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	4.0
Published	16th December 2021
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
5	1.5	Updated email section

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 and Emails

All Achieve+Partners electronic information is stored on the Microsoft 365 OneDrive. The Senior Management Team have access to the server which is controlled by the Operations Director. The Achieve+Partners emails are hosted by Microsoft 365.

Microsoft engineers administer OneDrive using a Windows PowerShell console that requires two-factor authentication. When data transits into the service from clients, and between datacentres, 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 datacentres 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 Business Premium 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 or use laptops to access Achieve+Partners systems.

+ 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.
+ All applications on laptops must be supported by a supplier that produces regular fixes for any security problems.
+ All high-risk or critical security updates for operating systems and firmware must be installed within 14 days of release and auto-updates enabled where possible.

Mobile Phones

Achieve+Partners employees who are issued with phones to be used for business purposes emails and contacts are synced from the users Microsoft 365 account.

+ All phones must be encrypted with an alphanumeric passcode (as recommended as the most secure method).
+ Only verified applications are to be downloaded onto phones.
+ No unauthorised applications are to be downloaded onto phones.
+ All applications on mobile devices must be supported by a supplier that produces regular fixes for any security problems.
+ All high-risk or critical security updates for operating systems and firmware must be installed within 14 days of release and auto-updates enabled where possible.
+ 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.

Website

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 UK GDPR compliance statement. The website is protected by an SSL Certificate.

The website is protected by the Wordfence plugin from various hacking attempts. It comprises of malware scanner and firewall to safeguard our site from security threats including:

+ Hacking
+ Malware
+ Brute Force attacks &
+ DDOS

The firewall further filters visitors clicking into our website and obstructs doubtful requests. And the malware scanner scans everything:

+ Core Files
+ Plugins
+ Themes
+ Doubtful Codes
+ Folders uploaded for transformations etc

Rogo

Achieve+Partners uses the Rogo system to manager learners, qualifications, EPA bookings and online testing and assessments.

Rogo by Eintech has been designed from the ground up to ensure very high data security. Rogo uses Microsoft's Azure for the highest level of security.

+ Physical security provided by Microsoft – data centres trusted by the U.S. Department of Defence
+ Data encrypted in transit and at rest
+ Data masking at database level
+ Customisable permission roles and eligibility
+ Grant permissions to individual qualifications or even units
+ Hidden if no access – areas that user has no permission for are completely hidden
+ Audit logs and access tracking

- Anti-malware
- Custom password security rules – including length, number of special characters, change frequency, auto-lockout, etc.
- Zero footprint settings – stop users downloading content to local machines
- Machine learning to protect against malicious attacks
- Intrusion detection and distributed denial-of-service (DDoS) attack prevention
- Weekly vulnerability audits
- Regular penetration testing

Eintech is ISO9001, ISO27001, and ISO22301 certified. They self-certify against CyberClear and have Cyber Essentials Plus certification.

Passwords

All users must use non-guessable passwords and are not permitted to use the same password for multiple accounts. Passwords must not be written down on paper. Passwords may be stored on the users laptop and users can use a password manager.

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 by 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 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.

Offline Back up

The Operations Director is responsible for creating, updating and holding an offline back up of the Achieve+Partners Server. This is backed up bi-weekly on an external hard drive specifically purchased for this purpose.

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 Hub as recommended by the Information Commissioner's Office.

SECTION 2 CYBER SECURITY INCIDENTS OR NEAR-MISSES

2.1 Cyber incidents

Where a significant cyber incident occurs, we will report this to the National Cyber Security Centre (the NCSC) and implement our Incident Management Plan.

The NCSC defines a cyber security incident as:

- A breach of a system's security policy in order to affect its integrity or availability
- The unauthorised access or attempted access to a system

Cyber incidents can take many forms, such as denial of service, malware, ransomware or phishing attacks.

Incidents that are not considered significant and those that might lead to a heightened risk of individuals being affected by fraud, will be reported to Action Fraud – the UK's national fraud and cybercrime reporting centre.

2.2 Reporting cyber security incidents or near-misses to Ofqual

Achieve+Partners will notify Ofqual of any cyber incidents or near-misses that we or our centres experience that affect the development, delivery and award of regulated qualifications. We will notify Ofqual as soon as we become aware of a cyber security incident or near-miss, where we believe that there is a potential or actual Adverse Effect e.g. any suspicious activity on your networks or where personal, sensitive, or classified data held by you or your centres, may be compromised.

These incidents could be the result of a deliberate a cyber-attack, or series of attacks, or they could equally be the result of unintended or accidental action such as the sharing of sensitive information through a wide distribution list. Whether deliberate or accidental, we will still report all incidents where Adverse Effects are likely to or have occurred.

We will notify Ofqual of the following information:

- How many candidates were/are affected, and how?
- How many centres were/are affected, and how?
- How many separate attacks there have been and the nature of those attacks?
- The nature and extent of the loss of data/evidence/information, such as assessment materials and qualification results.
- The potential or actual impact on our ability to develop, deliver and award your qualifications.

- Any concerns we may have about the centres' ability to meet their contractual agreements with us, in their delivery of qualifications and assessments.
- The extent to which any lost materials/data may constitute a GDPR breach, and confirmation that the centre/s have reported this through the appropriate channels.

2.3 Reporting a breach to the Information Commissioners Office (ICO)

There are certain incidents that we need to tell ICO about. This includes a personal data breach under the GDPR or the Data Protection Act 2018.

If we believe there has been a personal data breach we will complete a self-assessment to help determine whether we need to report to the ICO. If we are required to report the breach to the IOC we will call and provide the following information:

- what has happened;
- when and how you found out about the breach;
- the people that have been or may be affected by the breach;
- what you are doing as a result of the breach; and
- who we should contact if we need more information and who else you have told.

2.4 Centres

Centres must report any cyber security incidents, near-misses or data breaches that affect the delivery and award of regulated qualifications to Achieve+Partners as soon as possible. These must be reported to info@achievepartners.co.uk for the attention of the Operations Director.