Clearing House Data Protection and Information Sharing Policy 2019-2022

Contents

1. Introduction and Purpose

Clearing House collects and holds certain information on its clients and partners in order to successfully provide its service. The Clearing House service is used by homelessness organisations across London to submit applications for rough sleepers and former rough sleepers who they support in the provision of their own services. The information they submit to Clearing House is used to assess a client's eligibility, suitability and need for accommodation and support. Landlords (RPSHs) submit information about properties which form part of the RSI accommodation portfolio, also provided across London. It is these properties the accepted clients are matched to. Tenancy Sustainment Teams (TSTs) submit information about the current tenants on a quarterly basis.

Clearing House is committed to ensuring that all personal data that it stores will be dealt with in line with the Data Protection Act 2018[1] and EU General Data Protection Regulation (GDPR). To comply with the law, personal information will only be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures used by the Clearing House service.

This policy covers the Clearing House service, its managers, staff and volunteers.

As a matter of good practice, partner organisations and individuals working with the Clearing House, and who have access to personal information, will be expected to have read and comply with this policy.

2. Key Requirements

In line with the Data Protection Act 2018 principles, Clearing House will ensure that personal data will:

- Be processed fairly and lawfully
- Be processed for a specific purpose
- Be adequate, and relevant but not excessive
- Be accurate and kept up to date
- Be retained no longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA) unless the country has adequate protection for the individual

3. Definitions

a. "personal data"

Personal data means data which relates to a living individual who can:

(a) be identified from that data, or

[1] http://www.legislation.gov.uk/ukpga/2018/29/contents

(b) be identified from that data and other information which is in the possession of, or is likely to come into the possession of, the Clearing House[2]

Personal data includes any expression of opinion about the individual and any indication of the intentions of the Clearing House or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held is still "personal data".

The definition also specifically includes opinions about the individual, or what is intended for them.

The following is a non-exhaustive list of the types of data that Clearing House collects and holds which fall under the definition of personal data:

- Clients' personal information, including;
    - Unique identifiers (e.g. NINO)
    - Current address and housing history
    - Monitoring information (age, gender, etc.)
    - Support needs details
    - Contact details
    - Financial information (e.g. debts, benefits, etc.)
    - Details of other services involved in client support
    - Health details (physical and mental)
    - Offending history
    - Housing preferences
- Correspondence relating to referrals, nominations, transfer requests etc. (i.e. emails sent and received by CH team)

4. Data protection management and notification

The Clearing House will ensure that our details are registered with the Information Commissioner; we will notify and renew our notification on an annual basis. If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

5. Responsibilities

Overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of Clearing House this is the (Greater London Authority/St Mungos Board of Trustees).

The governing body delegates tasks to Clearing House. Clearing House is responsible for:

- understanding and communicating obligations under the Act
- identifying potential problem areas or risks
- producing clear and effective procedures

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes
- writing and regularly reviewing the data protection policy

All Clearing House staff and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

6. How we ensure data is:

a) Processed fairly and lawfully

Clearing House will be clear and open with individuals about the reasons for collecting, using and storing their personal data (as covered in section 6.b), and will seek consent to collect, use and store personal data for these purposes.

The Clearing House will not process personal data in a manner that causes unjustified detriment to the individual.

b) Processed for a specific purpose

Clearing House obtains personal data for one or more of the following reasons; to:

- determine a client's eligibility for the service
- determine the service's suitability for a client
- ensure the safety of support staff lone-working with clients
- appropriately match clients with a property that meets their needs and preferences
- be shared with specific partner agencies for the purpose of informing their assessments or decisions
- be shared with specific partner agencies to ensure that appropriate client support is provided
- enable us to contact partner agency staff and notify them of decisions
- monitor the service and its effectiveness

The overall reason for Clearing House to hold personal data on clients and their support workers is to enable to service to achieve its goals of assessing client' support and housing need and matching them appropriately to supported accommodation for rough sleepers as part of the Rough Sleepers Initiative (RSI).

c) Adequate, and relevant but not excessive

The Clearing House has a duty of care to its clients and partnership workers which requires us to collect sufficient personal data to ensure that appropriate decisions with regard to provision of services and support are made, and to ensure the safety and wellbeing of all involved in the RSI. However, there is also a legal requirement for the Clearing House to not hold more information than is necessary for these purposes.

The Clearing House will not obtain personal data that is not considered relevant to the purposes of section 6.b, and will regularly review the information that it collects to ensure this. Any irrelevant or excessive data provided to Clearing House will be deleted.

d) Accurate and up to date

Clearing House will take reasonable steps to ensure that the personal data that it holds is accurate and kept up to date.

Upon completion of a form providing personal data we will require clients and partnership workers to confirm that the information provided is accurate and complete.

Partnership workers will be given the facility to access the current records of their current clients in order to check that the information held is accurate. Workers will be encouraged to notify Clearing House of any inaccurate or out of data information held, and will be required to update and re-confirm the accuracy of existing data on a regular basis.

Clearing House staff will check and query any information held that is believed to be inaccurate or out of date; this may be done via email or telephone conversations. Records of any information gathered in this manner will clearly indicate how it was obtained, by whom, from whom and when.

e) Retained no longer than necessary

Clearing House will not retain personal data for any longer than is necessary in order to achieve its purpose. If it is identified that a piece of information in no longer required for any of the reasons given when it was collected, then this information will be deleted.

It should be noted that as one of the reasons that Clearing House collects personal information is related to statistical reporting and monitoring of the service, data may often be held beyond the end of a client's RSI tenancy.

Information is held on Clearing House on an ongoing basis. The reasons for this are:

- There is a possibility of clients returning to the service, and in that event the records of the service previously provided would be required to effectively provide support.
- Whilst a client is in receipt of an RSI service it will be necessary for their records to be kept in order to ensure the on-going provision of that service.
- Undertaking longitudinal analysis of pan London supported accommodation provision is essential to support the development of policies to alleviate homelessness for the GLA and other statutory agencies.

f) Processed in accordance with the rights of the data subject

This refers to the following rights:

- Right of access to a copy of the information comprised in their personal data
  This is referred to as a Subject Access Request. This right means that an individual may request and is entitled to be;
    - told whether any personal data is being processed

- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- given a copy of the information comprising the data; and given details of the source of the data
- See section 7 on Subject Access Requests for details about this process.

- Right to object to processing that is likely to cause or is causing damage or distress
  An individual has the right to object to the processing of their own personal data; they must do so in writing specifying why the data is causing unwarranted damage or distress. There are exemptions to this right, e.g. if the individual has consented to the processing of their data.

- Right to prevent processing for direct marketing
  Clearing House very rarely contacts clients directly, and has no current plans to do so. Should this change in the future we would comply with any client request to cease communication, in line with the Data Protection Act 2018.

- Right to object to decisions being taken by automated means
  The Clearing House uses a custom database system which uses some automated processes, however these are only ever applied to support human decisions, and the decisions themselves are not taken by automated means.
  There are no plans for this to change, however, where it to change in the future Clearing House would comply with the requirement to explain and/or reconsider this decision, as per the Act.

- Right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
  See section 6.d.
  If notified of inaccurate personal data, Clearing House will correct or delete it as appropriate within a reasonable timeframe.

- Right to claim compensation for damages caused by a breach of the Act

g) Subject to appropriate security measures

For operational and technical reasons some data may be duplicated and stored on St Mungos' own secure servers.
There are locks restricting access to the building, floor level and room where these servers are located, and staff must present their individual security card in order to gain access. Appropriate technical measures such as secure connections and firewalls are also in place and kept up to date.
The location of personal data saved to these servers can only be accessed by an authorised member of the Clearing House team who would have to access the network using their individual network account which is password protected.

All personal data held by Clearing House is stored electronically using the Salesforce platform[3]. Salesforce uses top-tier data centres to store data, and these include measures such as 24 hour security, site access controlled via biometric scanning, CCTV, secure network connections, firewalls, etc.[4]

The information held by Clearing House on the Salesforce platform can only be accessed by Clearing House staff. In order to access the data staff must first log in to the secure St Mungos network using their individual username and password, and then log in to the Salesforce system using a separate individual set of login details and passwords.

Clearing House access is allocated to individuals because of the specific role they work in. Workers may only use the system or look up information on the system where it is of direct use in the role for which they were granted access. Use of the system is monitored to ensure correct and appropriate use.

Users must never share their Clearing House log-ins, including their password, with any other person.

Organisations using Clearing House should have policies and processes in place to ensure that staff access data securely. For example, Clearing House should not be accessed on a computer which may be visible to clients of a service and should exercise caution in using mobile technology in public places.

Information should only be downloaded when necessary and where the file can be safely stored on a secure server. Downloaded data should be archived and destroyed in line with organisations' individual policies.

Clearing House aims to have a culture of security awareness. Staff receive the appropriate training in this area and understand the importance of data security.

h) Not transferred outside of the EEA unless there is adequate protection

Clearing House does not transfer personal data outside of the EU. The possible exception to this is where data is stored, via the Salesforce platform, in data centres in the United States of America. It should be noted that the data is not shared with or accessed by any partners in the US, it is only stored or transferred through the US.

In any case, Salesforce adheres to the US-EU Safe Harbour Framework[5] which is considered to constitute adequate protection under the Data Protection Act 2018.

7. Consent and exercising data subject rights

User Agreement
The partnership worker will sign up to user agreement when accepting a login for the Clearing House system. These will outline the terms within which the worker will operate, including the handling of data. Any breach of these terms will result in the access to the system being removed.

[3] https://trust.salesforce.com/trust/learn
[4] https://trust.salesforce.com/trust/learn/datacenters
[5] http://www.salesforce.com/uk/company/privacy/full_privacy.jsp

(a) Client consent
Obtaining client consent is a shared responsibility of all Clearing House users in inputting projects.
Consent should be obtained before someone is put onto Clearing House. When completing the referral form, workers will be requested to confirm that the client agrees for the referral and information in it to be submitted.

(b) Clients who refuse to give consent
If consent has not been secured, information can still be processed if it is in the legitimate interests of the data controller or the organisation adding information. There are times when information, including personal, sensitive information needs to be recorded on Clearing House without consent being given. It is important to record instances where consent was refused. Please see 4.2 below about clients' right to request that possessing of data ceases.

(c) Clients who withdraw consent at a later date
This will be considered under the amending or deleting data procedure below.

Subject Access Request
Under the data protection act 2018, individuals have the right to access the personal data that Clearing House holds about them. Anyone wishing to exercise this right should apply in writing to the Clearing House Manager, and should direct their application to ch@mungos.org or St Mungos, 3 Thomas More Square, Wapping, London, E1W 1YW. Your request may be for any or all of the following:

- to be told whether any personal data is being processed;
- to be given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- to be given a copy of the information comprising the data; and given details of the source of the data (where this is available)

If a specific piece of data is being sought this should be clearly stated. You will also be asked how you would prefer to receive the results of your request; in most cases an electronic copy is most appropriate.

Before a Subject Access Request is considered to have been received you will be required to provide proof of identification, in the form of a passport or similar document.

Once Clearing House has received all of the above we will seek to comply with the request as soon as possible and within the required 40 days from when all documents are received.

Amending or deleting data
Clients have the right to request have inaccurate personal data removed or corrected. If someone views their data or is told by a worker about some information on Clearing House which they think is inaccurate they can request this is removed. This request should be sent to the Clearing House team to be logged. The Clearing House team will ask an appropriate manager to investigate whether information is inaccurate and action will be taken accordingly.
An individual has the right to object to processing that is likely to "cause substantial damage or distress". In certain circumstances the processing of personal information may still continue when a client claims that it is causing them damage or distress because it is in the partnership workers legitimate interests.

If someone has asked for all their data to be removed from the system a short investigation about why this is will be undertaken by the Clearing House team and the main partnership workers in relation to the record (i.e. current or recent support workers). In some cases it will not be possible to remove a record from Clearing House as information is required to provide services and to help to support the individual to address their homelessness and support needs. The decision about removing or retaining a record will be made through consensus between the main partnership worker(s) and Clearing House staff. In the case of a decision not being reached the GLA will make the final decision on the best course of action to take. By adding data to Clearing House organisations agree that this information will be shared and that decisions about removing information will be made in conjunction with other services providers, Clearing House and the GLA who have final decision making authority.

Complaint
Clients should be able to make a complaint about workers recording information, or any other aspects of the service offered to them, by following individual organisations complaints processes. They may also choose to make a complaint to St Mungos about the Clearing House team and they can also contact the Information Commission if their complaint is specific to data recording.

8. Data Sharing

Data sharing is essential to the work of the Clearing House given our role as liaison between RSI partners and a conduit of client referrals between partners. Data sharing is essential to the way in which the RSI operates and the system that it relies on; without the sharing of personal data between Clearing House and our RSI partners the service objectives could not be achieved.

Clearing House seeks clients' consent to share necessary personal data at the point that their referral form containing said information is submitted to us. If consent is withheld or refused at this point we will not share the client's data with any partners, however neither will we be able to provide our service to the client in question.

In order for any RSI partner to gain access to the Clearing House system and input, edit or view information they must register with the Clearing House. The Clearing House will take appropriate steps to ensure that the agency is a legitimate RSI partner, and will provide guidance and training in the use of the system and the information that it contains prior to granting access. Access, if granted, will be given to named individuals, and the decision to do so is made on a case by case basis. If an individual working within a recognised RSI partner agency is granted system access they receive a set of log in details that are individual to them.

When a client is matched to a suitable accommodation Clearing House will share relevant personal data that is required in order for the RSI to function. This could include information such as a client's name, current address, financial information (i.e. income and debts), support needs information, etc. As part of this process, workers' details such as name, phone number, email address, etc. will also be shared in order to facilitate joint working between RSI partners.

Such data is routinely shared with our partner landlords (all of which are Registered Providers of Social Housing), and Tenancy Sustainment Teams (TSTs), which are also commissioned and monitored by the GLA, Clearing House's data controller and funder. In some cases information may also be shared with other referral agencies; however this is uncommon, and only likely to occur in instances whereby the client has ceased to be supported by the original referral agency and is now being supported by the agency with which we are sharing the information.

When completing a referral form, there is a degree of information sharing provided between referral agencies by default, however this is limited within each organisation with which Clearing House partners.

E.g. 1.
A client is engaged with support services at his hostel and also attends a day centre regularly. The two projects are run by *different* organisations. A worker at the hostel completes the first half of a referral form, and then leaves their job.

Because they belong to the same organisation other workers at the hostel will be able to view the incomplete referral and pick up where the original worker stopped. However, the client's workers at the day centre will not be able to see his referral information as they belong to a different organisation.

E.g. 2.
A client is engaged with support services at her hostel and also attends a day centre regularly. The two projects are run by the *same* organisation.
A worker at the hostel completes the first half of a referral form, and then leaves their job.

Because they belong to the same organisation both the other workers at the hostel and the workers at the day centre will be able to view the incomplete referral and pick up where the original worker stopped.

Information is only shared with landlords and TSTs at the point of nomination; this is the point at which Clearing House matches a client with a suitable property. When this happens the specific landlord which owns the property and the specific TST which covers that area are granted access to the data about that specific client. At no point is information made generally available to all partners or about all clients.

Access to shared information will continue for the specific partners involved in an individual's case until such time as the individual is no longer considered a client of that partner agency.

E.g. 1.
The referring agency will have access to the individual's data from the point that they input it on the Clearing House system, and for the duration of time that the individual is on the waiting list, and will continue to have access during the nomination process. Once the nomination has been successful and the individual has moved out of the referral agency's service and into an RSI property they are no longer considered to be a client of the referral agency, and so at the point that the tenancy starts the referral agency will no longer have access to the information held by Clearing House.

E.g. 2.
The landlord will be granted access to the individual's data when the nomination is first made. They with continue to have view only access to the information through the nomination process and whilst the individual is their tenant in the property. Once the tenancy ends and the individual moves to other accommodation, the landlord will no longer be able to view the information held by Clearing House.

Sharing information from Clearing House

Information from the CH system should not be shared with a worker or agency that cannot view or access that information for themselves. Clearing House should be contacted for advice if there are any doubts or concerns about information sharing.

Exceptional information sharing (outside of systematic data sharing for the agreed purpose of the service) such as to the police will only be agreed where a clear case is made involving the safety of the client or another individual or a serious crime, and the information cannot be obtained from other sources.

This is because of the consent clients give – for information to be shared to benefit them in terms of service provision.

When the police request information, the Clearing House team asks for a DPA form and a manager assesses the request on this basis and decides whether to refer the police to that service.

The Clearing House team do not generally respond to missing persons enquiries. This is not the purpose of the system. A search for information may be undertaken if there is there is a serious and immediate concern about the person.

9. **Dealing with a breach of this agreement**

If any user becomes aware of any misuse of Clearing House information they should inform the Clearing House team at St Mungos immediately. This includes any loss or unauthorised disclosure of personal data, damage or loss due to malicious software/hacking or disclosure to a person not entitled to receive information.

The Clearing House team will follow up any reports of a breach of this policy and the GLA will be informed. Initially those involved will be consulted by a manager from Clearing House team with a view to achieving a resolution that is acceptable to all concerned. If a reported breach is substantiated and deemed serious and significant by the GLA, the project or organisation concerned may have their access to Clearing House revoked.

10. Review

This policy will be reviewed every 3 years or when there is a significant change in the service, whichever comes first.