



Cloch Housing Association

Data Protection Policy

Policy Name	Data Protection
Policy Category	GOV
Policy Number	067
Date Adopted	25/05/2018
Last Review	12/03/2019
This Review	2/6/2022
Next Review	June 2025
Equalities Impact Assessment Required	No
Link to other policies	Privacy Notice, Fair Processing Notice, Acceptable Documents Policy
Consultation	No
Need for Procedure	No

1. Introduction

The lawful and appropriate management of personal data is extremely important to Cloch Housing Association (Cloch).

This policy sets our commitment to protecting personal data and how we will implement this in regards to the collection and handling of personal data as defined in the following legislation:

- UK General Data Protection Regulation
- UK Data Protection Act 2018 (DPA2018)
- Privacy and Electronic Communications Regulations 2003 (PECR)

Failure to comply with data protection legislation could lead to financial penalties, regulatory action, as well as reputational damage.

2. Scope

The Policy applies to all personal data that Cloch holds relating to living identifiable individuals regardless of the category of data or the format of the data. Personal data is any data that could be used to identify a living individual e.g. name, address, email, postcode, CCTV image, photograph and video recordings. Special categories of personal data is any information about racial or ethnic origin, political opinions, religious beliefs, health (mental and physical), sexual health, trade union membership and criminal convictions.

The policy applies to personal data held or accessed on Cloch premises and systems or accessed remotely via home or mobile working. Personal data stored on personal and removable devices is covered by this policy.

3. The Data Protection Principles

Data protection laws describe how organisations must collect, handle and store all personal data. Ensuring compliance is underpinned by the following principles.

Personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay;
- 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;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition to these principles the law requires organisations to be responsible for, and must be able to demonstrate, compliance with the above principles.

4. Responsibilities for Compliance

Cloch's Voluntary Board are ultimately responsible for ensuring that Cloch meets its legal obligations however, the day to day management is delegated to the Leadership Team.

All staff have a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in line with this policy and the data protection principles.

The Data Protection Lead Officer (Head of Corporate Services) is responsible for monitoring compliance with this policy and the data protection legislation; managing personal data breaches and data subject rights; recording and maintaining appropriate records of processing activities and the documented evidence required for compliance.

Data Protection Officer (DPO): Cloch employs a consultant DPO to oversee all the strategic work we do on data protection and Freedom of Information.

5. Compliance

Cloch will comply with our legal obligations and the data protection principles by:

Processing Lawfully and Fairly

Cloch will ensure processing of personal data, and special categories, meets the legal basis as outlined in legislation. Individuals will be advised on the reasons for processing via a freely available Privacy Notice.

Where data subjects' consent is required to process personal data, consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the process for Data Subjects to withdraw consent will be simple.

Purposes

Personal data will only be used for the original purpose for which it was collected. These purposes will be clear to the data subject.

If Cloch wishes to use personal data for a different purpose, we will notify the data subject prior to processing.

Adequate and Relevant data

Cloch will only collect the minimum personal data required for the purpose. Any personal data discovered as excessive or no longer required for the purposes collected for will be securely deleted.

Any personal information that is optional for individuals to provide will be clearly marked as optional on any forms.

Accurate

Cloch will take reasonable steps to keep personal data up to date, where relevant, to ensure accuracy.

Any personal data found to be inaccurate will be updated promptly. Any inaccurate personal data that has been shared with third parties will also be updated.

Retention

Cloch will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data are outlined in the Register of Processing (ROPA).

Data will be disposed of in a responsible way to ensure confidentiality and security.

Security

Cloch will implement appropriate security measures to protect personal data.

Personal data will only be accessible to those authorised to access personal data on a 'need to know' basis.

Employees will keep all data secure, by taking sensible precautions and following the relevant Cloch policies and procedures relating to data protection.

6. Data Sharing

In certain circumstances Cloch may share personal data with third parties. This may be part of a regular exchange of data, one-off disclosures or in unexpected or emergency situations.

Appropriate security measures will be used when sharing any personal data.

Where data is shared regularly a contract with data protection addendum, or data sharing agreement will be in place to establish what data will be shared and the agreed purpose.

Cloch will consider all the legal implications of sharing personal data prior to doing so.

Data Subjects will be advised of any data sharing in the Privacy Notice.

7. Data Processors

Where Cloch engage Data Processors to process personal data on our behalf, we will ensure:

- Data processors have appropriate organisational and technical security measures in place;
- No sub-processors are used without prior written consent from Cloch;
- An appropriate contract or agreement is in place explaining the full requirements of the data processor.

8. Security Incident & Breach Management

Occasionally Cloch may experience a personal data breach; this could be if personal data is:

- Lost, for example via misplacing documents or equipment that contain personal data, through human error, or via fire, flood or other damage to premises where data is stored;
- Stolen; theft or a result of a targeted attack on our network (cyber-attack);

- Accidentally disclosed to an unauthorised individual;
- Inappropriately accessed or used.

All security incidents or personal data breaches will be reported and managed by the Data Protection Lead Officer.

The Information Commissioner's Office and the individuals affected will be notified promptly, if required.

All breaches will be managed under Cloch's Breach Management Procedures.

9. Individual Rights

Cloch will uphold the rights of data subjects to access and retain control over their personal data held by us.

Cloch will comply with individuals':

- **Right to be Informed** – by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.
- **Right to Access** – by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a Privacy Notice and how to execute this right.
- **Right to Rectification** – by correcting personal data that is found to be inaccurate. We will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies will be rectified without undue delay.
- **Right to Erasure** (also known as 'the right to be forgotten') - we will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.
- **Rights to Restrict Processing** - we will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right.
- **Right to Data Portability** – by allowing, where possible, data to be transferred to similar organisation in a machine-readable format.
- **Right to Object** – by stopping processing personal data, unless we can demonstrate legitimate grounds for the processing that override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defence of legal claims.

10. Privacy by Design

We have an obligation to implement technical and organisational measures to demonstrate that we have considered and integrated data protection into our processing activities throughout the organisation.

When introducing any new type of processing, particularly using new technologies, we will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and carry out a Data Protection Impact Assessment.

All new policies including the processing of personal data will be reviewed by the Data Protection Lead Officer and the ITC Manager to ensure compliance with the law and establish if a Data Protection Impact Assessment is required.

Advice will be provided by the Data Protection Lead Officer and the ITC Manager on conducting Data Protection Impact Assessments in line with Cloch's Data Protection Impact Assessment Procedure.

11. Training

All staff will be aware of good practice in data protection and where to find guidance and support for data protection issues.

Adequate and role specific training will be provided regularly to everyone who has access to personal data, to ensure they understand their responsibilities when handling data.

12. Breach of Policy

Any breaches of this policy, may be considered under the Cloch disciplinary procedures, and may result in disciplinary action being taken, including dismissal.

13. Monitoring and Reporting

Audits will be carried out to check compliance with the law, this policy and any relevant procedures.

An annual report will be put to the Board at the beginning of each financial year about the previous year stating any breaches, subject access requests or DP Impact assessments done, and highlighting any outstanding risks in relation to the processing of personal data.

14. Related Policies & Procedures

The following policies and procedures should be read with this policy:

- Subject Access Request Procedures
- Breach Management Procedures
- Legitimate Interest Assessment Procedures
- Data Privacy Impact Assessment Procedures
- Data Security Related Polices
 - Password Policy
 - Email and Internet Policy
 - Mobile Device User Agreement
 - Social Media Policy
 - Document Management Strategy
 - IT Disaster Recovery Plan

15. Policy Review

This policy will be reviewed at least every three years, although changes will be made to the policy during the three-year period if required to meet changes in legislation and to address any weakness identified in the policy.

Certificate

Organisation Name:

Cloch Housing Association Limited

Reference number:

Z1221458

Tier:

Tier 1

Start date:

9 June 2008

End date:

8 June 2023

This data controller states that it is a public authority under the Freedom of Information Act 2000 or a Scottish public authority under the Freedom of Information (Scotland) Act 2002

Data Protection Officer

Name: RGDP LLP

Address: One Edinburgh Quay
133 Fountainbridge
Edinburgh
EH3 9QG

Email address: info@rgdp.co.uk

Telephone number: 0131 222 3239

Publish Contact Details: Yes