

Data Protection & Privacy Policy

Contents

VERSION HISTORY	Error! Bookmark not defined.
INTRODUCTION	3
PURPOSE	3
SCOPE	4
PERSONAL INFORMATION	4
SPECIAL CATEGORY PERSONAL DATA	5
CRIMINAL RECORD CHECKS	5
VULNERABLE GROUPS	6
PROTECTED CHARACTERISTICS	6
RESPONSIBILITIES	6
POLICY	8
LAWFUL BASIS	8
DATA PROTECTION PRINCIPLES	8
DATA SUBJECT RIGHTS (DSRs)	9
Informed	10
Subject access	10
Rectification	10
Erasure	10
Restriction of processing	10
Data portability	11
Object to processing	11
Object to automated profiling	11
CONSENT	11
SECURITY	12
PERSONAL DATA BREACHES	13
DATA TRANSFERS	13
DATA PROTECTION BY DESIGN	13
REVIEW	14

INTRODUCTION

This policy outlines our commitment to protecting the personal data of our learners, staff, and stakeholders in accordance with the UK General Data Protection Regulations (UK GDPR) and other data protection legislation such as the Data Protection Act 2018 (DPA 2018) and the Privacy & Electronic Communications Regulations (PECR) 2003.

Woodspeen Training Ltd (Woodspeen Training) needs to gather and use personal data about individuals (Data Subjects) and collects personal data only for specified, explicit, and legitimate purposes. This can include customers, suppliers, business contacts, employees, and other people Woodspeen Training have a relationship with or who may need to be contacted. The data collected is relevant and limited to what is necessary for the intended purpose.

This policy describes how personal data must be collected, handled, and stored to meet data protection standards and to comply with data protection laws. Personal data may be shared with third parties only when necessary and with appropriate safeguards in place. Woodspeen Training ensures that any third parties handling personal data comply with UK GDPR requirements.

Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected, and in accordance with legal, regulatory, and business requirements.

Woodspeen Training's Data Protection and Privacy Policy helps ensure Woodspeen Training:

- Complies with its obligations under regulations
- Protects the rights of staff, customers, and clients
- Is open about how the company stores and processes individual's data
- Protects Woodspeen Training from the risks of a data breach

PURPOSE

The objective of this policy is to ensure:

- Personal Data is processed by Woodspeen Training in compliance with the requirements of the:
 - Data Protection Act (DPA) 2018
 - UK General Data Protection Regulation (UK GDPR)
 - Privacy and Electronic Communications Regulations (PECR) 2003

- Employees are aware of their obligations when processing personal data on behalf of Woodspeen Training, its clients, staff, and customers

SCOPE

This policy applies to all personal data processed by Woodspeen Training relating to an identified or identifiable natural living individual and is part of its approach to compliance with data protection law.

All staff, partners or third parties who have, or may have access to personal data are expected to have read, understood, and complied with this policy. Failure to comply may lead to disciplinary action for misconduct, including dismissal or contract termination.

Pseudonymised personal data is covered by Data Protection legislation. However anonymised data is not regulated by the UK GDPR or DPA 2018, providing the anonymisation has not been done in a reversible way.

Data Protection law in the UK regulates how Woodspeen Training collects, handles, and stores personal data regardless of whether data is stored electronically or in paper format.

PERSONAL INFORMATION

Personal data means any information that relates to an identifiable, living individual. (*Identifiable means that you can put 1 or more pieces of information together to work out who someone is*) such as:

- Name
- Contact emails address
- Address
- Date of Birth
- National Insurance Number
- Finance information
- Employer, Role and qualifications
- PCI Card data
- IP Address
- URL
- Geographical location
- Site location
- Telephone number
- An identification number
- An online identifier

SPECIAL CATEGORY PERSONAL DATA

Some personal data is more sensitive and is afforded more protection, this is information relating to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric ID data
- Health data
- Sexual life and/or sexual orientation

Woodspeen Training will apply additional organisational and technical measures to protect special category data based on risk to the Data Subject.

Woodspeen Training will only process special category data where it has a lawful basis for doing so in line with Article 6 and Article 9 of the UK GDPR and where we have an exception to do so.

CRIMINAL RECORD CHECKS

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. Woodspeen Training cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of sensitive personal data and must be treated as such.

The UK GDPR gives extra protection to 'personal data relating to criminal convictions and offences or related security measures. Criminal data is information about offenders or suspected offenders in the context of criminal activity, allegations, investigations, and proceedings.

- It includes not just data which is obviously about a specific criminal conviction or trial, but also any other personal data 'relating to' criminal convictions and offences, it can also cover suspicion or allegations of criminal activity.
- 'Relating to' should be interpreted broadly. It covers any personal data which is linked to criminal offences, or which is specifically used to learn something about an individual's criminal record or behaviour.

VULNERABLE GROUPS

We need to even up the power balance between those who hold our most precious data and the most vulnerable who hand over their data, often with little knowledge of their rights. People need confidence in their privacy in order to participate in society.

We must protect the interests of vulnerable groups, such as:

- Children's personal information
- Individuals with learning difficulties
- The approach of police forces and third parties to collecting personal information
- Individuals with language difficulties

PROTECTED CHARACTERISTICS

Specific characteristics are protected from discrimination under the Equalities Act 2010 and include:

- race
- religion or belief
- sexual orientation
- disability
- pregnancy
- gender reassignment (as far as they may reveal information about a person's health)

RESPONSIBILITIES

Woodspeen Training is a Data Controller, and a Data Processor of personal data as defined by the UK GDPR and DPA 2018.

Key responsibilities are:

- The Board is accountable for data protection and ultimately responsible for ensuring that Woodspeen Training meets its legal obligations
- The Data Protection Officer (DPO) is responsible for:
 - Ensuring the inclusions of this policy are up to date
 - Keeping the Board updated about data protection responsibilities, risks, and issues
 - Reviewing all data protection policies and procedures in line with an agreed schedule
 - Providing data protection advice and guidance

- Support and review Impact Assessments and identifying risks to the business
- Ensuring data protection training and advice is available
- Ensure Data Subject Rights are responded to and recorded
- Logging, investigating, and mitigating personal data breaches and provide recommendations
- Reviewing contracts and agreements with third parties which may handle the company's sensitive data
- Being the first point of contact with the ICO and any supervisory authority in the jurisdiction out with the UK
- Resource manager is responsible for ensuring the provisions of this document are understood and adhered to by line management
- Information Security Officer (ISO) is responsible for ensuring all systems, services and equipment used for storing personal data meet acceptable security standards and performing regular checks and scans to ensure security hardware and software is functioning properly. Evaluating any third-party services the company is considering using to store or process data
- The Information Asset Owner (IAO) is responsible for:
 - Data Protection compliance in their area
 - Ensuring the Information Asset Register (IAR) is accurate and kept up to date
 - Ensuring the Records of Processing Activities (ROPA) Register is accurate and kept up to date
- Line management are responsible for:
 - ensuring the provisions of this document are understood and adhered to by all staff and others as appropriate
- Marketing Manager is responsible for:
 - Addressing any data protection queries from journalists or media outlets like newspapers, with support from the DPO
 - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles, with support from the DPO

Compliance with data protection law is the responsibility of all employees, partners and third parties working on behalf of Woodspeen Training. Woodspeen Training will ensure that all staff, partners or third parties who manage personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and complete mandatory annual data protection training.

Breaching this policy may result in disciplinary action or misconduct, including dismissal or contract termination. Obtaining (including accessing) or disclosing

personal data in breach of Woodspeen Training's data protection policies may also be a criminal offence.

POLICY

Woodspeen Training processes the personal data of staff/customers/suppliers and is committed to ensuring that all the personal data that it processes is conducted in accordance with all data protection law. Personal data must be protected from unauthorised access, accidental deletion and malicious hacking attempts and we take reasonable steps to ensure it is accurate and kept up to date. Woodspeen Training must ensure that personal data is only held for as long as necessary and not indefinitely, unless required by law, advice should be sought from the DPO and ensure good data protection practice is embedded in the culture of our staff.

Woodspeen Training's other data protection policies and procedures are:

- An Appropriate Document Policy
- A Record of Processing Activities and Assets
- Privacy Notices (website, clients, employees)
- Personal data breach reporting processes and a breach register
- Data Retention & Disposal Policy
- Data Subject Rights (DSR) procedures and register
- Information Security policies

LAWFUL BASIS

Woodspeen Training will establish a lawful basis for processing personal data. All departments, employees and contractors must ensure a lawful basis to legitimately process personal data, has been identified and established. The lawful basis for the activity will be documented in the RoPA Register, advice should be sought from the DPO.

DATA PROTECTION PRINCIPLES

To comply with data protection law, personal data must be collected and used fairly, stored safely and not disclosed unlawfully. Woodspeen Training complies with the seven UK GDPR data protection principles set out below. When processing personal data, Woodspeen Training will ensure that Personal Data 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')
- 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 reasonable steps will be taken to ensure that personal data that is 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 which 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')
- Accountable in demonstrating how we ensure compliance and how we process personal data

Woodspeen Training is responsible for complying with the data protection principles and will demonstrate this in accordance with Article 5(2) 'Accountability' by implementing policies and procedures, technical and organisational measures and keeping documentation such as breach and Data Subject Rights records.

DATA SUBJECT RIGHTS (DSRs)

Individuals have rights regarding their personal data and Woodspeen Training provides clear instructions on how individuals can exercise these rights in our External Privacy Notice published on our website. Woodspeen Training have processes in place to ensure 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 and can identify such a request and know who to send it to.

All requests will be considered without undue delay and satisfied within one calendar month of receipt unless there is a justifiable reason for extension, dependent on the complexity of the case, in which case the Data Subject will be informed of the extension within one calendar month that the response may take up to a further two calendar months to respond in full. Woodspeen Training will ensure the rights as detailed below can be exercised by Data Subjects.

Informed

The right to be informed about the collection and use of personal data is addressed via Woodspeen Training privacy notices.

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 period
- The right to lodge a complaint with the Information Commissioner's Office (ICO)
- The source of the information if not collected directly from the data subject
- The existence of any automated decision-making

Rectification

The right to allow a Data Subject to rectify inaccurate personal data concerning them.

Erasure

The right to have data erased and to have confirmation of erasure, but only where:

- The data is no longer necessary in relation to the purpose for which it was collected, or
- Where consent is withdrawn, or
- Where there is no legal basis for the processing, or
- There is a legal obligation to retain the data

Restriction of processing

The right to ask for certain processing to be restricted in the following circumstances:

- If the accuracy of the personal data is being contested, or
- If Woodspeen Training processing is unlawful but the Data Subject does not want it erased, or
- If the data is no longer needed for the purpose of the processing but it is required by the Data Subject for the establishment, exercise, or defence of legal claims, or

- If the Data Subject has objected to the processing, pending verification of that objection

Data portability

The right to receive a copy of personal data which has been provided by the Data Subject, and which is processed by automated means in a format which will allow the individual to transfer the data to another Data Controller. This would only apply if Woodspeen Training were processing the data using consent or processed based on a contract.

Object to processing

The right to object to the processing of personal data relying on the legitimate interests processing condition, unless Woodspeen Training can demonstrate compelling legitimate grounds for the processing which override the interests of the Data Subject or for the establishment, exercise, or defence of legal claims.

Object to automated profiling

The right to object where solely automated decision-making is being conducted that has legal or similarly significant effects on the Data Subject.

CONSENT

Woodspeen Training understands the conditions of consent as defined in Article 7 of the UK GDPR and will ensure:

- Consent is a specific, informed, and is an unambiguous indication of the Data Subjects wishes
- The Data Subject can withdraw consent at any time
- Withdrawal of consent is as easy as it was to give consent
- Where information society services are provided to children, consent of the parent/guardian will be obtained based on the age limits defined in the country concerned
- Records of consent are kept as evidence
- The Data Subject is competent to give consent and is doing so freely without duress

SECURITY

Woodspeen Training have appropriate technical and organisational measures in place to ensure personal data is stored securely using appropriate technical and organizational measures to prevent unauthorized access, alteration, or destruction.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. Woodspeen Training will ensure that all personal data is accessible only to those who have a valid reason for using it and will have in place appropriate security measures by:

- keeping all personal data in a lockable cabinet with key-controlled access,
- password protecting personal data held electronically,
- archiving personal data which will be kept securely (lockable cabinet),
- placing any PCs or terminals that show personal data so that they are not visible except to authorised staff,
- ensuring that PC screens are not left unattended without a password protected screensaver being used

The company ensures that data is kept accurate and up to date and Woodspeen Training will always assess the risk of processing personal data to the data subject to:

- ensure personal data is stored securely using software that is kept-up-to-date and supported
- Ensure access to personal data shall be role based, limited to personnel who need access and appropriate security shall be in place to avoid unauthorised sharing of information
- Ensure when personal data is deleted, this shall be done safely such that the data is irrecoverable
- Ensure appropriate back-up and disaster recovery solutions shall be in place
- Ensure staff receive regular Data Protection and Information Security training and information security policies and procedures on data protection principles and UK GDPR compliance to ensure they understand their responsibilities in handling personal data.
- Ensure personal data is encrypted where possible at rest and in transit
- Ensure where possible personal data masking via anonymisation or pseudonymisation is used
- Ensure all passwords used meet password policy requirements
- Ensure anti-malware software is deployed on all devices handling personal data
- Ensure paper documents containing personal data shall be stored in lockable cabinets
- Ensure physical security controls are in place to prevent unauthorised access to areas where personal data may be held
- Ensure all company information security certifications (Cyber Essentials) are maintained, and policies and procedures adhered to

PERSONAL DATA BREACHES

Any personal data incident or breach should be notified to the DPO immediately with as much detail as possible to Ellie.Robertson@woodspeentraining.co.uk and you should make yourself available in the event that the DPO requires further information from you. Woodspeen Training is dedicated to complying with the requirements for responding to and reporting a personal data breach. Personal Data breaches can come in many forms, including but not limited to:

- Insider threat
- Malware attacks
- Accidental web exposure
- Data in transit

Personal Data breaches will be identified, and, where they present a risk to the Data Subject, the ICO's office will be notified, by the DPO with consultation with the Board, without undue delay and within 72 hours of them being discovered and reportable breaches of PECR will be notified to the ICO within 24 hours of becoming aware of the incident. Personal Data Breaches will be assessed, and mitigation will be applied to ensure the breach does not continue and to try to prevent it from happening again. Data Subjects impacted by this will be notified where there is a high risk to them and/or according to the ICO advice. Any sub processors or data controllers' data will also be notified to them as per contractual agreements, where appropriate.

DATA TRANSFERS

Woodspeen Training may need to transfer data outside of the UK. Woodspeen Training will ensure that any personal data transferred to third countries which do not have adequacy controls in place, will not be transferred without suitable safeguards in place, which may include:

- Standard contract clauses
- Binding corporate rules
- A UK International Transfer Agreement (UK ITA)
- Adequacy decision
- An exception as defined in Article 49 of the GDPR

DATA PROTECTION BY DESIGN

Data protection by design allows for data protection to be built into a business's ethos but ensuring processes, services and other ideas are risk assessed from a UK GDPR point of view. Woodspeen Training is committed to practicing this to ensure systems

are built with data protection as the first thought, rather than an afterthought. All staff must declare new processes or systems involving data to ensure a Data Protection Impact Assessment (DPIA) is completed where needed. Advice should be sought from the DPO.

REVIEW

This policy was last updated on 27 November 2024 and will be reviewed on a Biennial basis. However, it may be updated from time to time if material changes are made.