Data Protection Policy

Introduction

The Portland Training Company Limited (The Data Controller) is required to maintain certain personal data about living individuals (Data Subjects) for the purposes of satisfying operational and legal obligations. Portland Training recognises the importance of the correct and lawful treatment of personal data. This maintains confidence in the organisation and provides for successful operations.

The types of personal data that Portland Training may require includes information about: current, past and prospective employees; learners; employers, suppliers and others with whom it communicates. This personal data (including digital and video images where applicable), whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the General Data Protection Regulation (GDPR).

Portland Training fully endorses and adheres to the key principles of GDPR which set out our main responsibilities. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. Data Controllers and Data Processors that collect, handle, process, transport and store personal data for Portland Training must adhere to these principles.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and subsequently requires more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics

	• Biometrics (such as fingerprints), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Purpose of the Data Protection Policy

1. The purpose of this Data Protection Policy is to ensure that Portland Training Data Controllers and Data Processors comply with the requirements of GDPR when processing personal data.

2. All Data Controllers must comply with and understand the key principles of GDPR. Article 5 states that:

   ‘the controller shall be responsible for, and be able to demonstrate, compliance with the principles’.

3. It is important to recognise that breach of GDPR by Processors and Controllers may expose both Portland Training and the individual to legal action and claims for substantial damages. Any breach of the regulation will be treated seriously by Portland Training and may be considered under disciplinary procedures for employees of Portland Training.

4. For Learner, employers, employees and suppliers to maintain confidence in Portland Training’s compliance with GDPR.

The General Data Protection Regulation

In accordance with the principles set out under the GDPR, all personal data held by Portland Training shall be:

Principles

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and where necessary, kept up to date; every reasonable step must 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;

e. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. 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.

Lawful basis for Processing

All personal data that is processed by Portland Training will be done so using a valid lawful basis, the most common lawful basis we use to process data is our legal obligation we have with the Department for Education (DfE). The lawful basis used for processing all data is listed within our Data Inventory and is communicated to individuals via our privacy notice(s).

Where Portland Training requests to publish digital video and/or images for success stories we will do so using the lawful basis of consent, the subject will be contacted prior to complete an Image Use Permission Form or their consent will be asked for at the enrolment stage prior to the commencement of learning. The subject has rights to decline this request and/or chose to stay anonymous.

Individual Rights

Individuals that we hold personal data for have the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Portland Training supports these rights by communicating how we collect and use personal data in our privacy notice(s), and it is company policy that we do not use automated decision making systems. The process for requesting access, rectification, erasure, restriction, data portability and objection can be found below.

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that Portland Training holds about them. This includes:

- confirmation that their personal data is being processed.
- access to a copy of the data.
- the purposes of the data processing.

- the categories of personal data concerned.
- with whom the data has been or will be shared.
- how long the data will be stored for or if this isn't possible, the criteria used to determine this period.
- the source of the data, if not the individual.
- whether any automated decision-making is being applied to their data and what the significance and consequences of this might be for the individual.

To access individual rights it must be requested in writing (Paper based or electronically) via a Subject Access Request (SAR) to Portland Training. Portland Training will respond to all requests no later than 1 month after receiving them. If the request is found to be manifestly unfounded or excessive, particularly if it is repetitive a small fee may be applied. Where Portland Training is legally obliged to retain data for a certain period we will be unable to action your request for deletion.

Subject access requests should include:

- name of individual.
- correspondence address.
- contact number and email address.
- details of the information requested.

Accountability and Governance

Portland Training (The Data Controller) holds contracts with the following organisations that process personal data on our behalf (The Data Processor) these include:

- Contracted Third Party IT Support vendor
- Department for Education (DfE)
- Other Training Providers or Further Education Colleges where we are subcontracting provision, including their MI System software suppliers
- Contracted MIS Provider
- Awarding Body Organisations
- Contracted ePortfolio Provider(s)
- Contracted Archival Storage and Retreival vendor

Portland Training employees only:

- Portland Training Holding Company
- Sage

- BACS
- Portland Training Company Bank
- Legal Advisors
- Breathe HR

Portland Training have a legal obligation to provide employee personal data to HMRC and Nest Pension.

Portland Training hold a data inventory of all data we process, to ensure the key principles of the GDPR are adhered to at all times, this is updated and reviewed accordingly when new business processes are implemented and further funding contracts are obtained.

Data Protection Compliance audits are carried out on a yearly basis and a review of this policy, the privacy notice(s) and data inventory.

Security - Paper Based Records and Files

All paper based documentation held for learners, employees and third parties is to be treated as confidential even if not so marked. This means that it is to be kept as per the policy below and if necessary destroyed securely via confidential waste bins or an appropriate shredder (P-4 rating cross-cut shredder). In regards electronic records for the same, these are also to be treated as confidential and only stored within the MIS or SharePoint as per the policy below.

Personal data that is held paper based for learners and employers is kept in secure and locked filing cabinets within the admin office at Portland Training. Personal data that is held paper based for Portland Training employees is kept secure and locked with restricted access to the managing director, relevant line managers and Human Resources only. Portland Training operates a clear desk policy which means paper based personal data that is actively being processed is allowed on employees' desks for no longer than is required. If it is no longer required for active processing it must be filed (as above) or confidentially destroyed. Portland Training contracts with Box-it to ensure secure shredding of all confidential waste. All offices at Davian House where personal data is being processed are key coded and a strict 'access only where required' policy is exercised.

Security - Electronic Records and Files

Personal Data that is held electronically for learners and employers may be stored in more than one place for contractual obligations or to support business processes. These are our MI System, tracking spreadsheets stored on SharePoint as part of the secure Microsoft Office 365 cloud, other provider MI or data sharing systems, awarding body and our electronic portfolio systems.

Access to personal data that is held electronically for learners and employers is restricted, and password protected log ins are only provided to Portland Training employees where required to fulfil their job role.

Personal Data that is held electronically for Portland Training employees is stored on our electronic HR system Breathe HR, in HR files on SharePoint as part of the secure Microsoft Office 365 cloud and in Sage for payroll purposes. Access to personal data that is held for Portland Training employees is restricted to the managing director, HR and Compliance Manager for the group and further restricted access to line managers only to enable them to fulfil their job role.

Version Control

Portland Training operates under ISO:9001 2015 Quality Management System. All documentation is controlled by version and date and is listed on a "Master Document List".

All Policies and Procedures held by Portland Training must be version controlled as follows:

- Name
- Version number (e.g 001)
- Created by (e.g AB)
- Date last updated (e.g LU June2019)
- Date to be reviewed (e.g TBR June2020)

All Documents and Forms created by Portland Training must be version controlled as follows:

- Name
- Version number (e.g 001)
- Created by (e.g AB)
- Date last updated (e.g LU June2019)

Document Management

Portland Training operates document management and handling based on a number of categories aligned version control, each with a corresponding classification and handling requirements as detailed below:

Document Type	Classification
Policy	Open unless HR then Confidential & Sensitive
Procedure	Open unless HR then Confidential & Sensitive
Form	Open if blank, Confidential if Filled
Report	Confidential
Document	Classified per document

When classifying documents the below questions will be considered to determine the correct classification where not covered above.

- Does the document contain information that originated from an open and publicly accessible source?
    - Provided the document contains information that was not obtained in breach of any confidentiality or secrecy obligation and is in the public domain, the document may be classified as open or public depending on the other questions to be considered below.
- Does the document contain personal data?
    - See above for a definition of "personal data", but as a general guide this is any information that may directly or indirectly identify an individual (called a "data subject"). Documents that contain personal data should be classified as Confidential.
- Does the document contain special categories of personal data or personal data relating to criminal convictions and offences?
    - See the above for a definition of these categories of personal data. This information requires additional procedures to be followed, and safeguards applied and should be classified as Secret.
- Does the document contain any information of commercial or competitive value for Portland Training Company or any other third party?
    - The document may contain commercially sensitive information or trade secrets relating to Portland Training Company or entrusted to Portland Training Company by a third party. In all cases this should be classified as Confidential & Sensitive as a minimum

Classification Definitions and handling procedures

Classification	Definition	Handling Procedures
Public	May be viewed by anyone, anywhere in the world	Can be distributed to the public
Open	Available to all authenticated members of staff	Paper – kept in filing cabinets when not in use Digital – Stored in SharePoint or MIS, may be distributed via Teams/email
Confidential	Available only to authorised and authenticated members of staff	Paper – kept in filing cabinets when not in use Digital – Stored in SharePoint or MIS, may be accessed directly only or sent via Signable, encrypted email attachment or secure portal
Confidential & Sensitive	Access is controlled and restricted to a small number of named, authenticated members of staff	Digital ONLY – Stored in access-controlled SharePoint Site/Folder or MIS. Direct access or distribution via encrypted attachment or secure portal
Secret	Known only to a very small number of authenticated members of staff	Digital ONLY – Stored in access controlled SharePoint Site/Folder. Direct access only.

Document Retention

All personal data that relates to funded training (such as by DfE or devolved authorities) will be retained and reviewed in line with contractual requirements.

All other personal data for learners and employers that does not relate to funded training will be reviewed either in accordance with Prime Contractor requirements as stated in the relevant contract documents or after 6 years.

Personal Data held for Portland Training employees will be reviewed after 6 years.

Once the retention period has passed, or upon review Portland Training will destroy the personal data held or anonymise (remove identifying particulars so the data is no longer personal) to continue to use the information for statistical purposes and to manage business performance effectively.

Passwords

All passwords used for Portland Training systems or authorised third party websites and applications must adhere to minimum complexity requirements:

Microsoft 365 and Windows

A minimum password length of at least 8 characters with no maximum length restriction including at least one upper case, one digit and one special Character (see below). Commonly used passwords will be detected by Microsoft Intune. Microsoft Authenticator is required as part of our security environment and will be configured by IT Desk and facilitated by the Data and Reporting Lead at induction of new staff.

Third Party Websites

A minimum password length of at least 12 characters with no maximum length restriction including at least one upper case, one digit and one special Character (see below). Please note that if the website/cloud service offers Multi-Factor Authentication this must be enabled using Microsoft Authenticator.

Password Expiration

Passwords for Windows, Microsoft 365 and the MIS are set to expire on a regular schedule and will need to be changed regularly. Previously used passwords will be blocked by these systems.

Notes

- Characters for passwords
    - Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
    - Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
    - Base 10 digits (0 through 9)
    - Non-alphanumeric characters (special characters): (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) Currency symbols such as the Euro or British Pound aren't counted as special characters for this policy.
- Creating strong passwords
    - Strong passwords can be created easily by stringing together three memorable words without spaces and adding a number and a special character to the end, for example BottleBridgeFish01!

- Storing passwords
  - Do not write your passwords down. If you do have trouble remembering your passwords consider using a secure password wallet app such as Google password manager.
  - If you do use these facilities ensure that you keep your account details to yourself and use their built in security checkup tools to keep your passwords secure

Device Locking

Windows Devices

Portland Training utilises Microsoft Intune to enforce multi-factor authentication supported by an 8-character password (in line with our password policy) on all windows devices through the use of Microsoft Authenticator as well as a strong password as detailed in the password policy. New staff will be given their login details at induction and the Windows Hello and Microsoft Authenticator (if the staff member is issued with a PTC mobile phone) will be configured by the Data and Reporting Lead in line with these policies. If the staff member is not issued with a PTC mobile phone then the Microsoft Authenticator will be configured in line with the Bring Your Own Device policy at induction.

Mobile Phones

Portland Training utilises Mobile Device Management software to ensure that all mobile devices are kept secure and can be remotely wiped in case of loss or theft. As part of this software a 6-digit PIN is required for all mobile devices where credentials are used solely to access the device. This will be enforced when the device is enrolled on to the MDM software and initially set by the Data and Reporting Lead and updated as part of the staff induction process. All access to emails via Outlook and Teams additionally requires the correct username, an 8-character password (in line with our password policy), and Microsoft Hello Authentication via Microsoft Authenticator.

Equipment Usage – Bring Your Own Device

Portland Training Company has undertaken research and review of its responsibilities in line with legislation and best practice in regards Data Protection and Information Security, safeguarding and the Prevent Duty and has made the following decisions in regards the use of personal devices in a work capacity:

- Portland Training strictly forbids the use of personal equipment to obtain, process or store personal data, only IT equipment supplied by Portland Training will be used to obtain, process and store personal data. Portland Trainings servers, network, and IT equipment are all certificated as compliant with the Cyber Essentials Plus scheme. As part of the compliance with the Cyber Essentials Plus scheme all laptops/desktops utilise native hard disk encryption (Microsoft BitLocker) which is monitored by IT Desk as part of our commitment to Data Security.

- The Microsoft Authenticator App may be used on a personal smartphone where required for multi-factor authentication for access to applications, websites etc as required by your job role. In this case the device must be secured with a 6-digit PIN and biometric security measures (Face, iris, fingerprint) must be enabled on the device and Microsoft Authenticator app
- PTC Employees must not use personal devices to conduct any form of communications (e-mail, telephone calls, social media messaging, direct messaging such as WhatsApp) with client businesses, associates, partners or learners. This is to ensure that any safeguarding or legal issues which may arise from such communications are minimized and, in the event of an issue arising, proper investigations may be conducted as required.

Portland Training Company does allow the use of personal devices for recreation during designated break times at the discretion of Line Managers. This recreational usage is subject to the Acceptable Use of ICT Policy

Staff Leaving

When a member of staff leaves employment with Portland Training the HR Team will inform the Contracted Third Party IT Support vendor, Data and Reporting Lead and (if necessary) Prime Contractors so that their access to Portland Training systems can be terminated in a timely manner. The email account associated with that member of staff will be archived for future access by the HR Team, their Line Manager or the Senior Management Team if required.

Data Breaches

Portland Training keeps a register to record when a data breach may occur, all breaches will be investigated and where required to do so they will be reported to the Information Commissioner's Office (ICO) within 72 hours. If a data breach occurs that may cause high risk to an individual's rights and freedoms Portland Training will notify the individual within 72 hours.

If a data breach occurs which would affect data processed on behalf of a Prime Contractor, Portland Training would also inform them in accordance with contractual requirements via their approved reporting method.

If a member of staff suspect that a data breach may have occurred, they should report it to their line manager and the Data Protection Officer immediately so that it can be handled as outlined below.

- Staff member reports suspected data breach to Line Manager and Data Protection Officer.
- LM and DPO will then confirm a data breach has occurred and gather required information to complete the Data Breach Log.
- LM and DPO will report the data breach to the Senior Management Team and determine if the data subject, prime contractor and/or the ICO need to be informed of the breach.
- LM will then inform the data subject and prime contractor of the breach if required.
- SMT will then inform the ICO of the breach if required.
- Remedial actions to either close the breach and re-acquire control of the breached details or minimise impact of the breach will then be taken in concert with third parties as needed.
- Data breach log will be completed with remedial actions and all evidence will be stored in SharePoint and, if required, sent to the prime contractor.
- Actions will be taken and documented to prevent reoccurrence of the breach in future.

Sales and Marketing

Portland Training operates a strict opt in policy when contacting individuals to carry out sales and marketing activities with personal data. Portland Training provides privacy notices to all learners and employers with whom it engages to give individuals the opportunity to opt in. Our privacy notices provide clear and concise information of how we process personal data. Where consent is not given this is recorded within our MI System and all employees of Portland Training are required to act in accordance with this decision.

Data we hold for employers that does not identify an individual (e.g a generic company email address info@exampleorganisation.co.uk) is not personal data and so not covered under GDPR.