Able2achieve Ltd
23-25 Princes Street, Yeovil, Somerset, BA20 1EN

## 1. Purpose

**1.1** The purpose of this policy is to ensure that Able2achieve Ltd and all its staff understand the principles set out in GDPR in relation to data retention and data security.
**1.2** By reviewing this policy, Able2achieve Ltd will be able to consider appropriate retention periods for the personal data it processes and ensure that it stores personal data for an appropriate period of time.
**1.3** This policy will enable Able2achieve Ltd and all staff working at Able2achieve Ltd to review the policies and procedures they have in place to ensure that personal data they process is kept secure and properly protected from unlawful or unauthorised processing and accidental loss, destruction or damage.
**1.4** To support Able2achieve Ltd in meeting the following Key Lines of Enquiry:

| Key Question | Key Lines of Enquiry |
|---|---|
| WELL-LED | W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed? |

**1.5** To meet the legal requirements of the regulated activities that {Able2achieve Ltd} is registered to provide:

- Data Protection Act 2018
- UK GDPR

## 2. Scope

**2.1** The following roles may be affected by this policy:

- All staff

**2.2** The following Service Users may be affected by this policy:

- Service Users

**2.3** The following stakeholders may be affected by this policy:

- Family
- Advocates
- Representatives
- Commissioners
- External health professionals
- Local Authority
- NHS

## 3. Objectives

**3.1** The objective of this policy is to enable Able2achieve Ltd to ensure that its data retention and data security policies are GDPR compliant.
**3.2** This policy will assist with defining accountability and establishing ways of working in terms of the use, storage, retention and security of personal data.

Able2achieve Ltd
23-25 Princes Street, Yeovil, Somerset, BA20 1EN

## 4. Policy

**4.1 Data Retention**

As a general principle, Able2achieve Ltd will not keep (or otherwise process) any personal data for longer than is necessary. If Able2achieve Ltd no longer requires the personal data once it has finished using it for the purposes for which it was obtained, it will delete the personal data unless it is required by law to retain the data for an additional period of time.

**4.2** Able2achieve Ltd may have legitimate business reasons to retain the personal data for a longer period. This may include, for example, retaining personnel records in case a claim arises relating to personal injury caused by Able2achieve Ltd that does not become apparent until a future date. Able2achieve Ltd should consider the likelihood of this arising when it determines its retention periods - the extent to which medical treatment is provided by Able2achieve Ltd will, for example, affect the likelihood of Able2achieve Ltd needing to rely on records at a later date.

**4.3** Able2achieve Ltd may be required to retain personal data for a specified period of time to comply with legal or statutory requirements. These may include, for example, requirements imposed by HMRC in respect of financial documents, or guidance issued by the Home Office in respect of the retention of right to work documentation (see the "Underpinning Knowledge" section).

**4.4** Able2achieve Ltd understands that claims may be made under a contract for 6 years from the date of termination of the contract, and that claims may be made under a deed for a period of 12 years from the date of termination of the deed. Able2achieve Ltd may therefore consider keeping contracts and deeds and documents and correspondence relevant to those contracts and deeds for the duration of the contract or deed plus 6 and 12 years respectively.

**4.5** Able2achieve Ltd will consider how long it needs to retain HR records. Able2achieve Ltd may choose to separate its HR records into different categories of personal data (for example, health and medical information, holiday and absence records, next of kin information, emergency contact details, financial information) and specify different retention periods for each category of personal data. Able2achieve Ltd recognises that determining separate retention periods for each element of personal data may be more likely to comply with GDPR.

Able2achieve Ltd may decide, however, that separating its HR records into different elements is not practical, and that it can determine a sensible period of time for which to keep the HR records in their entirety. The period of time that is appropriate may depend on the likelihood of a claim arising in respect of that employee in the future. If, for example, Able2achieve Ltd is concerned that an employee may suffer personal injury as a result of its employment with Able2achieve Ltd, Able2achieve Ltd may choose to retain its HR records for a significant period of time. If any such claim is unlikely, Able2achieve Ltd may choose to retain its files for 6 or 12 years (depending on whether the arrangement entered into between Able2achieve Ltd and the employee is a contract or a deed).

**4.6** Able2achieve Ltd will consider the following advice and guidelines when deciding for how long to retain HR data. Able2achieve Ltd acknowledges that the suggested retention periods below are based on guidance within relevant legislation:

- Immigration checks - two years after the termination of employment
- PAYE records - at least three years after the end of the tax year to which they relate
- Payroll and wage records for companies - six years from the financial year-end in which payments were made
- Records in relation to hours worked and payments made to workers - three years beginning with the day on which the pay reference period immediately following that to which they relate ends
- Records required by the Working Time Regulations:
  - Working time opt out - two years from the date on which they were entered into
  - Compliance records - two years after the relevant period
- Maternity records - three years after the end of the tax year in which the maternity pay period ends
- Accident records - at least three years from the date the report was made, or potentially longer if deemed appropriate given the possibility of ongoing relevance of the records

**4.7** Able2achieve Ltd will consider for how long it is required to keep records relating to Service Users. In doing so, Able2achieve Ltd will consider the data retention guidelines provided by the NHS, if applicable. Those guidelines can be accessed by using the link in the "Underpinning Knowledge" section.

If the NHS guidelines do not apply to Able2achieve Ltd, Able2achieve Ltd will determine an appropriate retention policy for Service User personal data. Able2achieve Ltd may choose to retain personal data for at least 6 years from the end of the provision of services to the Service User, in case a claim arises in respect of the services provided.

**4.8** Irrespective of the retention periods chosen by Able2achieve Ltd, Able2achieve Ltd will ensure that all personal data is kept properly secure and protected for the period in which it is held by Able2achieve Ltd. This applies in particular to special categories of data.

**4.9** Able2achieve Ltd will record all decisions taken in respect of the retention of personal data. Able2achieve Ltd recognises that if the ICO investigates the policies and procedures at Able2achieve Ltd, a written record of the logic and reasoning behind the retention periods adopted by Able2achieve Ltd will assist the position of Able2achieve Ltd.

**4.10** Able2achieve Ltd will implement processes for effectively destroying and/or deleting personal data at the end of the relevant retention period. Able2achieve Ltd will consider whether personal data stored on computers, including in emails, is automatically backed up and how to achieve deletion of those backups or ensure that the archived personal data is automatically deleted after a certain period of time. Able2achieve Ltd will consider circulating guidance internally to encourage staff to regularly delete their emails.

Able2achieve Ltd will introduce policies relating to the destruction of hard copies of documents, including by placing the documents in confidential waste bins or shredding them.

**4.11 Data Security**

Able2achieve Ltd will take steps to ensure that the personal data it processes is secure, including by protecting the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

**4.12** Able2achieve Ltd understands that all health and care organisations, as detailed below, are required to comply with the Data Security and Protection Toolkit. A link to an explanatory guidance note is included in the "Underpinning Knowledge" section. Compliance with the Data Security and Protection Toolkit facilitates compliance with GDPR.

Able2achieve Ltd understands that the following types of organisation must comply with the Data Security and Protection Toolkit:

- Organisations contracted to provide services under the NHS Standard Contract
- Clinical Commissioning Groups
- General Practices that are contracted to provide primary care essential services
- Local authorities and social care providers must take a proportionate response to the new toolkit:
  - Local authorities should comply with the toolkit where they provide adult social care or public health and other services that receive services and data from NHS Digital, or are involved in data sharing across health and care where they process confidential personal data of Service Users who access health and adult social care services
  - Social care providers who provide care through the NHS Standard Contract should comply with the toolkit. It is also recommended that social care providers who do not provide care through the NHS Standard Contract consider compliance with the toolkit as this will help to demonstrate compliance with the ten security standards and GDPR

**4.13** Able2achieve Ltd will implement and embed the use of policies and procedures to ensure that personal data is kept secure. The suggestions below apply in addition to the steps Able2achieve Ltd is required to take pursuant to the Data Security and Protection Toolkit, if the toolkit applies to Able2achieve Ltd.

Able2achieve Ltd will bear in mind the following principles when deciding how to ensure that personal data is kept secure:

- Confidentiality - ensuring that personal data is accessible only on a need to know basis
- Integrity - ensuring that there are processes and controls in place to make sure personal data is accurate and complete
- Availability - ensuring that personal data is accessible when it is needed for business purposes of Able2achieve Ltd
- Resilience - ensuring that personal data is able to withstand and recover from threats

For paper documents, these will include, where possible:

- Keeping the personal data in a locked filing cabinet or locked drawer when it is not in use

- Adopting a "clear desk" policy to ensure that personal data is not visible or easily retrieved
- Ensuring that documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them
- Redacting personal data from documents where possible
- Ensuring that documents containing personal data are placed in confidential waste bins or shredded at the end of the relevant retention period
- Minimising the transfer of personal data from outside of business premises and, where such transfer cannot be avoided, ensuring that the paper documents continue to be kept confidential and secure

For electronic documents, the measures taken by Able2achieve Ltd will include, where possible:

- Password protection or, where possible, encryption
- Ensuring that documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them
- Ensuring ongoing confidentiality, integrity and reliability of systems used online to process personal data (this may require a review of IT systems and software currently used by Able2achieve Ltd)
- The ability to quickly restore the availability of and access to personal data in the event of a technical incident (this may require a review of IT systems and software currently used by Able2achieve Ltd)
- Taking care when transferring documents to a third party, ensuring that the transfer is secure and the documents are sent to the correct recipient

Able2achieve Ltd will ensure that all business phones, computers, laptops and tablets are password protected.

Able2achieve Ltd will encourage staff to avoid storing personal data on portable media such as USB devices. If the use of portable media cannot be avoided, Able2achieve Ltd will ensure that the devices it uses are encrypted or password protected and that each document on the device is encrypted or password protected.

**4.14** Able2achieve Ltd will implement guidance relating to the use of business phones and messaging apps. Able2achieve Ltd understands that all personal data sent via business phones, computers, laptops and tablets may be captured by GDPR, depending on the content and context of the message. As a general rule, Able2achieve Ltd will ensure that staff members only send personal data by text or another messaging service if they are comfortable that the content of the messages may be captured by GDPR and may be provided pursuant to a Subject Access Request (staff should refer to the Subject Access Requests Policy and Procedure at Able2achieve Ltd for further details).

**4.15** Able2achieve Ltd will ensure that all staff are aware of the importance of keeping personal data secure and not disclosing it on purpose or accidentally to anybody who should not have access to the information. Able2achieve Ltd will provide training to staff if necessary. Able2achieve Ltd will consider in particular, the likelihood that personal data, including special categories of data, will be removed from the premises of Able2achieve Ltd and taken to, for example, Service Users' homes and residences. Able2achieve Ltd will ensure that all staff understand the importance of maintaining the confidentiality of personal data away from the premises of Able2achieve Ltd and take care to ensure that the personal data is not left anywhere it could be viewed by a person who should not have access to that personal data.

**4.16** Able2achieve Ltd will adopt policies and procedures in respect of recognising, resolving and reporting security incidents including breaches of GDPR. Able2achieve Ltd understands that it may need to report breaches to the ICO and to affected Data Subjects, as well as to CareCERT if Able2achieve Ltd is required to comply with the Data Security and Protection Toolkit.

**4.17** Able2achieve Ltd will adopt processes to regularly test, assess and evaluate the security measures it has in place for all types of personal data.

**4.18 Privacy by Design**

Able2achieve Ltd will take into account the GDPR requirements around privacy by design, particularly in terms of data security.

**4.19** Able2achieve Ltd understands that privacy by design is an approach set out in GDPR that promotes compliance with privacy and data protection from the beginning of a project. Able2achieve Ltd will ensure that data protection and GDPR compliance is always at the forefront of the services it provides, and that it will not be treated as an afterthought.

**4.20** Able2achieve Ltd will comply with privacy by design requirements by, for example:

- Identifying potential data protection and security issues at an early stage in any project or process, and addressing those issues early on; and
- Increasing awareness of privacy and data protection across Able2achieve Ltd, including in terms of updated policies and procedures adopted by Able2achieve Ltd

**4.21** Able2achieve Ltd will conduct Privacy Impact Assessments to identify and reduce the privacy and security risks of any project or processing carried out by Able2achieve Ltd. A template Privacy Impact Assessment is available within the Privacy Impact Assessment Policy and Procedure at Able2achieve Ltd.

## 5. Procedure

**5.1** Able2achieve Ltd will consider data retention and data security issues and concerns at the beginning of any project (whether the project is the introduction of a new IT system, a new way of working, the processing of a new type of personal data or anything else that may affect the processing activities at Able2achieve Ltd). Able2achieve Ltd appreciates that this is key for complying with the privacy by design requirements in GDPR.
**5.2** Able2achieve Ltd will review the periods for which it retains all the personal data that it processes.
**5.3** Able2achieve Ltd will, if necessary, adopt new policies and procedures in respect of data retention and will circulate those policies and procedures to all staff. Able2achieve Ltd will consider providing training to staff in respect of data retention.
**5.4** Able2achieve Ltd will review the security measures currently in place in respect of all the personal data it processes.
**5.5** Able2achieve Ltd will document the decisions it takes, and the logic and reasoning behind those decisions, in respect of both data retention and data security. Able2achieve Ltd will keep a record of all policies and procedures it implements to demonstrate its compliance with GDPR.

Able2achieve Ltd
23-25 Princes Street, Yeovil, Somerset, BA20 1EN

## 6. Definitions

**6.1 CareCERT**

- The Care Computing Emergency Response Team, developed by NHS Digital. CareCERT offers advice and guidance to support health and social care organisations to respond to cyber security threats

**6.2 Data Subject**

- The individual about whom Able2achieve Ltd has collected personal data

**6.3 Data Protection Act 2018**

- The Data Protection Act 2018 is a United Kingdom Act of Parliament that updates data protection laws in the UK. It sits alongside the General Data Protection Regulation and implements the EU's Law Enforcement Directive

**6.4 GDPR**

- **General Data Protection Regulation (GDPR)** (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It was adopted on 14 April 2016 and after a two-year transition period became enforceable on 25 May 2018. References to GDPR include references to the UK GDPR

**6.5 Personal Data**

- Any information about a living person including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV and special categories of data, defined below

**6.6 Process or Processing**

- Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending or transferring it. You do not need to be doing anything actively with the personal data - at the point you collect it, you are processing it

**6.7 Special Categories of Data**

- Has an equivalent meaning to "Sensitive Personal Data" under the Data Protection Act 2018. Special categories of data include but are not limited to medical and health records (including information collected as a result of providing health care services) and information about a person's religious beliefs, ethnic origin and race, sexual orientation and political views

**6.8 UK GDPR**

- The UK GDPR is the retained EU law version of GDPR that forms part of English law

## Key Facts - Professionals

Professionals providing this service should be aware of the following:

- Anybody who processes personal data on behalf of Able2achieve Ltd should be made aware of and should comply with the policies at Able2achieve Ltd in respect of data retention and data security
- Personal data will not be kept longer than necessary
- Personal data will be deleted when no longer needed
- Personal data may be held for longer than needed for the purposes of processing if there are justified reasons such as to meet regulations, insurance or other statutory requirements
- Retention periods are the decision of Able2achieve Ltd, but guidance
- All personal data will be kept securely
- All retention periods need to be documented and justified
- Able2achieve Ltd has effective and robust processes for destroying data
- Able2achieve Ltd will comply with the Data Security and Protection Toolkit when necessary
- Electronic devices will be password protected to aid security
- Documents containing personal data are only shared with people who need to know the content

Able2achieve Ltd
23-25 Princes Street, Yeovil, Somerset, BA20 1EN

## Key Facts - People affected by the service

People affected by this service should be aware of the following:

- Able2achieve Ltd will implement and embed the use of policies and procedures to ensure that all personal data processed about people affected by the services provided by Able2achieve Ltd, including you, is retained and is kept secure and protected in accordance with GDPR

## Further Reading

As well as the information in the 'underpinning knowledge' section of the review sheet we recommend that you add to your understanding in this policy area by considering the following materials:

The consultation for the draft Records Management Code of Practice 2020 has now concluded. The revised version of the code will be published once NHSx have analysed the responses and updated the code. Please note that the 2016 version is still valid until the new code has been finalised. This is cited above and is referenced in the Archiving, Disposal and Storage of Records Policy and Procedure. The link to the draft is here.

## Outstanding Practice

To be ‘ outstanding ’ in this policy area you could provide evidence that:

- You have considered the personal data you process and adopted and documented appropriate retention periods for each type of personal data
- You have reviewed the security measures in place in respect of the personal data Able2achieve Ltd processes
- You have reviewed and considered the documents and guidance referenced in the "Underpinning Knowledge" and "Further Reading" sections
- The wide understanding of the policy is enabled by proactive use of the QCS App