DATA STORAGE POLICY

Document control

Audience	Internal colleagues, External colleagues, Customers, External Quality Assurance bodies and regulators
Application	This policy applies to all Achieve+Partners personnel and bodies that work it
Version	1.0
Published	1st January 2020
Document status	Published
Responsibility	The Operations Director is accountable for ensuring the implementation of this policy. All Achieve+Partners employees are responsible for carrying out the requirements of this policy.

Document change record

Changes to specific sections of the document are listed below:

Page	Section	Change
None to date		

SECTION 1: POLICY

1.1 Introduction

Achieve+Partners is committed to ensuring that data is stored securely and in an accessible way for its workforce. All data is held in line with the Data Protection Act and systems used within the company provide a secure platform to store data.

1.2 Purpose

This policy sets out Achieve+Partners specific approach to the storage of data it processes and in particular details the security arrangements of systems used.

1.3 Scope

This policy is relevant to all employees and contractors of Achieve+Partners Business. The policy covers arrangements for the storage of data across the business.

This policy does not include arrangements for the protection of data under the Data Protection Act. Details of this can be found in the Achieve+Partners Data Protection Policy. Furthermore, arrangements for the control of documents used within the company are provided in the Document Control Policy.

1.4 Responsibility

Employees of Achieve+Partners should be aware of the requirements for the storage and security of records relating to the registration and certification of learners and all documentation referring to centres.

Achieve+Partners are responsible for:

1. Ensuring all records are:
   - accurate
   - legible
   - up to date
   - securely stored and not disclosed to any unauthorised persons
   - made available for external quality assurance and auditing by relevant regulatory authorities and that they allow for learner achievements to be monitored and reviewed in relation to the centre’s equal opportunities policy
   - retained in-line with the Data Protection Policy

2. Identifying learners who may require reasonable adjustments to the assessment process and applying to Achieve+Partners for authorisation to implement special assessment arrangements.
3. retaining reports, certification data and other materials representative of the continuing compliance of centres in-line with the Data Protection Policy
4. Using only Achieve+Partners approved data storage facilities and software for data generated through the activities of the organisation

1.5 Security

Server

All Achieve+Partners electronic information is stored on the Microsoft 365 OneDrive.

Microsoft engineers administer OneDrive using a Windows PowerShell console that requires two-factor authentication. When data transits into the service from clients, and between datacenters, it is protected using transport layer security (TLS) encryption. Each file is encrypted at rest with a unique AES256 key. These unique keys are encrypted with a set of master keys that are stored in Azure Key Vault. Microsoft datacenters are geo-distributed within the region and fault tolerant. Data is mirrored into at least two different Azure regions, which are at least several hundred miles away from each other, allowing us to mitigate the impact of a natural disaster or loss within a region.

Microsoft 365

The senior management team and associated personnel currently make full use of Microsoft 365 to carry out daily activities. Copies of all documentation created is held on the Achieve and Partners server. This gives Achieve+Partners advanced protection from viruses and cybercrime, tools to help keep information secure and private, and ways to recover files from malicious attacks.

Laptops

Achieve+Partners employees who are issued with company laptops.

- Laptops are username and password protected.
- Passwords must be a minimum of 6 characters long and a mixture of letter and numbers at minimum, it is recommended that at least one symbol is also included.
- No passwords must be disclosed to other parties.
- Passwords should be changed every 6 months.
- Laptops are not to be used by anyone outside the organisation.

- No unauthorised software to be downloaded onto laptops.
- Anti-virus software must be kept up to date and a system scan should be run at least once per month.

Mobile Phones

Achieve+Partners employees who are issued with phones to be used for business purposes emails and contacts are synced from the users 1&1 Ionos account. All phones must be encrypted with an alphanumeric passcode (as recommended as the most secure method).

The passcode must be a minimum of 6 characters long and must be a mixture of letter and numbers at minimum, it is recommended that at least one symbol is also included. It is also recommended that settings are updated to delete data after 10 failed passcode attempts.

All users must have a connected Cloud account with back up of emails and contacts disabled. Find my phone must be enabled. This will enable all data to be deleted remotely if the phone is lost or stolen.

Bring your own device

See Achieve+Partners Bring Your Own Device Policy.

Emails

The Achieve+Partners emails are hosted by 1&1 Ionos https://www.ionos.co.uk/

Wordpress

The Achieve+Partners website is hosted by 1&1 Ionos Wordpress online enquiries are received and stored via the website. All enquiries must be deleted on a monthly basis by the Operations Director. Wordpress have issued a GDPR compliance statement. The website is protected by an SSL Certificate.

ACE360 Apprenticeship Management system

Achieve+Partners implements the ACE360 secure apprenticeship management system to manage registrations, Gateway, the end-point assessment outcomes, re-sits, certification claims and data requests. The ACE360 system integrates with ESFA certification system to claim certificates. ACE360, although a cloud-based system, sits behind at least two firewalls at all times both physical and software based.

They take all reasonable steps to protect data by implementing:

- A lock out system
- Data is captcha protected
- Brute Force Protection
- Secure password and data reset options
- Regular penetration testing by a trusted IT security company
- Cyber essentials certified.

Booking System

Achieve+Partners uses Knack to host the EPA Booking Portal. To ensure our data is secure at all times, all data is encrypted at rest as well as in transit. This means even if someone were able to access the data through an attack of some sort, it is indecipherable. Additionally, Knack use the highest security options available via Amazon Web Services. AWS is considered an industry leader in cloud services and is trusted by organizations like DOW Jones, Pfizer, and the CDC.

Finally, secure user access is a feature we use on the app. This prevents open access to data and requires users to authenticate to access restricted areas of the application. For more information on Knack's security and the steps they take to ensure our data is secure at all times, please take a look here: Security and Infrastructure.

Online testing

Achieve and Partners has an online exam system, we use the Easy LMS system for this purpose. This includes built-in security features such as data encryption, XSS prevention and data sanitisation. User input data is always validated on the server, even if client-side validation is also used. Easy LMS runs on an Amazon Web Services cloud, or AWS for short. The servers and databases are physically located in Frankfurt, Germany.

1.6 Control of data

Accessing Data

Electronic data is held securely on the Achieve and Partners server and is password protected to only allow access to authorised personnel. The server and all computers are firewall protected.

Archived Data

All archived electronic data is held securely on the Achieve and Partners server and is password protected to only allow access to authorised personnel. No hard copy personal data is archived.

All financial, assessment and quality assurance documentation is held securely for 7 years to support legal and regulatory obligations.

Deleting Electronic Data

Data must be deleted securely using a software programme (such as CCleaner) that enables secure deletion using an advanced overwrite of at least 3 passes to ensure that any deleted data cannot be recovered. It is recommended that all employees run the secure deletion programme at least once per month on their laptops.

Deleting Hard Copy Data

Hard copy data must be securely destroyed, for example by shredding before safe disposal.

1.7 Data Protection Impact Assessments (DPIA)

Achieve and Partners will carry out a DPIA if we plan to:

+ Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
+ Process special category data or criminal offence data on a large scale.
+ Systematically monitor a publicly accessible place on a large scale.
+ Use new technologies.
+ Use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit.
+ Carry out profiling on a large scale.
+ Process biometric or genetic data.
+ Combine, compare or match data from multiple sources.
+ Process personal data without providing a privacy notice directly to the individual.
+ Process personal data in a way which involves tracking individuals’ online or offline location or behaviour.
+ Process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
+ Process personal data which could result in a risk of physical harm in the event of a security breach.

We consider carrying out a DPIA if we plan to carry out any other:

- Evaluation or scoring.
- Automated decision-making with significant effects.
- Systematic monitoring.
- Processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing involving preventing data subjects from exercising a right or using a service or contract.

If we decide not to carry out a DPIA, we will document our reasons. We consider carrying out a DPIA in any major project involving the use of personal data. We will carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

All DPIA's completed will be published on the Achieve and Partners secure website area as recommended by the Information Commissioner's Office.