
- 4.10. We consider personal data breach incidents and have a reporting mechanism that is communicated to all staff. We assess whether we need to report breaches to the ICO as the Regulator of DPA. We take appropriate action to make data subjects aware if needed.

5. Underpinning policies & procedures

- 5.1. This policy is underpinned by the following:

- 5.1.1. **Data Quality Policy** – outlines procedures to ensure the accuracy of records and the correction of errors (annexed here);
- 5.1.2. **Record Keeping Policy** – details transparency procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures), information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share (annexed here);
- 5.1.3. **Data Security Policy** – outlines procedures for the ensuring the security of data including the reporting of any data security breach (annexed here);
- 5.1.4. **Business Continuity Plan** – outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day to day running of our organisation;
- 5.1.5. **Staff Data Security Code of Conduct** - provides staff with clear guidance on the disclosure of personal information (annexed here).

6. **Data protection by design & by default**

- 6.1. We have appropriate organisational and technical measures to uphold the principles outlined above. We integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.
- 6.2. We uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.
- 6.3. All new systems used for data processing will have data protection built in from the beginning of the system change.
- 6.4. We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.
- 6.5. In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required (under law or in accordance with the terms of contracts agreed with local councils) for the purposes of processing or any other legal requirement to retain it.

6.6. Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and supported children, noting that in accordance with the GDPR and DPA18 such data remains protected. If the situation allows, data will be anonymised to fully protect an individual's data.

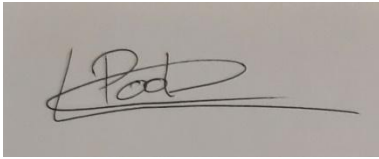
7. Responsibilities

7.1. Our designated Data Security and Protection Lead is Lauren Poole. The key responsibilities of the lead are:

- 7.1.1. To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the relevant legislation and principles;
- 7.1.2. To define our data protection policy and procedures and all related policies, procedures and processes and to ensure that sufficient resources are provided to support the policy requirements.
- 7.1.3. To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with senior management to fulfil this work.

8. Approval

8.1. This policy has been approved by the undersigned and will be reviewed at least annually.

Name	Lauren Poole
Signature	
Approval Date	1 November 2023
Review Date	

ANNEXURE 1

Data Quality Policy

Data Quality Policy Statement

Those we work alongside (“our partners”) must:

- submit complete and accurate data in their work with us
- ensure that a reasonable, minimum proportion of the data they submit to us can be validated by us
- be satisfied that the email address or contact details supplied for the purposes of contacting them is a reliable means of contact

Incomplete Data

Where data submitted is incomplete, we will contact the relevant partner to ensure that the additional and required data is supplied without delay.

Data Validation

Our partners must take appropriate steps to allow us to confirm that the data provided is valid if and when concerns regarding the validity of it are raised.

Updating this policy

We will review this policy on a regular basis in order to ensure that it continues to reflect best practice and current practices within the industry.

ANNEXURE 2

Records Management Policy

Introduction and Purpose

This policy sets out our commitment to achieving high standards in records management. Records management is vital to the delivery of our services in an orderly, efficient, and accountable manner. Effective records management will help ensure that we have the right information at the right time to make the right decisions. It will provide evidence of what we do and why, therefore protecting the interests of the company, our staff and all who interact with us.

We will create and manage records efficiently, make them accessible where possible, protect and store them securely and dispose of them safely at the right time.

By adopting this policy we aim to ensure that the record, whatever form it takes, is accurate, reliable, ordered, complete, useful, up to date and accessible whenever it is needed to:

- help us carry out our business;
- help us to make informed decisions;
- protect the rights of employees, regulated entities, and the public
- track policy changes and development;
- make sure we comply with relevant legislation;
- provide an audit trail to meet business, regulatory and legal requirements;
- make sure we are open, transparent and responsive; and
- promote our achievements.

Scope

This policy, applies to the management of all documents and records, in all technical or physical formats or media, created or received by Cottongrass Homes in the conduct of its business activities. It applies to all staff, contractors, consultants and third parties who are given access to our documents and records and information processing facilities.

Statutory and Regulatory Environment

Cottongrass Homes is a data controller with obligations set out in the Data Protection Act 1998.

Responsibilities

We have a responsibility to ensure that our records are managed well.

Data Security and Protection Lead is Lauren Poole

In addition, all staff, contractors, consultants and third parties - everyone who receives, creates, maintains or has access to our documents and records is responsible for ensuring that they act in accordance with this policy, standards guidance and procedures.

Relevant standards, guidance and procedures

This policy is supported by the standards set out below which detail best practice and serve as a reference when needed.

The table(s) below are intended to assist staff in implementing this policy and its supporting standards.

IF IN DOUBT REGARDING DATA AND THE LAWFULL USE OF IT (WHETHER THAT IS THE HOLDING OF IT, PROVISION OF IT, DESTRUCTION OF IT ETC) – SPEAK WITH LAUREN POOLE BEFORE ACTING

<i>Records relating to the children we support and staff</i>	
Description	<i>All documents which name or relate in any way to a child/young person or member of staff – whatever form the document takes (word/email/hand written etc)</i>
What types of documents can be kept	Only those that are adequate, relevant, and limited to what is necessary. All documents must be accurate.
Retention Period	<ol style="list-style-type: none"> 1. If the document relates to a child the document must be retained for the length of time specified by the contract under which we accommodated the child. 2. If the document relates to a member of staff it must be retained for 24 months after the date of their last working day with Cottongrass. However, one document must be maintained in relation to the staff member after this time to allow for the provision of a reference if and when requested. Such a document needs only to list: their name, dates of employment.
Disposition	<ol style="list-style-type: none"> 1. Electronic documents must be permanently deleted

	<p>2. Any hard copy documents must be shredded</p>
Storage	<p>Hard copy – any and all such documents are to be kept in the appropriate file within the locked office of the home the documents relate to – e.g. if child X lives in home A his/her documents must be kept in a file relating to child X in the locked office at home A</p> <p>Digital copies – all such documents are kept on a ‘cloud’ system. A system which is secure in accordance with the requirements of the Data Protection Act 1998.</p> <p>Access to documents is password restricted in accordance with the ideal of ‘Least Privilege’ – i.e. every member of staff is given only the least amount of access that they need to complete their job.</p>

ANNEXURE 3

Data Security Policy

1. Introduction

This policy is Cottongrass Homes' (hereafter referred to as "us", "we", or "our") policy regarding the safeguarding and protection of sensitive personal information and confidential information as is required by law (including, but not limited to, the Data Protection Act 2018, Health & Social Care Act 2012, and the Common Law duty of confidentiality).

2. Purpose

2.1. The purpose of this document is to outline how we prevent data security breaches and how we react to them when prevention is not possible. By data breach we mean a security incident in which the confidentiality, integrity or availability of data is compromised. A breach can either be purposeful or accidental.

2.2. This Data Security Policy covers:

2.2.1. Physical Access procedures;

2.2.2. Digital Access procedures;

2.2.3. Access Monitoring procedures;

2.2.4. Data Security Audit procedures;

2.2.5. Data Security Breach procedures.

3. Scope

3.1. This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes, but is not limited to, special categories of data.

3.2. This policy applies to all staff, including temporary staff and contractors.

4. Physical Access Procedures

4.1. Physical access to records shall only be granted on a strict 'Need to Know' basis.

4.2. During their induction each staff member will be trained on the safe handling of all information and will be taught the procedures which govern how data is used, stored, shared and organised in our organisation.

4.3. Our staff must retain personal and confidential data securely in locked storage when not in use.

4.4. All offices, when left unoccupied, must be locked.

4.8. An audit will be completed at least annually to ensure that information is secured properly and that access is restricted to those who have a legal requirement to use the information.

5. **Digital Access Procedures**

- 5.1. Access shall be granted using the principle of 'Least Privilege'. This means that every program and every user of the system should operate using the least set of privileges necessary to complete their job.
- 5.2. During their induction each staff member will be trained on the use of the system, given their user login details, and they will be required to sign to indicate that they understand the conditions of access.
- 5.3. In the instance that there are changes to user access requirements, these can only be authorised by Lauren Poole.
- 5.4. We will follow robust password management procedures and ensure that all staff are trained in password management.
- 5.5. As soon as an employee leaves, all their system logons are revoked.
- 5.6. As part of the employee termination process Lauren Poole is responsible for the removal of access rights from the computer system.
- 5.7. Lauren Poole will review all access rights on a regular basis, but in any event at least once a year. The review is designed to positively confirm all system users. Any lapsed or unwanted logons which are identified are disabled immediately and deleted unless positively reconfirmed.
- 5.8. When not in use all screens will be locked and a clear screen policy will be followed.

6. **Access Monitoring Procedures**

- 6.1. The management of digital access rights is subject to regular compliance checks to ensure that these procedures are being followed and that staff are complying with their duty to use their access rights in an appropriate manner.
- 6.2. Areas considered in the compliance check include whether:
 - 6.2.1. Allocation of administrator rights is restricted;
 - 6.2.2. Access rights are regularly reviewed;
 - 6.2.3. Whether there is any evidence of staff sharing their access rights;
 - 6.2.4. Staff are appropriately logging out of the system;
 - 6.2.5. Our password policy is being followed;
 - 6.2.6. Staff understand how to report any security breaches.

7. **Data Security Audit Procedures**

- 7.1. Confidentiality audits will focus on controls within electronic records management systems and paper record systems; the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of insufficient

controls. Audits of security and access arrangements within each area are to be conducted on a six-monthly rolling programme.

- 7.2. Audits will be carried out as required by some or all of these methods:
 - 7.2.1. Unannounced spot checks to random work areas;
 - 7.2.2. A series of interviews with management and staff, where a department or area of the organisation have been identified for a confidentiality audit. These audits will be carried out by Lauren Poole or the House Manager (under the guidance of Lauren);
 - 7.2.3. Based on electronic reports.
- 7.3. The following checks will be made during data security audits
 - 7.3.1. Failed attempts to access confidential information;
 - 7.3.2. Repeated attempts to access confidential information;
 - 7.3.3. Access of confidential information by unauthorised persons;
 - 7.3.4. Previous confidentiality incidents and actions, including disciplinary, taken;
 - 7.3.5. Staff awareness of policies and guidelines concerning confidentiality and understanding of their responsibilities with regard to confidentiality;
 - 7.3.6. Appropriate communications with service users;
 - 7.3.7. Appropriate recording and/or use of consent forms;
 - 7.3.8. Appropriate allocation of access rights to confidential information, both hardcopy and digital;
 - 7.3.9. Appropriate staff access to physical areas;
 - 7.3.10. Storage of and access to filed hardcopy service user notes and information;
 - 7.3.11. Correct process used to securely transfer personal information by any means
 - 7.3.12. Appropriate use and security of desktop computers and mobile devices in open areas;
 - 7.3.13. Security applied to PCs, laptops and mobile electronic devices;
 - 7.3.14. Evidence of secure waste disposal;
 - 7.3.15. Appropriate transfer and data sharing arrangements are in place;
 - 7.3.16. Security arrangements for recording access to manual files both live and archive
 - 7.3.19. Appropriate staff use of computer systems, e.g. no excessive personal use, no attempting to download software without authorisation, use of social media, attempted connection of unauthorised devices etc

8. Data Security Breach Procedures

- 8.1. In order to mitigate the risks of a security breach we will:

- 8.1.1. Follow the Physical Access, Digital Access, Access Monitoring and Data Security Procedures set out above;
- 8.1.2. Ensure our staff are trained to recognise a potential data breach whether it is a confidentiality, integrity or availability breach;
- 8.1.3. Ensure our staff understand the procedures to follow and how to escalate a security incident to Lauren Poole in order to determine if a breach has taken place.
- 8.2. In the instance that it appears that a data security breach has taken place:
 - 8.2.1. The staff member who notices the breach, or potential breach, will notify Lauren Poole without delay;
 - 8.2.3. Lauren Poole will begin an investigation into the breach;
 - 8.2.4. In the instance that the breach is a personal data breach and it is likely that there will be a risk to the rights and freedoms of an individual then the Information Commissioner's Office (ICO) will be informed as soon as possible, but at least within 72 hours of our discovery of the breach, via the DSPT Incident Reporting Tool (www.dsptoolkit.nhs.uk/incidents/);
 - 8.2.5. As part of our report we will provide the following details:
 - 8.2.5.1. The nature of the personal data breach (i.e. confidentiality, integrity, availability);
 - 8.2.5.2. The approximate number of individuals concerned and the category of individual (e.g. employees, mailing lists, service users);
 - 8.2.5.3. The categories and approximate number of personal data records concerned;
 - 8.2.5.4. Lauren Poole's full contact details;
 - 8.2.5.5. The likely consequences of the breach;
 - 8.2.5.6. A description of the measures taken, or which we will take, to mitigate any possible adverse effects.
- 8.2.6. Lauren Poole will inform any individual that their personal data has been breached if it is likely that there is a high risk to their rights and freedoms. We will inform them directly and without any undue delay;
- 8.2.7. A data security breach will prompt an audit of all processes in order to correct any procedure which led to the breach;
- 8.2.8. A record of all personal data breaches will be kept including those breaches which the ICO were not required to be notified about.

9. **Approval**

- 9.1. This policy has been approved by the undersigned and will be reviewed at least annually.



Name

Signature

Approval Date

Review Date

ANNEXURE 4

Staff Data Security Code of Conduct**Introduction**

Every member of staff that works for Cottongrass Homes, irrespective of their position, is required to promote and uphold the privacy, dignity, rights, health and wellbeing of the children/young people they support at all times.

Respecting the data rights of our children and fellow employees is of the utmost importance.

During your job you may be required to handle, collect, or share information of a sensitive nature relating to a child or another member of staff. ***It is vital that our policies and processes are followed when you handle personal information.*** This will ensure that your, your fellow employees and the children we support rights, dignity and wellbeing are upheld and promoted at all times.

Disclosure

You must not disclose, either during or after your employment here:

- i. any trade secrets e.g. financial & staff information or;
- ii. other sensitive personal information or confidential information, including but not limited to; a child's/young person's medical records, family background, family history, sexuality, ethnicity etc

Except where this is necessary for your job or if you are required to do so by law.

We provide training to all staff on data security and protection and proper information sharing. If you feel that you require more training, or if you have any questions or concerns, please contact **Lauren Poole**.

So that we can make sure that confidential information is accessed by those individuals that have a legitimate right of access, we undertake monitoring on a regular basis. Audits are also carried out with a view to discover whether confidentiality has been breached. It is important that you know that if we discover that our policies and procedures have been breached, this may result in disciplinary action including dismissal.

Lauren Poole should be your first contact point if you have any questions or concerns.

If you receive any request to disclose information about; a child/young person we support or have supported in the past or a current or past member of staff please discuss the request in full with **Lauren Poole** **BEFORE** making any disclosure.