Primary Goal

Data Protection Policy

Introduction and Purpose

Primary Goal collects and uses certain types of personal information about staff, learners and employers who come into contact with the organisation in order to provide education and training. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of the Education & Skills Funding Agency (ESFA), Department for Education & Training (DfE), Local Authorities (LAs), European Social Funding (ESF) government agencies and other bodies.

This policy also applies to the processing of personal data in manual and electronic records kept by Primary Goal in connection with its HR function. It also covers the Organisation's response to any data breach and other rights under the General Data Protection Regulation and current Data Protection Act.

This policy applies to the personal data of learners, staff, employers, job applicants, former employees, apprentices, volunteers, placement students, workers, and self-employed contractors.

This policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

Primary Goal makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of the Organisation, the Organisation will ensure that the third party takes such measures in order to maintain the Organisation's commitment to protecting data. In line with current data protection legislation, Primary Goal understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Definitions

Consent

The consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.

Data Controller

The natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to employers, leaners and staff used in our business for our commercial purposes.

Data Processor

A natural or legal person or organisation which processes personal data on behalf of a data controller.

Data Subject

A living, identified, or identifiable natural person about whom the Company holds personal data.

EEA

The European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway.

Personal Data

Any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Data Processing

Any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymisation

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

Special Category Personal Data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

Types of Data Held

The following learner personal data is collected, held, and processed by the Company to ensure eligibility and compliance, Personal Learning record (PLR) checks, European Social Fund (ESF) contract requirements, and to set up access to ePortfolio accounts:

- Name
- Date of birth
- National Insurance number
- Address
- Previous names
- Identity checks/confirmations
- Contact details
- Gender
- Nationality
- Employment status
- Care leavers
- Educational Health Care Plan
- Medical information
- Disabilities/learning difficulties
- Prior attainment, previous qualifications and achievements
- Equal opportunities monitoring (e.g. age, ethnicity)

Staff personal data is kept in personnel files within Primary Goal's HR systems (BrightHR and SharePoint). The following types of data may be held by the Organisation, as appropriate, on relevant individuals:

- Name, address, phone numbers - for individual and next of kin.
- CVs and other information gathered during recruitment.
- References from former employers
- National Insurance numbers

- Job title, job descriptions and pay grades.
- Conduct issues such as letters of concern, disciplinary proceedings.
- Holiday records
- Internal performance information
- Medical or health information
- Sickness absence records
- Tax codes
- Terms and conditions of employment
- Training details

Relevant individuals should refer to Primary Goal's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

Data Protection Principles

All personal data obtained and held by Primary Goal will:

- Be processed fairly, lawfully and in a transparent manner.
- Be collected for specific, explicit, and legitimate purposes.
- Be adequate, relevant and limited to what is necessary for the purposes of processing.
- Be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay.
- Not be kept for longer than is necessary for its given purpose.
- Be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisational measures.
- Comply with the relevant data protection procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- The right to be informed.
- The right of access.
- The right for any inaccuracies to be corrected (rectification).
- The right to have information deleted (erasure).
- The right to restrict the processing of the data.
- The right to portability.
- The right to object to the inclusion of any information.
- The right to regulate any automated decision-making and profiling of personal data.

Scope

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

The Board and Senior Management are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

Our managed service provider, Ask4Support, may process personal data on our behalf for the purposes of providing IT support, system maintenance, cybersecurity, and infrastructure management, in accordance with applicable data protection legislation and contractual confidentiality obligations.

Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Officer, Roy Morden, Head of IT: roy.morden@primarygoal.ac.uk . In particular, the Data Protection Officer should always be consulted in the following cases:

a) If there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed.
b) If consent is being relied upon in order to collect, hold, and/or process personal data.
c) If there is any uncertainty relating to the retention period for any type(s) of personal data.
d) If any new or amended privacy notices or similar privacy-related documentation are required.
e) If any assistance is required in dealing with the exercise of a data subject's rights.
f) If a personal data breach (suspected or actual) has occurred.
g) If there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data.

h) If personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors).
i) If personal data is to be transferred outside of the UK and there are questions relating to the legal basis on which to do so.
j) When any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities.
k) When personal data is to be used for purposes different to those for which it was originally collected.
l) If any automated processing, including profiling or automated decision making, is to be carried out.
m) If any assistance is required in complying with the law applicable to direct marketing.

Procedures

Primary Goal has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- It appoints or employs employees with specific responsibilities for the following, with clear lines of responsibility and accountability for these roles:
    a) the processing and controlling of data.
    b) the comprehensive reviewing and auditing of its data protection systems and procedures
    c) overviewing the effectiveness and integrity of all the data that must be protected.
- It provides information to data subjects on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way.
- It provides employees with specific responsibilities with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially.
- It can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with.
- It carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the Organisation.
- It recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The Organisation understands that consent must be freely given, specific, informed, and unambiguous. The Organisation will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time.
- It has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner and is aware of the possible consequences.
- It is aware of the implications of international transfer of personal data.

Access to Data

Relevant individuals have a right to be informed whether Primary Goal processes personal data relating to them and to access the data that the Organisation holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- An email making a subject access request should be made to the Shared Services Manager.
- The Organisation will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request.
- The Organisation will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform Primary Goal immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The Organisation will take immediate steps to rectify the information.

Data Disclosures

The Company processes personal data using automated means. All learner information is shared with the Education & Skills Funding Agency (ESFA) on behalf of the Secretary of State for the Department of Education (DfE) through a secure government portal provided by our Learner Management provider (BUD). Learner personal data will also be shared with our partner BUD for the purpose of learning and access to learners ePortfolio.

Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the right, under the UK GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects through encrypted/ password protected electronic documents/files.

Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller. All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

In relation to staff, the Organisation may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- Any employee benefits operated by third parties.
- Disabled individuals - whether any reasonable adjustments are required to assist them at work.

- Individuals' health data - to comply with health and safety or occupational health obligations towards the employee.
- For Statutory Sick Pay purposes.
- HR management and administration - to consider how an individual's health affects his/her/their ability to do their job.
- The smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data Security

Primary Goal adopts procedures designed to maintain the security of data when it is stored and transported.

In addition, employees must:

- Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them.
- Ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people.
- Refrain from sending emails containing sensitive work-related information to their personal email address.
- Check regularly on the accuracy of data being entered into computers.
- Always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.
- Use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the Chief Operating Officer. Where personal data is recorded on any such device it should be protected by:

- Ensuring that data is recorded on such devices only where absolutely necessary.
- Using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
- Ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow the Organisation's rules on data security may be dealt with via appropriate disciplinary procedures. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

International Data Transfers

The Organisation does not transfer personal data to any recipients outside of the EEA.

Breach Notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the Organisation becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, Primary Goal will do so without undue delay.

Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for Primary Goal are trained appropriately in their roles under data protection legislation.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Organisation of any potential lapses and breaches of the Organisation's policies and procedures.

Records

The Organisation keeps records of its processing activities including the purpose for the processing and retention periods. These records will be kept up to date so that they reflect current processing activities.

Review

Primary Goal will continue to review the contents of this policy annually.