LHA Data Protection Policy

including Key Procedures

.

HEADING	SECTION CONTENT
Aims of this Policy	LHA London Ltd needs to keep certain information on its employees, volunteers, service users and trustees to carry out its day to day operations, to meet its objectives and to comply with legal obligations. The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will 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 within the organisation. This policy covers employed staff, trustees and volunteers.
Definitions	In line with the Data Protection Act 1998 principles, LHA will ensure that personal data will: • Be obtained fairly and lawfully and shall not be processed unless certain conditions are met • Be obtained for a specific and lawful purpose • Be adequate, relevant but not excessive • Be accurate and kept up to date • Not be held 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) The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer. The Information Commissioner sets out some guidance on the practical ways in which processing can be fair and lawful . We must; • have legitimate grounds for collecting and using the personal data; • not use the data in ways that have unjustified adverse effects on the individuals concerned; • be transparent about how we intend to use the data, and give individuals appropriate privacy notices when collecting their personal data; • handle people's personal data only in ways they would reasonably expect; and • make sure we do not do anything unlawful with the data.

	What is Personal Data? "*Personal data*" is non-trivial data that relates to a living individual who can be identified *either* from that data itself *or* from that data when combined with any other information which is in (or is likely to come into) the possession of the data controller. Conversely, if information has been sufficiently anonymised that no individual can be identified by it, even when joined with other data which the data controller has access to, it will not constitute personal data and the DPA will not apply to it. As well as letters, emails, and documents held in files and folders, personal data includes the following less obvious materials: • Photographs and video recordings • Voicemail recordings • Some SMS texts • Some minutes of meetings • CCTV images There is also a sub-category of personal data which is referred to in the DPA as "*sensitive personal data*". This is data which relates to an individual's: • political opinions • racial or ethnic origins • mental or physical health • sexual life • religious persuasion • trade union affiliation; or • or criminal record. The obligations imposed upon data controllers in relation to sensitive personal data are more onerous that those imposed in relation to personal data.
Responsibilities	Overall responsibility for personal data In LHA rests with the board of trustees. The Data Controller is responsible for: • specifying what the data can and cannot be used for • understanding and communicating obligations under the Act • identifying potential problem areas or risks • producing clear and effective procedures • notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes • monitoring compliance within LHA with policies and procedures • putting in place security measures such as encryption • dealing with any complaints All employed staff, trustees 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.

	Breach of this policy will result in appropriate disciplinary measures for employed staff, and potential termination of the volunteer agreement for volunteers. Staff and volunteers will have this policy included in their terms and conditions of employment or their volunteer agreement.
Policy Implement-ation	To meet our responsibilities staff and volunteers will: • only collect and process personal data in accordance with their authorisation to do so • Ensure any personal data is collected in a fair and lawful way; • Explain why it is needed at the start; • Ensure that only the minimum amount of information needed is collected and used; • Ensure the information used is up to date and accurate; • Review the length of time information is held; • Ensure it is kept safely; • Ensure the rights people have in relation to their personal data can be exercised We will ensure that: • Everyone managing and handling personal information is trained to do so. • Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do; • Any disclosure of personal data will be in line with our procedures. • Queries about handling personal information will be dealt with swiftly and politely.
Training	Training and awareness raising about the Data Protection Act and how it is followed in this organisation will take the following forms: On induction, we will run through the full policy with explanations and get a signature to ensure understanding. General training/ awareness raising: We will carry out regular refresher training every year.
Gathering and checking information	Before personal information is collected, we will consider: • What details are necessary for your purposes • How long we are likely to need this information We will inform people whose information is gathered about the following: • why the information is being gathered • what the information will be used for • who will have access to their information (including third parties) (in most cases, this is simply stated on the form that they complete) We will obtain all necessary consents to the intended uses when we collect the data. We will take the following measures to ensure that personal information kept is accurate: • due diligence and checking on collation of the data

	Personal sensitive information (about ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, criminal convictions) will not be used apart from the exact purpose for which permission was obtained.
Data Security	The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken: • Using lockable cupboards (restricted access to keys) • Password protection on personal information files • Setting up computer systems to allow restricted access to certain areas • Not allowing personal data to be taken off site (as hard copy, on laptop or on memory stick) • Back up of data on computers (onto a separate hard drive / onto tapes kept off site) • Entering into data processing and sharing agreements with any third parties using or processing data on our behalf • Ensuring any contractors or other third parties who may have access to data sign confidentiality agreements in advance e.g. people working on site or servicing IT systems Any unauthorised disclosure of personal data to a third party by an employee may result in appropriate disciplinary action. Any unauthorised disclosure of personal data to a third party by a volunteer or trustee may result in their removal. Any breach of data security will be investigated immediately and a report made to the Board. The Data Controller will decide whether a breach should be notified to the ICO, taking appropriate advice.
Subject Access Requests	Anyone whose personal information we process has the right to know: • What information we hold and process on them • How to gain access to this information • How to keep it up to date • What we are doing to comply with the Act. They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong. Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to Natasha Grant, HR, LHA London, 11 Belgrave Road, London SW1V 1RB We may make a charge of £10 on each occasion access is requested. The following information will be required before access is granted: • Full name and contact details of the person making the request

	• their relationship with the organisation (former/ current member of staff, trustee or other volunteer, service user • Any other relevant information- e.g. timescales involved We may also require proof of identity before access is granted. The following forms of ID will be required: • Passport • Driving license • National ID card Queries about handling personal information will be dealt with swiftly and politely. We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request and relevant fee.
Complaints	If you have a complaint about how we have handled your access request please write in the first instance to the person who handled your request stating exactly what your complaint is. Your complaint will then be forwarded to a member of senior management who will review your complaint and then reply within a reasonable timescale. This review and reply will be the final review available within our internal process.
Review	This policy will be reviewed at intervals of at least 3 years and sooner if there are any problems with the policy or security breaches to ensure it remains up to date and compliant with the law.