



Hackney Quest

1 Poole Road
London E9 7AE

Tel: (020) 8533 5480

www.hackneyquest.org.uk

e-mail: enquiry@hackneyquest.org.uk

DEVELOPING THE POTENTIAL OF YOUNG PEOPLE, FAMILIES AND THE COMMUNITY

Hackney Quest GDPR Privacy Policy

General Information

Hackney Quest (HQ) is committed to protecting the rights and privacy of individuals in accordance with **the UK General Data Protection Regulation (UK GDPR) which ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.**

HQ processes information about its staff, students and other individuals it has dealings with for a range of administrative purposes (e.g. to recruit and pay staff, administer programmes of activities and comply with legal obligations to funding bodies and government).

In order to comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Hackney Quest does not authorise any employee, volunteer or agent of Hackney Quest to hold or process any personal data on its behalf except as stated in task descriptions. Users of personal data on or off premises (e.g. pc at home or laptop) should consider the legal position before attempting to process personal data.

Our data protection officer is Karen Bance (karen@hackneyquest.org.uk).

Personal data we hold

Personal data that we may collect, use, store and share (when appropriate) includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Characteristics, such as ethnic background, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs

Data held is obtained from membership forms, volunteer registration, job applications, point of recruitment, and verbal communication. We may also hold data that we have received from other organisations, including schools, local authorities and other organisations.

Why we use this data

We use this data to:

- Support people
- Monitor and report on progress

UK GDPR PRIVACY POLICY

- Provide appropriate pastoral care
- Protect welfare
- Assess the quality of our services
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest (in our case, supporting young people)

Less commonly, we may also process personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using personal data overlap, and there may be several grounds, which justify our use of this data.

Collecting this information

While the majority of information we collect is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information in both electronic and paper formats. We may also keep it beyond attendance at our Head Office if this is necessary in order to comply with our legal obligations. The maximum period would be 10 years in accordance with LB Hackney's monitoring requirement.

Data sharing

We do not share information with any third party without consent unless the law and our policies allow us to do so.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Rights regarding personal data

■ **Request access** to your personal information (more commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. We do have to take into account the interests of others though, so this is not an absolute right.

■ **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

■ **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

■ **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a

UK GDPR PRIVACY POLICY

third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

■ **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

■ **Request the transfer** of your personal information to another party.

If you would like to make a request please contact our data protection officer, Karen Bance (karen@hackneyquest.org.uk).

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer, Karen Bance (karen@hackneyquest.org.uk).

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Other information

Only appropriate information will be requested from Volunteers/staff and the maintenance of records will aim to be factual, if an opinion is recorded we will aim to back that up with evidence, we will aim to only record information we would be happy for the data subject to see.

All confidential records will be disposed of safely e.g. shredded.

You should not disclose personal data to colleagues unless they have a legitimate interest in the data concerned. As there is no definition as to what a "legitimate interest" is, it will have to be a matter of judgment in each case. As a rule you should consider whether or not the information is necessary to allow your colleague to perform their task and the level of detail necessary.

References must contain factually correct information, sensitive data will not be disclosed without the explicit consent of the volunteer where opinions about a person's suitability are disclosed they must be defensible and justifiable on reasonable grounds.

If we are unable or unwilling to give a reference, such a refusal must be communicated carefully, without, in effect, implying a negative reference and thus disclosing personal data.

All confidential paper information, should ideally be cross shred onsite, bulk files will be shredded using an independent company and security certificate obtained.

For confidential, electronic information:

DVDs/CDs should be shredded and then put into the recycling stream.

UK GDPR PRIVACY POLICY

Computer hard drives and external storage media (such as USB sticks) should be wiped with a suitable software tool. No unencrypted data should be left on these types of media before re-using/recycling/disposal.

Media that cannot be wiped initially will need to be sufficiently protected before being overwritten e.g. locked filing cabinet

Reviewed: January 2024

Review: January 2026

Approved by: *Colette Allen* [Colette Allen, CEO and Safeguarding lead].