DATA PROTECTION

&

CONFIDENTIALITY

POLICY

Published Date:	03/12/2018	Author:	Shabir Siddiq – Operations Manager

Version	Change Detail	Latest Review Date	Date of Next Review	Updated By:
1.0	Annual Review	03/12/2019	03/12/2020	Shabir Siddiq
2.0	Annual Review & Policy Amended	03/12/2020	03/12/2021	Shabir Siddiq
2.1	Annual Review & Policy Amended	07/12/2021	07/12/2022	Shabir Siddiq
2.2	Annual Review & Policy Amended	07/12/2022	07/12/2023	Shabir Siddiq
2.2	Annual Review Changed to Academic Year Start	01/08/2023	31/07/2024	Shabir Siddiq
2.3	Annual Review	01/08/2024	31/07/2025	Shabir Siddiq

Alphabet Training aims to promote the highest standards of confidentiality and data protection throughout its organisation.

INTRODUCTION

Alphabet Training holds information about customers and employees. Everyone who works for or represents Alphabet Training must protect the personal data that they use and be aware of their obligations. The use of personal data must be fair, legal, and proportionate.

The protection of individuals via the lawful, legitimate, and responsible processing and use of their personal data is a fundamental human right. Individuals may have a varying degree of understanding or concern for the protection of their personal data but Alphabet Training must respect their right to have control over their personal data and ensure it always acts in full compliance with legislative and regulatory requirements. If individuals feel that they can trust Alphabet Training as a custodian of their personal data, this will also help Alphabet Training to fulfil its wider objectives. The General Data Protection Regulation (GDPR), as supplemented by the Data Protection Act DPA 2018 (DPA), is the main piece of legislation that governs how we collects and processes personal data. Failure to comply with this legislation may have severe consequences for Alphabet Training, including potential fines based on the severity of the data breach.

Therefore, staff must not use personal data obtained at work for their own purposes. It is a criminal offence knowingly or recklessly to disclose personal data without Alphabet Training's permission. Anyone who uses, discusses or discloses personal data held by the Alphabet Training without lawful authority may commit this offence.

Staff who knowingly disclose or misuse Alphabet Training's data for their own purposes, or who knowingly ignore the requirements of this policy will face disciplinary action in line with the company's procedures, regardless of any possible criminal sanction. This could lead to dismissal in some cases.

POLICY STATEMENT

Alphabet Training as a national Training Provider will take all appropriate steps to ensure that all personal data as defined and regulated by the Data Protection Act (DPA) 2018 and the General Data Protection Regulations (GDPR) see separate GDPR policy is processed accordingly.

This policy sets out how the Act applies to Alphabet Training and its commitment to ensuring that any personal data which it processes, is carried out in compliance with data protection law. Get SET

Academy ensures that good data protection practice is embedded in the culture of our staff and our organisation. The policy sets out some specific measures to assist compliance.

Data is defined as any personalised information held in any form – be it electronic or paper based and the DPA relates equally to all forms. Alphabet Training is committed to ensuring that all processing of personal data complies with these principles.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles. They must make sure the information is:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
- All adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- Accurate and, where necessary, kept up to date and that reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
- 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').
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Other policies/processes/information that compliment/support/impact data protection:

- Privacy policy.
- Records Management Policy.
- Data Retention Policy.
- Data Breach reporting process and breach register.

PROCESS/PROCEDURES/GUIDANCE

Data Protection Principles

The GDPR is based on a set of core principles that Alphabet Training must observe and comply with at all times from the moment that personal data is collected until the moment that personal data is archived, deleted or destroyed.

Alphabet Training will:

- Ensure that the legal basis for processing personal data is identified in advance and that all processing complies with the law.

- Not do anything with your data that you would not expect given the content of this policy and the fair processing or privacy notice.
- Ensure that appropriate privacy notices are in place advising staff and others how and why their data is being processed, and, in particular, advising data subjects of their rights.
- Only collect and process the personal data that it needs for purposes it has identified in advance.
- Ensure that, as far as possible, the personal data it holds is accurate, or a system is in place for ensuring that it is kept up to date as far as possible.
- Only hold onto your personal data for as long as it is needed, after which time Alphabet Training will securely erase or delete the personal data – Alphabet Training's data retention policy sets out the appropriate period.
- Ensure that appropriate security measures are in place to ensure that personal data can only be accessed by those who need to access it and that it is held and transferred securely.

Alphabet Training will ensure that all staff who handle personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

Breaching this policy may result in disciplinary action for misconduct, including dismissal. Obtaining (including accessing) or disclosing personal data in breach of Alphabet Training's data protection policies may also be a criminal offence.

DATA SUBJECT RIGHTS

The GDPR provides data subjects with a number of rights in relation to their personal data. Alphabet Training has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.

All requests will be considered without undue delay and within one month of receipt as far as possible.

Subject access: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- The purpose of the processing.
- The categories of personal data.
- The recipients to whom data have been disclosed or which will be disclosed.
- The retention periods.
- The right to lodge a complaint with the Information Commissioner's Office.
- The source of the information if not collected direct from the subject, and
- The existence of any automated decision making.

Right to withdraw consent: where the lawful basis relied upon by Alphabet Training is the data subject's consent, the right to withdraw such consent at any time without having to explain why.

Right to be informed: the right to be provided with certain information about how we collect and process the data subject's personal data (Transparency).

Right of subject access: the right to receive a copy of the personal data that we hold, including certain information about how Alphabet Training has processed the data subject's personal data.

Right to rectification: the right to have inaccurate personal data corrected or incomplete data to be completed.

Right to erasure (right to be forgotten): the right to ask Alphabet Training to delete or destroy the data subject's personal data if: the personal data is no longer necessary in relation to the purposes for which it was collected; the data subject has withdrawn their consent (where relevant); the data subject has objected to the processing; the processing was unlawful; the personal data has to be deleted to comply with a legal obligation.

Right to restrict processing: the right to ask Alphabet Training to restrict processing if: the data subject believes the personal data is inaccurate; the processing was unlawful and the data subject prefers restriction of processing over erasure; the personal data is no longer necessary in relation to the purposes for which it was collected but they are required to establish, exercise or defend a legal claim; the data subject has objected to the processing pending confirmation of whether Alphabet Training's legitimate interests or grounds for processing override those of the data subject.

Right to data portability: in limited circumstances, the right to receive or ask Alphabet Training to transfer to a third party, a copy of the data subject's personal data in a structured, commonly used machine-readable format.

Right to object: the right to object to processing where the lawful basis for processing communicated to the data subject was Alphabet Training's legitimate interests and the data subject contests those interests.

Right to object to direct marketing: the right to request that we do not process the data subject's personal data for direct marketing purposes.

Right to object to decisions based solely on automated processing (including profiling): the right to object to decisions creating legal effects or significantly affecting the data subject which were made solely by automated means, including profiling, and the right to request human intervention.

Right to be notified of a personal data breach: the right to be notified of a personal data breach which is likely to result in a high risk to the data subject's rights or freedoms.

Right to complain: the right to make a complaint to the ICO or another appropriate supervisory authority.

All staff must immediately forward any request made by a data subject (even if you are uncertain whether it represents a request as listed above) to the Information Communications Officer/Data Protection Lead. Alphabet Training will only have 30 days to respond in most circumstances. You must observe and comply with these guidelines.

RESPONSIBILITY FOR THE PROCESSING OF PERSONAL DATA

The Managing Director and Information Communications Officer take ultimate responsibility for data protection.

If you have any concerns or wish to exercise any of your rights under the GDPR, then you can contact the data protection lead in the following ways:

Name: Shabir Siddiq.
Address: Central Buildings, Richmond Terrace, Blackburn, BB1 7AP
Email: shabir@alphabet-training.co.uk
Telephone: 01254 679998.

ALPHABET TRAINING OBLIGATIONS

All Alphabet Training staff and sub-contractors will:

- Ensure that all relevant staff attends training on data protection.
- Inform Alphabet Training of any new services, projects and processes involving the use of personal data, or of significant changes to existing ones.
- Report all losses, thefts or breaches of security involving personal data to Alphabet Training.
- Notify Alphabet Training of all data or information sharing agreements or protocols.
- Participate in data audits.

1. AWARENESS & TRAINING

We will promote the need to respect privacy and confidentiality so that people remain confident about using Alphabet Training's services. People must be told how we will use their data, so that they are not reluctant to provide it to us.

2. OBTAINING INFORMATION

People must be informed when we record information about them, unless there is a specific legal reason for not doing so. Any process involving the collection and use of personal data must conform to the DPA principles. All staff must ensure that the use of personal data meets these conditions.

3. APPLICATION FORMS AND TOOLS TO GATHER INFORMATION

Any form or process designed to gather information must include a simple explanation about why personal data is needed, and what we will do with it. This 'fair processing notice' (as directed by the DPA) must also spell out whether data will be shared. Existing forms or methods of collection without fair processing information must be amended to do so.

4. RECORD KEEPING

Alphabet Training is responsible for and must be able to demonstrate compliance with the data protection principles and other obligations under the GDPR. This is known as the 'accountability principle'. Therefore, we will have in place adequate records management procedures, including measures to ensure that working records of people are fair, accurate, up-to-date and not excessive. Records about people must be secure, traceable and accounted for at all times. Each department must ensure that its records comply with the Alphabet Training's Records Management Policy which should contain a retention and disposal schedule. Records must be disposed of securely in accordance with the disposal schedule within the Policy. Records management procedures, including retention and disposal apply equally to paper and electronic records including emails. Managers will regularly need to assure themselves that they are compliant with statute and policy.

5. NEED TO KNOW

Access to personal data must only be available to those who need it, in line with fair processing principles. Data should be used when necessary and not purely because it is convenient to do so. Each Alphabet Training staff is responsible for restricting access to personal data and ensuring compliance. This must apply to all staff. All access to systems containing personal data must be logged. There must be a facility to log and record when a member of staff is given the right to access data and when they do access it.

6. PHYSICAL SECURITY

Alphabet Training must be notified of any actual loss, theft or accidental disclosure of personal data. All premises and electronic systems where personal data is held must have adequate security.

Access to areas where information is held should be controlled, paper files containing personal data must be locked away when not in use, and computer data must be protected by adequate security measures. Access to data should be restricted to authorised staff only; such staff should receive training on the security of the system prior to being allowed access to it.

Electronic data must only ever be stored on official servers. If this is impractical, data must be only stored in locations agreed by the Alphabet Training Management Team.

All valuable files, client personal information and documents must be stored on the appropriate server on the Alphabet Training's network and not on desktop PCs or laptops or other electronic storage devices. Information stored on desktop PCs, laptops, etc. is at risk of loss through hardware or software failure or automated administrative activity, or loss or theft of equipment.

Where information is gathered and recorded through mobile working then staff should download the data onto the appropriate network server as soon as possible.

Personal data should not be stored on unencrypted devices. Any such temporary storage must have a risk assessment prior to data being stored, which should be logged.

If in exceptional circumstances data is not stored on the network, then it is the responsibility of users to ensure that the data is secure and appropriate back-up procedures are operated. All staff must ensure that when dealing with customers they should not have access to screens or data on which other clients' records are displayed or can be seen.

Care should be taken if personal data is used outside the office environment, whether it is on paper or in a computer file. Data must only be stored on devices or equipment that are under the Alphabet Training's control, or which have been approved and are encrypted.

Data must not be stored on any equipment owned by members of staff including, but not limited to, mobile phones or PDA's, MP3 players, cameras, memory sticks, home computers or laptops.

All data, physical or electronic, must be disposed of securely, in accordance with the Alphabet Training's records management policy.

7. VALIDATING REQUESTS FOR INFORMATION

Departments must understand the legal framework that affects their work, so that they know when they have the power or the obligation to disclose information to other organizations e.g., the Skills Funding Agency or members of the public, and to obtain it from them.

If a request for personal data is made to Alphabet Training, the member of staff must raise the proposal to the Data Protection Lead/Information Communications Officer who will help them determine the appropriate response to the request and ensure that the correct information is released only where appropriate and legal to do so – in an agreed and secure format.

8. SECURITY OF TRANSFER

Information should be shared by the most secure method available; this will mean using an 'encrypted' approved email system for electronic transfers of personal data.

Any data remains the responsibility of the Alphabet Training staff that transfer it at all times and all are equally responsible for its continued, safe use.

If email is the best option, staff must use the correct email address and be aware that email inboxes may be monitored by managers or others who may not be entitled to access personal data. Sensitive data should not be sent by email unless steps have been taken to ensure that the recipient is not forwarding mail to another inbox, or that the inbox is not being monitored. Personal data should not be sent via fax or any other unsecure means without adequate protection being put in place and agreed.

Data transported outside of the training center must be done so in a secure manner – all efforts must be taken to ensure it is stored securely and that the risk of theft or loss is minimized, including the use of lockable storage, briefcases and boxes at all times. No data, whether electronic or paper, must be left unattended at any time – i.e., in cars or on public transport.

9. INFORMATION-SHARING AGREEMENTS

An information-sharing agreement or protocol is not a legal requirement to share information – sharing can happen without one. An agreement does not create a legal gateway if one does not already exist, however the use of a protocol will ensure best practice by all partners in any information sharing partnership. Any information sharing should be carried out using a risk assessment process.

10. CONTRACTS

If a contract or agreement involves the sharing of personal data, the contract should include measures to ensure that the data is used safely and appropriately. Information supplied to contractors can only be used for agreed purposes and must not be used or disclosed for any other reason without further consultation with Alphabet Training.

11. ACCESS TO PERSONAL DATA

Staff will only assist customers to gain access to data that we hold about them, as detailed in our Privacy Policy. This might be by providing access to files, by advising them about Alphabet Training's procedures, or by referring requests for access to Alphabet Training ICO.

12. COMPLAINTS ABOUT PERSONAL DATA

If any person identifies errors or inaccuracies in the data, we hold about them, or points out unfair uses of their data identified by requesters because of access to their files, these must be rectified immediately (once verified). Alphabet Training must keep records of such complaints and notify Alphabet Training of any unresolved disputes.

13. DATA PROTECTION OFFICER AND NETWORK

There is a legal requirement for Alphabet Training to have a nominated member of staff with specific responsibility for data protection policy, advice, training and good practice. This will be the Operations Manager who is the Data Protection lead/ICO.

14. INDUCTION

Information about confidentiality and data protection must be provided to all new members of staff and customers prior to them having access to a Alphabet Training's network and any personal data. Basic guides to all data protection issues are available on government websites.

15. CONFIDENTIALITY

Information explicitly accepted in confidence or as part of a confidential relationship can only be disclosed to someone else in exceptional circumstances. Employees must not disclose confidential information to anyone else without the permission of the individual who first gave the information to them unless the information is about serious wrong-doing or harm.

All staff have a duty to report any criminal activity or any wrongdoing to the proper authorities if they become aware of them. Alphabet Training operates a Whistle Blowing Policy, which provides further advice on what to do in these situations; this can be found on Alphabet Training's intranet.

Furthermore, Alphabet Training will never sell, market, distribute or give access to any information that it is required to hold. This information is only available to authorised personnel during specified audit and quality assurance meetings as required by Awarding and funding Bodies.

Learners may need to speak to tutors, assessors, teachers, or advisory staff from time to time. All one-to-one conversations are treated in the strictest confidence and no information will be passed on to third parties without the express permission of the learner. The only exception to this is where Alphabet Training staff may consider that the information given may be of a nature that it is relevant to a criminal offence or the potential for a criminal offence to be committed.

Alphabet Training actively encourages all learners to speak to our advisors if there are any issues or potential problems that may be encountered in terms of the records and information we are obliged to hold regarding our employees and learners.

16. MONITORING AND EVALUATION

Alphabet Training will periodically commission audits of Alphabet Training to ensure that it complies with the Data Protection Act.

17. REVIEW OF THIS POLICY

This policy will be reviewed, every year to ensure that it takes account of new legislation and expected developments in the areas of personal privacy and data sharing.

18. WELCOME PACK STATEMENT TO LEARNERS

Alphabet Training is required by the Qualification Awarding Bodies to maintain a database of learners for regulatory, auditing, and quality assurance purposes.

This information is strictly protected in accordance with the **Data Protection Act 2018** and the **Information Commissioner's Office** guidelines including password protection and staff restrictions on data access.

www.**ico**.gov.uk

MONITORING AND REVIEW

This policy was last updated on 1 Aug 2024 and shall be regularly monitored and reviewed every year.