Data Protection Policy

Overview

The Organisation (Community Renewal Trust) takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part o our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

The Organisation is a 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how the Organisation will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing, or storing personal data in the course of working for, or on behalf of, the Organisation.

It is intended that this policy is fully compliant with the 2018 Data Protection Act and GDPR (2018) legislation. If any conflict arises between those laws and this policy, the Organisation intends to comply with the 2018 Data Protection Act and the GDPR (2018) legislation.

Data Protection Principles

Personal data must be processed in accordance with six 'Data Protection Principles'.

It must:

- be processed fairly, lawfully and transparently.

Community Renewal Trust, 311 Calder Street, Glasgow,
G42 7NQ. Tel: **0141 423 7111**

• be collected and processed only for specified, explicit and legitimate purposes.

• be adequate, relevant and limited to what is necessary for the purposes for which it is

processed.

• be accurate and kept up to date. Any inaccurate data must be deleted or rectified.

without delay.

• not be kept for longer than is necessary for the purposes for which it is processed; and

• be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

How We Define Personal Data

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else or it could be created by us. It could be provided or created during the registration process

We may collect, store and use the following kinds of personal data:

(a) information about your computer and about your visits to and use of this website including your IP address, geographical location, browser type, referral source, length of visit and number of page views;

(b) information relating to any transactions carried out between you and us on or in relation to this website, including information relating to any contribution you make to us;

(c) information that you provide to us for the purpose of registering with us or signing a form or a petition e.g. your email address, phone number, address and other personal and health information when you sign

(d) information that you provide to us for the purpose of subscribing to our website services, email notifications and/or newsletters; and

(e) any other information that you choose to send to us.

How We Define Special Categories of Personal Data

'Special categories of personal data' are types of personal data consisting of information as

to:

- your racial or ethnic origin.
- your political opinions.
- your religious or philosophical beliefs.
- your trade union membership.
- your genetic or biometric data;
- your health.
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use some of these special categories of your personal data if required by the Homes for Health Project and in accordance with the law.

How We Define Processing

'Processing' means any operation which is performed on personal data such as:

• collection, recording, organisation, structuring, or storage.

• adaption or alteration.

• retrieval, consultation, or use.

• disclosure by transmission, dissemination or otherwise making available.

• alignment or combination; and

• restriction, destruction, or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

How Will We Process Your Personal Data?

The Organisation will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

We will use your personal data:

• for complying with any legal obligation; or

• if it is necessary for our legitimate interests (or for the legitimate interests of someone

else).

However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights below.

Community Renewal Trust, 311 Calder Street, Glasgow,
G42 7NQ. Tel: **0141 423 7111**

We can process your personal data for these purposes without your knowledge or consent.

We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data, you should be aware that we may not be able to progress your submission.

Examples of when we might process your personal data

We have to process your personal data in various situations.

For example:

- To ascertain whether you are eligible to submit a housing enquiry to the homes for health project.
- To monitor diversity and equality
- To monitor the health issues caused by housing in Govanhill.
- To report on housing issues caused by housing in Govanhill
- To respond to any enquiry, you have made.
- To report to our funders
- To contact you about being a potential case study in a report or press story.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

• where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent.

• where you have made the data public.

• where processing is necessary for the establishment, exercise or defence of legal claims.

We might process special categories of your personal data for the purposes in the above list. In particular, we will use information in relation to:

• your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;

Community Renewal Trust, 311 Calder Street, Glasgow,
G42 7NQ. Tel: **0141 423 7111**

Sharing Your Personal Data

By submitting information, you are agreeing to share your housing and health situation for use in campaigning with the Homes for Health project.

We will anonymise your case unless you have given us permission to use your name.

Organisation's Data Security and Data Retention policies.

Data submitted online will be stored using a secure and private cloud storage (Google Workspace) as our data processor.

The Organisation's Privacy Officer – Sheila Thomson is responsible for reviewing this policy and updating the Board of Trustees on the Organisation's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

You should not share personal data informally.

You should use strong passwords.

Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Privacy Officer – Sheila Thomson

How to Deal with Data Breaches

We have robust measures in place to minimise and prevent data breaches from taking place.

Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals,

then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact the Privacy Officer - Sheila Thomson immediately and keep any evidence you have in relation to the breach.

Subject Access Requests

Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to the Privacy Officer – Sheila Thomson who will coordinate a response.

If you would like to make a SAR in relation to your own personal data you should make this in writing to Privacy Officer Sheila Thomson. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

Your Data Subject Rights

• You have the right to information about what personal data we process, how and on what basis as set out in this policy.

• You have the right to access your own personal data by way of a subject access request (see above).

• You can correct any inaccuracies in your personal data. To do you should contact the Privacy Officer Sheila Thomson.

• You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to

process it for the purpose it was collected. To do so you should contact the Privacy Officer – Sheila Thomson.

• While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Privacy Officer – Sheila Thomson.

• You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

• You have the right to object if we process your personal data for the purposes of direct marketing.

• You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

• With some exceptions, you have the right not to be subjected to automated decisionmaking.

• You have the right to be notified of a data security breach concerning your personal data.

The Organisation follows the retention periods recommended by the Information Commissioner in its Employment Practices Data Protection Code. These are as follows, in the absence of a specific business case supporting a longer period

Document Retention period

In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Privacy Officer – Sheila Thomson.

You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

Community Renewal Trust, 311 Calder Street, Glasgow,
G42 7NQ. Tel: **0141 423 7111**

Client/Family Data

Community Renewal shall comply fully with the Caldicott Principles.

The Caldicott Principles:

I. Justify the purpose(s) of using confidential information.

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an

appropriate guardian.

II. Do not use patient-identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

III. Use the minimum necessary patient-identifiable information that is required

Where use of the patient-identifiable is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

IV. Access to patient-identifiable information should be on a strict need-to-know basis

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

V. Everyone with access to patient-identifiable information should be aware of their responsibilities

Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical employees – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

VI. Understand and comply with the law

Every use of patient-identifiable information must be lawful. Someone in each project handling patient information should be responsible for ensuring that the organisation complies with the legal requirements.

Any disclosure to a third party must comply with Caldicott Guardian principles. The transfer of such material, for instance through the mail, should be subject to the same level of security precautions as patient health records

If you have any questions about this privacy policy, questions about the treatment of your personal data, or if you wish to exercise any of your rights under GDPR legislation, please write to us by
email data.protection@communityrenewal.org.uk