General Data Protection Relation Policy (GDPR)

This policy works in conjunction with the Privacy Policy.

### Introduction

### We have updated our privacy policy to reflect the changes in the general data-protection relation laws (2018).

**GDPR Update 2022**

On 4 March 2022, the European Data Protection Board ("EDPB") published the final version of its adopted guidelines (the "CoC Guidelines") on using codes of conduct ("Codes") as appropriate safeguards for international transfers of personal data under the EU GDPR.

KASBAH abide by the following principles set by GDPR (March 2020):

**The Seven Principles**

1. Lawfulness, fairness and transparency.
2. Purpose limitation.
3. Data minimisation.
4. Accuracy.
5. Storage limitation.
6. Integrity and confidentiality (security)
7. Accountability

Four new additional rights under GDPR are:

**The right to be informed**. **The right of access**. **The right to rectification**. **The right to erasure**.

All personal data will be held in accordance with the principles and requirements of GDPR and other relevant legislation. Procedures have been put in place to ensure the fair processing of data subjects. KASBAH and all staff who process, or use personal data must ensure that they abide by these principles at all times.

Relevant data protection information will be included in all induction, staff/volunteer handbooks and training.

### Information held by KASBAH

Information held by KASBAH relates to individuals (volunteers, employees, board members, service users/members, potential staff, trainers and consultants, current, past and potential), voluntary and community organisations, other organisations (including those in the public and private sectors) which support, assist, provide services to, work within or alongside, or fund voluntary and community organisations or which KASBAH provide services to.

KASBAH will ensure that individuals know enough about how information held about them is used or disclosed. Information held about individuals will only be collected and recorded with good reason. It will be stored securely and for only as long as required.

The organisation will not give out information about any individual unless it is satisfied that the individual knows that this type of disclosure may be made and/or the information is already in the public domain (or that there is some over-riding reason for the disclosure).

Information about individuals will not be published in any type of directory without the written consent of the individual.

No details of individuals will be passed to other organisations for marketing, fundraising or circulating information unless the individual has been informed that this might happen and been given the opportunity to opt-in or opt-out as appropriate.

The web site will not contain any personal data that is not absolutely necessary. Where information is captured on the web site, a clear Cookies statement will be provided, and no personal data will be captured without the knowledge and permission of the data subject.

Photographs, recordings, videos or DVDs in which individuals are identifiable will only be used with their explicit written consent.

Manual files containing sensitive information about individuals will be labelled confidential and kept in locked filing cabinets, accessible only to relevant staff and the Chief Executive Officer.

Computer files containing sensitive information about individuals will be password protected, accessible only to relevant staff and the Chief Executive Officer. In addition professional anti-virus software will be installed and annually maintained to minimise the risk of corruption of data.

Information no longer required will be disposed of appropriately including ensuring that data is non-recoverable from any computer system.

**Employees**

The organisation requires all employees to comply with the GDPR in relation to the information about other staff. Failure to do so e.g. unauthorised, inappropriate or excessive disclosure of - or obtaining information about individuals, will be regarded as serious misconduct and will be dealt with in accordance.

The organisation operates a whistle-blowing policy, which gives effect to our wish that no employee should feel reluctant, for fear of management’s response, to give us information about wrongdoing within the organisation.

**Sharing of information:**

**\*No information would be released to any third party or international organisation unless it meets the below criteria.**

* **Police investigation requires KASBAH to participate with information on a subject.**
* **Pension auto enrolment (a legal requirement)**
* **Payroll company used by KASBAH to process NI & PAYE calculations.**
* **HMRC - when paying employee NI & Income tax based on salary**
* **Citation/Atlas – HR & Employment Law support**

### Personnel Records

The names and post held by staff within KASBAH are considered to be in the public domain and may be made freely available in any format to anyone.

The names, organisation and role held of Board members within KASBAH – and people seeking election or nomination as Board members – are considered to be in the public domain and may be made freely available in any format to anyone.

The address, telephone number, fax number, and email address of Board members shall be made available to staff and Board members only and only for the purpose of making contact in furtherance of KASBAH’s governance.

The home and mobile telephone numbers of staff are confidential but shall be made available to other staff members for the purpose of making contact in an emergency or urgent work related matter.

All material in respect of all applicants (other than the successful applicant), gained during the selection of staff or volunteers is confidential and shall be retained for twelve months after the effective start date of the staff member or volunteer, at which point it shall be destroyed.

All information required for the purposes of payroll is confidential and made available only to the Treasurer of the Board, the Chief Executive Officer and the Finance and HR staff. Information will be passed to statutory bodies if a legal requirement, such as in connection with tax and national insurance.

All other information within personnel records is confidential and can only be made available to the HR staff, Chair of the Board and the Chief Executive Officer. Personnel records are only used for matters connected with the individual’s employment at KASBAH or to help with references KASBAH might write in future at the individual’s request.

Information about age, gender, geographical location, ethnicity, sexual orientation, marital status and disability of staff, volunteers and Board members is kept for the purposes of monitoring our equal opportunities policy.

Current staff, volunteers and board members will be given full open access to their complete personnel records without question and without charge. Further details on access requests are within the ‘Access to Information’ section below.

**Databases of Organisations and other Contacts**

Data about individuals (including those who are contacts for organisations) shall be confined to contact details and information directly relevant to the reason for their inclusion on KASBAH’s databases. Other information about organisations may be held provided this is not personal data.

Information about age, gender, geographical location, ethnicity and disability of users (individuals and board members) will be kept confidential and password protected. The information is collected for the purposes of monitoring our equal opportunities policy and for reporting back to funders.

Data about individuals shall be deleted/destroyed on the request of the individual when the data is no longer used or required by KASBAH for legal, financial or contractual reasons.

KASBAH for shall only use data about individuals:

* Circulating KASBAH’s publications and other information about KASBAH and its work, via regular mailings to all on that particular database
* Direct marketing of KASBAH’s training, events or services to selected individuals/organisations, unless the individual/ organisation has opted out of receiving direct marketing
* Providing contact details for a specified organisation when requested or when it is considered that another organisation offers a service of benefit to users, unless that individual/organisation has requested that all or some of the contact details not be made available outside KASBAH
* Circulating information or direct marketing on behalf of another body on the grounds that it will potentially be of benefit to users and/or KASBAH’s charitable objects, unless the individual/organisation has requested that all or some of the contact details not be made available outside KASBAH
* Any other reason, which has been specifically agreed with that individual/organisation in advance.

Data about individuals shall not be used for direct marketing if the individual has exercised their right to opt out of this.

### Time Lines Set By KASBAH

**Personnel Files:**

* Current Employees – held and accumulated throughout period of employment
* Ex employees (normal circumstances) – records will be held for seven years in line with CQC requirements, then destroyed
* Applications for job vacancies – records will be kept for one year then destroyed
* Suitable candidates CVs kept on file – for one year then destroyed unless additional permission is given
* References requested by another employer – will be given up to five years of the finish date of employment with KASBAH

### General Office Files

* All administrative files to be reviewed every two years (older files/contacts/contracts/grant agreements can be kept for historical knowledge)
* Financial documents to be archived annually (by April of the following year) and stored for seven years then destroyed
* AGM agenda / minutes etc to be kept indefinitely (depending on significance)
* Board meeting and Sub Committee meeting minutes - to be kept for five years then destroyed
* House/Staff/Hive minutes – to be kept for three years then destroyed
* Chief Executive Officer and Manager reports - to be kept for three years then destroyed

**Member files**

* All files with a data protection consent slip can be kept until the member requests to be taken off our database and/or membership
* The member consent slip entitles KASBAH to hold information on the individual with the condition in addition to one Carer/parent, even if located at a different address
* Contents will be reviewed every two years, relevant documents will be kept for the life of the membership
* Any member no longer wishing to receive KASBAH correspondence will be edited in the database to not receive mailings but still be considered a member UNLESS they state otherwise and specify they no longer wish to be a member.
* Any deceased member file is to be kept in relation to family matters/circumstance for six months and then destroyed.

### Trainee / Day Service User Files/Outreach logs

* All current files – will be kept open for the duration of the training programme
* Outreach logs will be kept for three years (archived) and then destroyed.
* Ex trainee/Day service files – to be re-filed into the membership files and kept in line with the Data Protection Policy

**DIAL/Disability Assist**

* All current enquiry forms will be kept open for the duration of the disability application(s) and then deleted from all hardware systems in the next new financial year
* Every other year, all hard copies of enquiry forms filed can be shred in April.
* Once a year audit in April to remove enquiry forms from all DIAL desktops older than two years if they should be mis-saved.

### Database

* To be kept in line with members’ consent

## Access to Information

Data Subject Access requests should be made in writing and signed by the individual and addressed to the Data Protection Officer at KASBAH.

In response to a Data Subject Access request, KASBAH aims to disclose as much information as possible within 30 days, while respecting the right of any third party to maintain confidentiality wherever reasonable.

**How we safeguard personal information when taken off site**

Any company laptop taken off site are password protected, passwords are changed every 12 months and any sensitive paperwork must come back to the office the next day (inform an office manager the day before).

When hardware or paperwork is mislaid, report to the DPO in writing.

**How do we safeguard information held by the Trustees and how they store this?**

When information is given in paper format, these papers must be handed back to the manager at the end of the meeting to be shred (if this is a live meeting).

Any emails that are sent are password protected if there is a document attached and it is confidential.

**In the Event of Loss, Corruption of Damage to Data**

We maintain a high level of physical and electronic security in relation to the collection, storage and disclosure of your information. We take reasonable steps to ensure that any information we hold about you is protected.

In the event of loss, corruption or damage to personal data, the individuals involved will be notified as soon as this is discovered and appropriate steps to safeguard each person will be taken – this will be dependent on the specific situation.

**Information Commissioners Officer**

If the ICO think the organisation has not complied with its obligations they can give the organisation advice and ask it to solve the problem. They cannot award anyone compensation. Their main aim is to improve the information rights practices of organisations, where there is an opportunity for the ICO to do so.

They will not usually investigate concerns where there has been an undue delay in bringing it to their attention. You should raise your concerns with then within three months of your last meaningful contact with the organisation concerned.

**Breach of Confidentiality**

Serious breaches of confidentiality will be reported to the Information Commissioner’s Office (ICO) within 72 hours.

Please note that KASBAH does not meet the criteria for the [National Security Provisions](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/national-security-provisions/) in Part 3 of the DPA18 (and updated the [Guide to Intelligence Services Processing](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/)).

## Queries

In case of any queries or questions in relation to this policy please contact the KASBAH’s Data Protection Officer: Emma Carver (Chief Executive Officer) or Sophie Aiken (HR Manager) on 01474 536501.