## ico_master_blue_rgb_ DPIA – KASBAH General Processing of Data

This template follows the process set out in the DPIA guidance, and should be read alongside that guidance and the [Criteria for an acceptable DPIA](http://ec.europa.eu/newsroom/document.cfm?doc_id=47711) set out in European guidelines on DPIAs.

# Submitting controller details

|  |  |
| --- | --- |
| Name of controller | KASBAH |
| Subject/title of DPO | Personal information held on members, volunteers, staff. |
| Name of controller contact /DPO  (delete as appropriate) | Emma Carver |



# Step 1: Identify the need for a DPIA

|  |
| --- |
| Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. |
| This DPIA relates to the information collected and held by KASBAH for the following reasons:  Supporting KASBAH members/service users/their families with their individual needs.  Recruitment and personnel documentation relating to staff and holding this information in line with CQC guidelines.  Board and volunteer information  Processing of DBS checks for charity safeguarding |

# Step 2: Describe the processing

|  |
| --- |
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
| KASBAH will never share information unless it is with a statutory body and there is a duty of care and or safeguarding alert (unless it is with an outsourcing company such as payroll, pensions, Citation etc).  All personal information is locked away in a lockable cabinet in locked offices.  All computers are password protected and changed annually. Sensitive documents shared on email are password protected etc Emails are encrypted if sensitive information is included.  See the privacy and GDPR policies for the full breakdown.. |

|  |
| --- |
| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
| Yes specific forms hold special category and criminal office data.  Personnel information will be stored inline with CQC guidelines and policies.  KASBAH staff numbers are approx.. 55 and a large amount of ex staff to be kept for 7 years.  This covers the North Kent area. |

|  |
| --- |
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
| Employer of the individuals and supporter of the members with disabilities.  Each person is able to access their personal data that is held and are aware why we hold it and what is stored. This includes children and vulnerable people due to the H&SC setting and provision we offer.  There are no public concerns at present or prior concerns over this type of processing or security flaws.  Technology is checked regularly with monthly IT health checks undertaken. |

|  |
| --- |
| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly? |
| General personnel processing in line with CQC Regulation 7 ([Regulation 7: Requirements relating to registered managers | Care Quality Commission (cqc.org.uk)](https://www.cqc.org.uk/guidance-providers/regulations-enforcement/regulation-7-requirements-relating-registered-managers)  Member and family personal details to enable support and appropriate care to supported living residents. |

# Step 3: Consultation process

|  |
| --- |
| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
| We gain member, service user and staff feedback on a monthly basis. We ask for support at our AGM’s and publish the results. If there is a new member need, KASBAH endeavor to find a solution.  Regarding technology, we have an IT consultant to advise. |

# Step 4: Assess necessity and proportionality

|  |
| --- |
| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
| General personnel processing in line with CQC Regulation 7 ([Regulation 7: Requirements relating to registered managers | Care Quality Commission (cqc.org.uk)](https://www.cqc.org.uk/guidance-providers/regulations-enforcement/regulation-7-requirements-relating-registered-managers)  This is the most appropriate way to achieve this outcome.  We keep paperwork to a minimum when we can.  We process data in line with data protection legislation. We undertake data checks.  International transfers are not appliable.  All members have the option to cancel their membership and be removed from KASBAH database and filing systems as advertised on all membership forms.  All staff have the right to access their personnel files. |

# Step 5: Identify and assess risks

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| Any hack or phishing email that leave the organisation open to abuse or virus.  Loss of paperwork when removing from site.  Loss of hardware such as laptops when taken off site. | Possible  Possible  Possible | Significant  Remote  Remote | Medium however the anti virus does warn it may be unsafe  Low as sensitive paperwork is not removed from site  Low due to password protection changed regularly |

# Step 7: Sign off and record outcomes

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/position/date** | **Notes** |
| Measures approved by: | Emma Carver | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | Emma Carver | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: |  | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: | | |
| DPO advice accepted or overruled by: |  | If overruled, you must explain your reasons |
| Comments: | | |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: | S Aiken | The DPO should also review ongoing compliance with DPIA |