

1. Introduction

- 1.1. This Data Protection Policy is the overarching policy for data security and protection for **Khaya Project** (hereafter referred to as "us", "we", or "our").

2. Purpose

- 2.1. The purpose of the Data Protection Policy is to support the 7 Caldicott Principles, the 10 Data Security Standards, the Data Protection Act (1998), the General Data Protection Regulations (2016) and Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

- 2.2. This policy covers

- 2.2.1. Our data protection principles and commitment to common law and legislative compliance;
- 2.2.2. procedures for data protection by design and by default;

3. Scope

- 3.1. This policy includes in its scope all data which is stored, recorded or transferred either in hardcopy or digital copy and of which we can reasonably be stated to be either the data controller or data processor, this includes special categories of data.
- 3.2. This policy applies to all staff, including temporary staff and contractors.

4. Principles

- 4.1. We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012.

- 4.2. We will establish and maintain policies to ensure compliance with the Data Protection Act 1998, Human Rights Act 1998, the common law duty of confidentiality and the GDPR and Data Protection Action 2018, and all other relevant legislation.
- 4.3. We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation and citizen consent.
- 4.4. Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in the Data Quality Policy. We ensure that it is as easy to withdraw as to give consent.
- 4.5. We will undertake annual audits of our compliance with legal requirements.
- 4.6. We acknowledge our accountability in ensuring that personal data shall be:
 - 4.6.1. Processed lawfully, fairly and in a transparent manner;
 - 4.6.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - 4.6.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
 - 4.6.4. Accurate and kept up to date;
 - 4.6.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
 - 4.6.6. Processed in a manner that ensures appropriate security of the personal data.
- 4.7. We uphold the personal data rights outlined in the GDPR;
 - 4.7.1. The right to be informed;
 - 4.7.2. The right of access;

- 4.7.3. The right to rectification;
 - 4.7.4. The right to erasure;
 - 4.7.5. The right to restrict processing;
 - 4.7.6. The right to data portability;
 - 4.7.7. The right to object;
 - 4.7.8. Rights in relation to automated decision making and profiling.
- 4.8. **There is still uncertainty about how much of the social care sector needs to appoint a Data Protection Officer. As this role becomes clearer the CPA will provide more information on this topic.**

In line with legislation we will employ a Data Protection Officer (DPO) who will report to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise. We guarantee that the DPO will not be pressured on how to carry out their tasks, and that they are protected from disciplinary action when carrying out the tasks associated with their role.

5. Underpinning Policies & Procedures

These policies and procedures are recommendations which we have provided templates for based on our understanding of the draft Data Security and Protection Toolkit. It is up to each organisation to assess whether they are necessary – for example, there is no need to have a Network Security Policy if you do not have a network. If you have policies already which contain the same information but they have different names then that's fine.

- 5.1. This policy is underpinned by the following:
- 5.1.1. Data Quality Policy – outlines procedures to ensure the accuracy of records and the correction of errors;
 - 5.1.2. Records Management Policy – details the management of records from creation to disposal, this is inclusive of retention and disposal procedures;

- 5.1.3. Data Security Policy – outlines procedures for the ensuring the security of data including the reporting of any data security breach;
- 5.1.4. Network Security Policy – outlines procedures for securing our network;
- 5.1.5. Business Continuity Plan –outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of
- 5.1.6. hardcopy information necessary to the day to day running of our organisation;
- 5.1.7. Staff Confidentiality Code of Conduct - provides staff with clear guidance on the disclosure of personal information.

6. Data Protection by Design and by Default

The CPA recognises that this may well be very new to much of the sector. As more guidance if from the ICO on this topic we hope to be able to provide more guidance.

- 6.1. We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will take into account the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.
- 6.2. We shall uphold the principles of data protection by design and by default from the beginning of any data processing.
- 6.3. Any new high-risk data processing activities will be assessed by the DPO using a Data Privacy Impact Assessment (DPIA) before the processing will commence.
- 6.4. All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.

6.5. We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

6.6. In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

7. Responsibilities

7.1. Our designated Data Security and Protection Lead is **Ndumie Mafu**. The key responsibilities of the lead are:

7.1.1. To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles;

7.1.2. To define our data protection policy and procedures and all related policies, procedures and processes and to ensure that sufficient resources are provided to support the policy requirements.

7.1.3. To complete the Data Security & Protection Toolkit (DSP Toolkit) annually and to maintain compliance with the DSP Toolkit.

7.1.4. To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with the Senior Information Risk Owner (SIRO) and DPO to fulfil this work.

7.2. **Please bear in mind the note about re: DPOs.** Our Designated Data Protection Officer (DPO) is **Ndumie Mafu**, they can be contacted via email: khayaproject@btconnect.com; phone: **0208 554 7902**; or at the following address: **71 Wellesley Rd, Ilford IG1 4LJ**.

The key responsibilities of the DPO are:

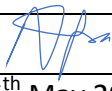
- 7.2.1. Overseeing changes to systems and processes;
 - 7.2.2. Monitoring compliance with the GDPR;
 - 7.2.3. Completing DPIA
 - 7.2.4. Reporting on data protection and compliance with legislation to senior management;
 - 7.2.5. Liaising, if required, with the Information Commissioner's Office (ICO).
- 7.3. Our Senior Information Risk Owner (SIRO) is **Ndumie Mafu**.

The key responsibilities of the SIRO are:

- 7.3.1. To manage, assess and mitigate the information risks within our organisation;
- 7.3.2. To represent all aspects of information and data protection and security to senior management and drive engagement in data protection at the highest levels of the organisation.

8. Approval

- 8.1. This policy has been approved by the undersigned and will be reviewed at least annually.

Name	Ndumie Mafu
Signature	
Approval Date	16 th May 2018
Review Date	TBA