



# Lee Hub – Independent Community Library

## Data Protection Policy

### Contents

1. Aims .....	2
2. Legislation and Guidance .....	2
3. Definitions .....	2
4. The Data Controller .....	3
5. Roles and Responsibilities .....	4
6. Data Protection Principles .....	5
7. Collecting Personal Data .....	5
8. Sharing Personal Data .....	7
9. Subject Access Requests and Other Rights of Individuals .....	8
10. CCTV .....	10
11. Photographs and Videos .....	10
12. Data Protection by Design and Default .....	11
13. Data Security and Storage of Records .....	11
14. Disposal of Records .....	12
15. Personal Data Breaches .....	12
16. Training .....	12
17. Monitoring Arrangements .....	13
Appendix: Personal Data Breach Procedure .....	13

## 1. Aims

Lee Hub aims to ensure that all personal data collected about Trustees, volunteers, members and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy does not form part of any Trustee or volunteer's contract and we may amend it at any time.

## 2. Legislation and Guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) website.

It also reflects the ICO's Code of Practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and Charity constitution.

## 3. Definitions

Term	Definition
<b>Personal data</b>	<p>Any information relating to an identified, or identifiable, living individual. This may include the individual's:</p> <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li><li>• Location data</li><li>• Online identifier, such as a username</li></ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. It may also include expression of opinion about the individual or our intentions about the individual.</p>

<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> </ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.</p>
<b>Data subject</b>	<p>The identified or identifiable individual whose personal data is held or processed.</p>
<b>Data controller</b>	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
<b>Data processor</b>	<p>A person or other body, other than an employee or volunteer of the data controller, who processes personal data on behalf of the data controller.</p>
<b>Personal data breach</b>	<p>A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.</p>

#### 4. The Data Controller

Lee Hub processes personal data relating to Trustees, volunteers, members and others, and therefore is a data controller.

Lee Hub has paid its data protection fee to the ICO as legally required.

## 5. Roles and Responsibilities

This policy applies to all Trustees and volunteers carrying out duties within Lee Hub, and to external organisations or individuals working on our behalf. Individuals who do not comply with this policy may face disciplinary action.

### 5.1 Trustees

The Trustees have overall responsibility for ensuring that Lee Hub complies with all relevant data protection obligations.

### 5.2 Data Protection Lead

The Chair of Trustees, acting as Data Protection Lead (DPL) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Trustees and, where relevant, report to the board their advice and recommendations on data protection issues.

The DPL is also the first point of contact for individuals whose data Lee Hub processes, and for the ICO.

### 5.3 Chair of Trustees

The Chair of Trustees acts as the data controller on a day-to-day basis.

### 5.4 All Trustees and Volunteers

Trustees and Volunteers are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing Lee Hub of any changes to their personal data, such as a change of address
- Contacting the DPL in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals

- If they need help with any contracts or sharing personal data with third parties.

## 6. Data Protection Principles

The GDPR is based on data protection principles that Lee Hub must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

This policy sets out how Lee Hub aims to comply with these principles.

## 7. Collecting Personal Data

### 7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Lee Hub can fulfil a contract with the individual, or the individual has asked Lee Hub to take specific steps before entering into a contract
- The data needs to be processed so that Lee hub can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that Lee Hub can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of Lee Hub or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a child) has given explicit consent

- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a child) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

## 7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Volunteers must only process personal data where it is necessary in order to carry out their day-to-day activities within Lee Hub.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate and volunteers should notify us if their personal details change or if they become aware of any inaccuracies in the personal data we hold about them.

When trustees and volunteers no longer need the personal data they hold, they must ensure it is deleted or anonymised.

## 8. Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a child, vulnerable adult or other member that puts the safety of our trustees and volunteers at risk
- We need to liaise with other agencies - we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our volunteers and members - for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a contract with the supplier or contractor, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our members or volunteers.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

## 9. Subject Access Requests and Other Rights of Individuals

### 9.1 Subject Access Requests

Individuals have a right to make a 'Subject Access Request' to gain access to personal information that Lee Hub holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be shared with,
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The safeguards provided if the data is being transferred internationally
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested.

If volunteers or Trustees receive a subject access request in any form, they must immediately forward it to the DPL.

### 9.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children below 12 may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children above the age of 12 may not be granted without the express permission of the young person. This is not a



rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

### 9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of a child, young person, vulnerable adult or another individual
- Would reveal that the child, young person or vulnerable adult is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the individual's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

### 9.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, (in certain circumstances)
- Prevent use of their personal data for direct marketing

- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (e.g. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPL. If Trustees or volunteers receive such a request, they must immediately forward it to the DPL.

## 10. CCTV

We may use CCTV in various locations around Lee Hub to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. If in use, security cameras will be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

## 11. Photographs and Videos

As part of Lee Hub activities, we may take photographs and record images of individuals participating in our events.

We will obtain written media consent from all adults who agree to share their images on social media.

In addition, a media consent form is required for all parents / carers for photographs to be taken of children for communication, marketing, and promotional materials. When obtain parental consent, we will clearly explain how the photograph and / or video will be used to both the parent / carer and child.

Any photographs taken by members at Lee Hub events for their own personal use are not covered by data protection legislation. However, we will ask that photographs or videos of children / vulnerable adults are not shared publicly on social media for safeguarding reasons, unless all the relevant parents / carers (or adults where appropriate) have agreed.

Where Lee Hub takes photographs and videos, uses may include:

- within Lee Hub on notice boards and in Hub magazines, brochures, newsletters, etc
- outside of Lee hub by external agencies such as the newspapers or campaigns
- online on the Lee Hub website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child or vulnerable adult, to ensure they cannot be identified.

## 12. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPL, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Training for trustees and volunteers on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK and European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of Lee Hub and DPL and all information we are required to share about how we use and process their personal data
  - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

## 13. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on desks, tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, trustees must be aware that it is their responsibility to keep it secure

- Volunteers are reminded to change their passwords at regular intervals and not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Trustees and volunteers who store personal information on their personal devices are expected to follow the same security procedures as for Lee Hub-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

## 14. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out-of-date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on Lee Hub's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

## 15. Personal Data Breaches

Lee hub will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a Hub computer containing non-encrypted personal data about members.

If you consider that the data protection principles have not been followed in respect of personal data about yourself or others you should raise the matter with the DPL. Any breach of the GDPR will be taken seriously and may result in disciplinary action.

## 16. Training

All volunteers are provided with data protection training as part of their induction process.

A summary of the data protection regulations, together with practical examples, is included in the Volunteers Handbook.

Data protection will also form part of continuing development, where changes to legislation, guidance or Lee Hub's processes make it necessary.

## 17. Monitoring Arrangements

The DPL is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated annually and shared with the Lee hub Trustees.

## Appendix: Personal Data Breach Procedure

This procedure is based on guidance produced by the ICO.

- On finding or causing a breach, or potential breach, the member or volunteer must immediately notify the DPL.
- The DPL will investigate the report and determine whether a breach has occurred. To decide, the DPL will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people.
- The DPL will alert the Chair of Trustees.
- The DPL will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant volunteers where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPL will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPL will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPL will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation

- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPL must notify the ICO.

- The DPL will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPL will do this via the ['report a breach' page of the ICO website](#) or through their breach report line (0303 123 1113) within 72 hours . As required, the DPL will set out a description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPL
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPL will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPL expects to have further information. The DPL will submit the remaining information as soon as possible.

- The DPL will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPL will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach
  - The name and contact details of the DPL
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

As above, any decision on whether to contact individuals will be documented by the DPL.

- The DPL will notify any relevant third parties who can help mitigate the loss to individuals - for example, the police, insurers, banks or credit card companies.
- The DPL will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts relating to the breach
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

- The DPL will meet with the trustees to review what happened and how it can be avoided in the future. This meeting will happen as soon as reasonably possible.

### Actions to minimise the impact of data breaches

We will review the effectiveness of these actions and amend them as necessary after any data breach.

### Special category data (sensitive information) being disclosed via email (including safeguarding records)

- If special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error  
Volunteers who receive personal data sent in error must alert the sender and the DPL as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPL will ask the Network Manager (or someone in the IT Technician Team) to recall it
- In any cases where the recall is unsuccessful, the DPL will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPL will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPL will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

\*

### Version Control

V1: Created By Paul Twine	Date: 14 December 2020
V2: Reviewed by Christine McGrew	Date 21 <sup>st</sup> February 2022
V3: Reviewed by Christine McGrew	Date 18 <sup>th</sup> April 2024