**Kafwa Data Protection Policy**

**Management Statement**

At Kafwa we take our responsibility to keep applicant information safe and secure. We aim to satisfy the UK Data Protection Act standards (Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) 2018 ) within our organisation and we will actively encourage and train our staff to ensure that data privacy is a key element of their role.

**Principles by which we manage our data.**

The following chart shows the guiding principles for our organisation.

|  |
| --- |
|   |

All information used within the organisation is managed in accordance to the HORUS model:

1. **H**eld securely

2. **O**btained fairly and efficiently

3. **R**ecorded accurately and reliably

4. **U**sed effectively and ethically

5. **S**hared appropriately and lawfully.

**Our standards**

We will abide by our ten point principle

1. All staff must have password protected hardware (laptops and desktops)

2. All staff phones must be password protected

3. The files where we store our applicant information must be password protected and access must be restricted to only those who need to see the information contained in the files.

4. We will only hold data on applicants (successful or otherwise) for 6 years.

5. We will only hold images and details of Identity documents and other sensitive data (passports, TB checks, Police checks, Government ID etc for 2 years)

6. We will only transfer data to third parties using secure means, typically encrypted files or file transfer such as WhatsApp or via Third Party data gateways.

7. We will let our data subjects gain access to the information we hold on them if they request it.

8. We will delete a data subjects’ information from our systems should they request it.

9. We will only ask for the information we need in order for us to carry out our business.

10. We will recognise the confidential nature of the information we hold and treat it with all due respect.