Oxford Professional Education Group

January 2020

Reviewed January 2024

Review Date Jan 2025

Reference number 4

GDPR Data Protection Policy

Introduction -The 2018 Data Protection Act and General Data Protection Regulations (GDPR) regulates how organisations may use personal data and protects the rights of individuals with regard to the use of their personal data.

The Act re-enforces 6 principles that apply to the use of personal data.

The Data Protection Act principles are:

• The processing of personal data must be lawful, fair and transparent;

• The purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and must not be processed in a manner that is incompatible with the purpose for which it is collected;

• Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed;

• Personal data undergoing processing must be accurate and, where necessary, kept up to date;

• Personal data must be kept for no longer than is necessary for the purpose for which it is processed;

• Personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data;

The use of personal data is also governed by other statutory and common law requirements, including the laws of confidence and defamation. OXPEG is committed to ensuring that its use of personal data is fully compliant with the law and best practice and to this end has approved this Data Protection Policy.

Objectives

The purpose of this policy is to set out clearly OXPEG's Policy in respect of Data Protection and the procedures to be followed by OXPEG staff and Learners.

Scope

This policy applies to:

• all Learners;

• permanent, fixed term and temporary staff;

• third party representatives;

• partners;

• contractors and sub-contractors;

• consultants;

• agency workers;

• volunteers;

• apprentices;

• agents;

• sponsors engaged with OXPEG.

Personal & Sensitive Data

Personal Data is information that relates to an identified or identifiable individual and could be as simple as a name, address or tel. no, or other identifiers such as a Learner or staff ID no, Unique Learner Number, name abbreviations, an IP address or a cookie identifier.

If it is possible to identify an individual directly from the information processed, then that information may be personal data.

If an individual cannot be identified directly from the information, then it should be considered whether the individual is still identifiable. OXPEG Staff and Learners should take into account the information being processed together with all the means reasonably likely to be used by a person to identify that individual.

If Information that seems to relate to an individual is inaccurate (i.e. it is factually incorrect or is about a different individual), the information is still personal data, as it relates to that individual.

Special Category Data (Sensitive Data)

Special category data is more sensitive, and so needs more protection.

Special category data may include:

• race;

• physical or learning disabilities

• politics;

• religion;

• genetics;

• biometrics (where used for ID purposes);

• health;

• sexual orientation.

This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Data Breaches -Definition of a Data Breach

An event which has caused or has the potential to cause damage to an individual's or OXPEG's information assets or reputation.

Examples are:

• Accidental loss or theft of personal data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick);

• Unauthorised use of personal data;

• Access to or modification of data or information systems;

• Accidental or deliberate sharing of user login details to gain unauthorised access to systems;

• Accidental or deliberate unauthorised disclosure of personal data, sensitive or confidential information;

• Email sent to an incorrect recipient;

• Document posted to an incorrect address or addressee;

• Accidental disclosure of user login details;

• Equipment failure;

• Malware infection;

• Disruption to or denial of ICT services.

Data Breach Reporting

When a member of staff or learner suspects a data breach, they, should immediately notify OXPEG Data Protection Director, Rosemary Craig, with full details of the breach. If the member of staff or learner has been the cause of the breach or part of a process that has led to the breach, the person should not continue with that process until investigation has completed.

The Data Protection Director will investigate the nature of the breach, the type of data involved, and where personal data is involved, who the subjects are and how many personal records are involved. The investigation will consider the extent of a system compromise or the sensitivity of the data involved, and a risk assessment will be performed as to what might be the consequences of the incident; for instance whether harm could come to individuals or whether data access or ICT services could become disrupted or unavailable.

• Take appropriate action to prevent the breach from escalating;

• Inform those individuals without undue delay if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms;

• Keep a record of the data breach regardless of whether OXPEG is required to notify the ICO;

• Assess whether the ICO should be notified of the breach within 72 hours of becoming aware of the breach, where feasible.

If the investigation finds a possible breach, then depending on the importance further advice maybe sought from the ICO. The Data Protection Director reserves the right to seek the advice from the ICO on any matter that is not trivial.

If the DPD is satisfied that the integrity of OXPEG is still intact, the breach can be dealt with internally. A review of internal procedure and process may be needed,

or a more detailed investigation may be carried out. All breaches will be reported to SMT and the wider OXPEG Management Team.

A failure to report a breach when required to do so could result in a fine as well as a fine for the breach itself. Fines may be imposed by the ICO amounting to 10 million euros or 2 per cent of global turnover.

Responsibilities

This part of the Policy identifies the Data Protection responsibilities of various members of staff and learners.

The Senior Management Team (SMT) and OXPEG Middle Management Team is committed to ensuring that OXPEG is fully compliant with the law and best practice for handling personal information. To this end the SMT and OXPEG Middle Management Team will:

• Approve OXPEG policies & procedures for handling personal data;

• Allocate resources (staff time and budget) to enable the Data Protection Action Plan included in the Overall Annual Development Plan to be delivered and compliance of the Data Protection legislation;

• Determine OXPEG's Records Management and Information Strategies concerning how information, including personal data, is organised, categorised, stored and retrieved;

• Ensure all OXPEG staff and Learners receive Data Protection training.

The Data Protection Director along with the Quality and Compliance Manager will be responsible for maintaining OXPEG's Data Protection system (its policies and procedures) as outlined below:

• Maintain OXPEG's Data Protection Registration with the ICO;

• Monitor ICO guidance, data protection legislation and GDPR;

• Make recommendations to the Middle Management Team on good practice and Data Protection policy;

• Provide training, guidance, disseminate information and advice on any specific Data Protection issues;

• Deal with Subject Access requests and co-ordinate responses to complaints that have a bearing on other data subjects' rights (unwarranted substantial

damage or distress; direct marketing; rectifying, blocking, erasing & destroying inaccurate personal data and disputed cases of inaccuracy or other alleged breaches);

• Manage data breach process;

• Co-ordinate and advise on all non-routine requests for disclosure of personal information;

• Investigate personal data breaches in line with Data Protection legislation and General Data Protection regulations;

• Undertake periodic data protection audits and Privacy Impact Assessments;

• Review OXPEG policies and procedures in line with The Data Protection Action 2018 and GDPR;

• Maintain OXPEG Data Asset Register.

Responsible Managers

Personal data is processed across the breadth of OXPEG's normal everyday activities. Good personal data handling is one aspect of what employees need to do to deliver excellent services to learners and internal customers. The key to achieving high standards in handling personal information is recognising that the primary responsibility for complying with legislation and good practice lies with those staff and managers who are responsible for deciding how in practice personal information will be used. The line managers of departments who process personal information are the responsible managers for this policy.

Responsible Managers will, in respect of their departments:

• Ensure that they are satisfied with the legality of holding the information and how it is used;

• Make appropriate provision for the security of both manual and computerised personal data where held locally (Back-up, contingency plans for catastrophic failure/migration of data to new systems, access to physical environment, locked files, guidelines on processing off-site, secure disposal etc). The security arrangements for computerised personal data must comply with OXPEG's IT Policy;

• Ensure Staff only have access to data including network drives required for their role;

• Ensure that staff with access to personal data receive appropriate guidance and training covering:

- The security arrangements for the data;
- How personal data is to be collected and recorded including approved sources;
- How consent is to be obtained where this is the ground for processing personal information;
- The information data subjects are entitled to receive under the Fair Processing Code and that application forms include this information;
- Any permitted routine disclosures of the data and how to respond to other requests for disclosure;
- Procedures for regularly reviewing personal data to check that it is adequate, accurate, up to date, not excessive and deleted when no longer needed;

• Refer any non-routine requests for disclosure to the Data Protection Director;

• Promptly inform the Data Protection Director of any requests for subject access so that they can be responded to within the appropriate time limits;

• Be aware of data subjects rights to compensation in certain cases and their right to rectify, block, erase & destroy inaccurate personal data and inform the Data Protection Director of any complaints alleging breaches of the Act or any cases where the data subject's complaint of inaccuracy is disputed;

• Ensure that personal data is not transferred outside the EEA other than in accordance with the Act;

• Ensure that any processing of personal data that is carried out by a contractor on behalf of OXPEG is subject to a written contract that requires the data processor to act only on instructions and makes appropriate provision for the security of the data;

• Report any suspected data breach to the Data Protection Director Director;

• Retain and archive personal data in line with the Retention and archiving section of this policy.

Systems and Services (In conjunction with 3rd parties)

All staff and users of personal data have some responsibility for the security of that data. IT services have an important role in ensuring the security of computerised data.

In particular they will:

• Undertake a Data Privacy Impact Assessment (DPIA) for the introduction of any potential high-risk situation for example where new technology is being deployed or where a profiling operation is likely to significantly affect individuals. If the DPIA indicates high risk processing this will be discussed with the Senior Management Team which may result in the ICO being consulted;

• Consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data;

• Be responsible for advising OXPEG on the state of technological development with regard to IT security;

• Back up data on OXPEG's servers and IT systems;

• Implement virus detection software and measures to prevent malicious software spyware, and hacking to identify potential data breaches;

• Place restrictions on access so that individuals only have access to personal data in which they have a legitimate interest;

• Require the use of complex passwords and ensure that they are changed regularly;

• Promote and police policies for use of OXPEG systems and IT facilities including e-mail, intra and Internets that ensure compliance with OXPEG's Data Protection obligations and investigate breaches of IT security and report suspected data breaches to the Data Protection Director;

• Ensure all Apprenticeship laptops have BitLocker installed (extension planned within overall Annual Development Plan)

Human Resources

An important aspect of security is ensuring the reliability of staff. The Human Resources team can contribute to this aim in a number of ways. They will:

• Ensure that OXPEG's Employment Practices are consistent with the Information Commissioner's Employment Practices Code of Practice using external advisers

• Ensure that the Data Protection obligations of staff are reflected in OXPEG's Disciplinary Procedures and contracts of employment;

• Ensure that all staff are aware of the types of personal information that OXPEG will routinely make public (e.g. name, post, academic qualifications, OXPEG telephone and e-mail) and that individuals have the right to object to that disclosure where they consider it may cause them substantial damage or distress;

• Provide advice to responsible managers and others on the application of the pre and post -employment vetting process;

• Report any suspected personal data breach to the Data Protection Director.

Marketing

The SMT member who is responsible for marketing will ensure that explicit consent is obtained for the purpose of marketing courses and events at OXPEG and photography and video usage.

All Staff

All staff are likely to use and have access to some personal data in the course of their duties, for example other staff, learners or members of the public.

They will:

• Respect the privacy and confidentiality rights of all data subjects. In particular they should be careful that personal data are not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party. (Unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases). This includes making sure that casual access to data is not possible, (for example by members of the general public seeing computer screens or printouts);

• Only use personal data for approved purposes and ensure that they comply with any instructions and guidelines they are given about the use of personal data;

• Inform the 'Responsible Manager' of any proposed new uses of personal data;

• Keep all personal data secure and not remove it from OXPEG premises without the permission of the appropriate 'Responsible Manager';

• Comply with all OXPEG policies regarding the use of IT facilities, e-mail and Inter/Intranets;

• Ensure USB memory sticks and personal devices are encrypted and/or password protected;

• Check that the information they provide to OXPEG in connection with their employment is accurate and up to date and inform OXPEG of changes to or errors in information held;

• Report any suspected personal data breach to the Data Protection Director;

• Ensure the email and communication etiquette is followed during all communication;

• Contact the Data Protection Director with any data protection queries;

• Ensure there is no sub processing of data without written authorisation from the Senior Management Team.

Learners

Learners will not normally process personal data in the course of their studies or in other ways on behalf of OXPEG. However, where from time to time this happens, they will need to inform their Tutor/Trainer/Assessor and comply with the Guidelines and any other instructions given to them.

At all times learners will:

• Respect the privacy and confidentiality rights of all data subjects;

• Not seek to use or gain unauthorised access to personal information;

• Comply with all OXPEG policies regarding the use of IT facilities, e-mail and Inter/Intranets;

• Check that the information they provide to OXPEG in connection with their studies is accurate and up to date and inform OXPEG of changes to or errors in information held;

• Report any suspected personal data breach to the Data Protection Director;

• Contact the Data Protection Director with any data protection queries;

• Ensure the communication etiquette is followed during all communication**;**

Misuse of Data

Disciplinary action, including dismissal or termination of contract may be taken against any employee or contractor who contravenes any instruction contained in, or following from, this Data Protection Policy and Guidelines issued by OXPEG. Upon discovering that this Policy is not being complied with, or if an intentional breach of the Data Protection Principles has taken place, the Data Protection Director in consultation with the senior team, shall have full authority to take such immediate steps as considered necessary.

Data Retention and Archiving - Data Retention Periods

Health and Safety /HR & Contractor Records

Staff bank contact information	Duration of contract + 3 months
Annual leave records (overtime and time in lieu)	1 year (after leave date)
Initial Training Plan/Induction and Staff or Professional Development Logs and/or Appraisals – staff/contractors	Kept during employment or contract and then for 7 years after
Sickness Records (HR	7 years
Mitigation circumstances information, medical records, police records, any evidence for a Mitigating Circumstance HR related matter or claim	6 years
Job descriptions	Indefinitely
Staff Photo for ID	For the duration of the employment
CV	6 months after staff leave
Copies of passports	Duration of employment
Visitor Log	1 month
Conflict of Interest register	3 years

Property Matters	12 years where they relate to title for existing assets
Unsuccessful job applications	6 months
Successful job applications	Duration of employment + 7 years
Safeguarding Files	7 years (This period can be extended if extension criteria is match – Retention Policy)

Learner Support

Indication of Support form and copy (IOS)	Duration of course NON-**Apprentices only**
Summary of Support form (SOS) Current academic year	3 years where additional agencies are involved
Learner difficulty declaration information (for learners not enrolling)	3 months
Learner Difficulty declaration Information	(deleted every December the following academic year) ALS
Registers including Learner names	7 years
Communication to Learners	7 years
Complaints and Grievances	7 years
Disability Records	7 years
Learner Counselling Referral records	7 years
Mitigation circumstances information, medical records, police records, any evidence for a Mitigating circumstance claim for	7 years

Learner Disciplinary letters/misconduct minutes	7 years
CRM Pipeline Employer details for prospective employer customers	2 years

Quality /Delivery

Learning audit /deep dive evidence or Observation records non-Apprentice learners	3 years
Assessment records	3 years
Learner Feedback Duration of course	3 years
Learners marks and results	7 years
IQA Sampling Plans	7 years
Learner Progression Information	1 year in full detail (merged into summary to keep for 3 years as trend data)
Class Registers / Contact sheets for funded learners (Apprenticeships)	31th December 2030.
Copies of Examination Records for funded learners (Apprenticeships)	31th December 2030.
Apprenticeship & non-Apprenticeship course learner work evidence	Kept electronically for 3 years

Finance Documents

Finance documents	7 years
General Financial Correspondence	2 years
Learner Bank Details for Refunds (held in Finance)	7 years
Records for MIS	31st December 2030

Marketing Documents

Images and videos of learners	5 years permission requested
Learner Photos for Prospectus	5 years permission requested
Prospective Learners information	2 years
Client mailing listing information	2 years

Data Retention Periods – Apprenticeships

Copy of Application Form for Apprenticeships	6 Years
Non-Starters (Individuals)	3 months
Non-Starters (Employers)	2 years
Interview/Enquiry Form - name/Learner ID/GCSE results	6 Years
Copy of Enrolment Form - personal data	6 Years

Original and any Copy of Indication of Support Needs Form	6 Years
Contract - Employer/Apprentice	6 Years
Vacancy Matching Application	6 Years
ILP/Reviews	6 Years
Grant or Incentive letters or evidence while being processed by MIS or Main provider	6 Years
CRM Pipeline employer details for prospective employers	2 years
Occasional apprentice details for sending out application while being processed email enquiries/telephone notes	3 months
Copies (Not original records) of ALS/health plans/care plans/safeguarding	6 Years
Copy of Apprenticeship Copy of Apprenticeship Completion Form Length Completion Form	Length of course + 1 year (any original must be kept for 6 years)
Contacts/comments sheet - emails from parents/employers	6 Years
Employer meeting minutes	6 Years
Course Review/progression review/Apprenticeship Learning Visit	6 years
Copies of Exam Booking Forms	6 years
Copies of Certification info/certificates/ACE	6 years
Copy of Break on learning / Returning Forms End of course Unemployed:	6 years

Initial eligibility assessment/criminal record	
Employer evaluation/impact surveys	6 years
Telephone Survey Audits	6 years
Evaluation Forms - Learner name	6 years
Tutor/Trainer Assessor Observations	6 years
EQA Reports	6 Years
Minutes of Assessor/IQA meetings	6 Years
Attendance records	6 Years
Progression Trackers - Learner names/employer/progress	6 Years
Apprenticeship Contractor Invoice payment records	6 Years
Learner Database archived electronically – indefinitely Action & Assessment Plans	6 Years
Sub-Contractor Meeting minutes	6 Years
SAR and QIP Reports	6 Years

Records for archiving should be filed with details of the owner and destroy date in line with the retention period listed above.

The Head of each Department is responsible for maintaining a record of the data retained within the archive in line with OXPEG data retention periods.

Privacy Notices

Details of staff and Learner privacy statements are available on OXPEG the website. These set out how personal information is used and in particular:

• Why OXPEG collects personal information;

• The personal information that OXPEG collects

- How OXPEG collects the personal information;
- How the personal information is stored;
- How OXPEG uses the personal information;
- The legal basis on which OXPEG collects and use personal information;
- Who has access to personal information;
- How OXPEG shares personal information;
- The transfer of personal information outside of Europe;
- How OXPEG protects personal information;
- How long OXPEG retains personal information;
- An individual's rights over personal information.

General Enquiries

A learner or member of staff can ask OXPEG to see information that OXPEG holds about them by making a general enquiry to the appropriate department, such as how much they owe OXPEG in fees if they are a Learner. OXPEG may carry out identity checks to ensure that they are who they say they are, but in general, the information will be disclosed to them.

Data Subject Access Requests

An individual also has a legal right under the Data Protection Act 2018 and GDPR to be informed about whether any information is held about them and to see a copy of it. This is known as a right of Subject Access. OXPEG Learners and Staff have the right to:

- A copy or description of the information that OXPEG holds about them. This information may be held electronically (for example on computer, closed circuit TV, video or audio recordings) or in paper records. OXPEG will provide the information in an electronic format where possible. Paper records will be scanned unless the original paper copy is requested.

Learners have the right to see some exam-related information, such as marks, examiner's comments and minutes of examination appeals panels. If a learner asks for exam results before they have been announced, OXPEG will respond within 30 days from when the individual's results are published.

There may be circumstances where not all information about an individual can be provided. There may be exemptions under the Act that OXPEG needs to apply, these are:

• Crime prevention and tax collection;

• Immigration control;

• Required by law / legal proceedings;

• Regulatory functions;

• Third party data;

• Management forecasts / negotiations;

• Confidential references;

• Exams, scripts and marks;

• Health, social work, child abuse and education records (serious harm).

Timescale

OXPEG will endeavour to reply promptly to the request within one month, provided that OXPEG has evidence of the individual's identity and enough information to search for the -information. Where OXPEG asks for additional information, the one-month countdown starts when the additional information has been received.

Where OXPEG is not taking action in response to a request, OXPEG will explain why to the individual, informing them of their right to complain to the supervisory authority without undue delay and at the latest within one month.

Cost

There will be no cost for a subject access request unless the request is manifestly unfounded or excessive by the data subject such as a repeated request.

Where a request from a data subject is manifestly unfounded or excessive, OXPEG may charge a reasonable fee for dealing with the request or refuse to act on the request.

How to Make a Subject Access Request

Data Subject Access should be emailed or sent in writing to OXPEG Data Protection Director, Rosemary Craig.

The individual will need to provide:

• The necessary information from the individual to confirm the individual identity. Please provide a photocopy of any of the following items:

> Birth certificate, marriage or civil partnership certificate, driving licence (photo card or paper), passport, two different utility bills (for example gas, electricity or water).
>
> Sufficient information from the individual to help OXPEG locate the information that the individual has requested.

The information that the individual provides will be used to manage and administer the individual's request and carry out searches for information that is held about the individual.

Requests on Behalf of Other People

An individual may make an access request on behalf of another person. OXPEG will send them a copy of information held only with the consent and authorisation of the subject.

If a parent or guardian makes a request on behalf of an individual person under 18, OXPEG may make additional enquiries to confirm that they have parental responsibility before releasing information. This may involve discussing the request with staff members within OXPEG or with relevant external organisations.

Information That Relates to Other People

Under the Data Protection Act 2018, an individual is only entitled to see information that is held about them. There may be occasions when information about other people is held on the individuals' records. OXPEG may inform the third party that a subject access request has been made and inform them that their personal data is contained within the request. OXPEG may contact the third party for their consent to release information that identifies or relates to them. OXPEG is entitled to withhold information about the subject if the third-party consent has been withheld or cannot be obtained.

Automated Decision Taking

OXPEG does not make decisions solely based on automated decision-making.

Correction or Deletion of Inaccurate Information

On receipt of a correction or deletion of inaccurate information OXPEG will investigate the inaccuracy and any changes will be made within one month.

OXPEG Forms and Procedures

All OXPEG forms and procedures must be reviewed by OXPEG Data Protection Director or Quality and Compliance Manager who will assess for Data Protection Act 2018 and GDPR requirements.

All OXPEG forms must include:

• Why OXPEG is collecting the data;

• How long it is retained and that it is destroyed;

• Where it is stored (electronically and paper based);

• Who has access to it;

• Who it is shared with.

OXPEG Procedures

OXPEG procedures and amendments must be approved by the Data Protection Director or the Quality and Compliance Manager as part of a wider SMT group approval.

Glossary of Terms

Data is information, which is processed automatically (by a computer), or is manual data which forms part of a relevant filing system. A relevant filing system is a system that is structured either by reference to an individual or by criteria relating to individuals so that specific details relating to a individual may be easily selected from that system. Data can be written information, photographs, or information such as fingerprints or voice recordings.

The Freedom of Information Act extends the definition of data to include unstructured manual data that is held for personnel purposes - where employees request to have access to their own personal data.

Personal Data is information that relates to a living individual who can be identified from that data and other information in or likely to come into the

possession of the Data Controller (OXPEG). The Act does not apply to statistical or anonymised information where individuals cannot be identified, neither does it apply to people who are deceased.

Processing is anything done with the data including holding and viewing data. It includes:

• obtaining;

• reading and consulting;

• holding;

• disclosing;

• amending;

• transferring;

• collating and compiling;

• blocking, deleting or destroying information.

The Data Subject is the individual who is the subject of personal data. This will include staff, learners, suppliers of goods and services including delivery contractors etc.

The Data Controller is the legal person or body who (either alone or jointly or in common with other

persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. OXPEG is the Data Controller.

Data Processor is any person other than an employee of the Data Controller who processes data on behalf of the Data Controller.

We do not sell your personal data for commercial purposes and will only disclose it if required by law, necessary to arrange your event/training attendance, or with your consent.

To contact Oxford Professional Education Group with a data protection query regarding the processing of your personal data, please email **enquiries@oxfordpeg.com**.

Further Details of our Processing

We believe that all these purposes are justified on the basis of our legitimate interests in running and promoting the company and our contractual requirements to deliver the agreed services to you, the exception is for sending email marketing which we carry out on the basis of consent.

Clients, Delegates and Learners

As a client, delegate or learner, we will hold the following information about you:

- Your name and contact information;
- Personal information including special needs / requirements;
- Information about your business activities and job role;
- Information and documents relating to the course we are providing, including communications with you;
- Billing and payment information.

We use the information we hold about you and your business, both personal and otherwise, to give you the best service we can.

We also use your information to invoice you, and to keep track of payments that you make.

We currently use the following third-party online tools to administer the courses effectively:

- Salesforce CRM to record contact information and to project manage our contracts with you. Salesforce is hosted in Germany. For more information, please view Salesforce's **Privacy Policy.**
- Oxcom Learning (MoodleRooms) to access all course information and materials. For more information please view **Privacy Policy** and **here.**
- SagePay for payments made online. For more information, please view SagePay's **Privacy Policy.**
- Zapier for collating groups of delegates for Learner support purposes. For more information, please view Zapier's **Privacy Policy.**

- Intuit Quickbooks Accounting to manage your billing and payment details. For more information, please view Intuit Quickbooks **Privacy Policy.**
- Xero Accounting software to manage your billing and payment details. For more information, please view Accounting software to manage your billing and payment details. For more information, please view Xero Privacy Policy.
- Apprentices and associated assessors will use OneFile software to track progress. For more information, please view OneFile Privacy Policy.
- G suite business cloud. For more information, please view G Suite **Privacy Policy.**
- After a module or a course, you may be asked for feedback via Survey Monkey. For more information, please view Survey Monkey **Privacy Policy.** Adobe Connect for webinars during your course. For more information, please view Adobe Connect **Privacy Policy.**

Job Applicants, Associates, Our Current and Former Employees and Contracting Training Staff

As a job applicant, associate, current or former employee or a contracting trainer, we will hold the following information about you:

- Your name, contact information and CV;
- Proof of your identity;
- Proof of your qualifications;
- Bank details (if successful to process salary payments) and National Insurance;
- Emergency contact details.

All the information you provide during the recruitment process will only be used for the purpose of progressing your application, or to fulfil legal or regulatory requirements if necessary.

We will not share any of the information you provide during the recruitment process with any third parties for marketing purposes. The information you

provide will be held securely by us whether the information is in electronic or physical format.

We will use the contact details you provide to us to contact you to progress your application. We will use the other information you provide to assess your suitability for the role you have applied for.

All employees and subcontractors will be trained in GDPR responsibilities and all have signed confidentiality agreements at contract stage.

Visitors to our Website

When you visit our websites, we use a third-party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to various parts of the website. The information is only processed in a way which does not identify anyone, except for IP address.

To opt-out of being tracked by Google Analytics across all websites, You Tube and Facebook. For more information please visit **http://tools.google.com/dlpage/gaoptout**.

Cookies

We use cookies to compile visitor statistics such as how many people have visited our website, what type of technology they are using (e.g. Mac or Windows which helps to identify when our site isn't working as it should for technologies), how long they spend on the site, what page they look at etc. This helps us to continuously improve our website. These analytics programs also tell us if, on an anonymous basis, how people reached this site (e.g. from a search engine) and whether they have been here before.

Google Analytics

__utma
Collects data on the number of times a user has visited the website as well as dates for the first and most recent visit. Used by Google Analytics.
2 years

__utmb
Registers a timestamp with the exact time of when the user accessed the website. Used by Google Analytics to calculate the duration of a website visit.
Session.

__utmc
Registers a timestamp with the exact time of when the user leaves the website. Used by Google Analytics to calculate the duration of a website visit.
Session.

__utmt
Used to throttle the speed of requests to the server.
Session.

__utmv
Saves user-defined tracking parameters for use in Google Analytics.
Session.

__utmz
Collects data on where the user came from, what search engine was used, what link was clicked and what search term was used. Used by Google Analytics.
6 months

Google's privacy policy

Remarketing Cookies

You may notice that sometimes after visiting a site you see increased numbers of adverts from the site you visited. This is because advertisers, including ourselves pay for these adverts. The technology to do this is made possible by cookies and as such we may place a so-called remarketing cookie• during your visit. We use these adverts to offer special offers etc to encourage you to come back to our site. Don't worry we are unable to proactively reach out to you as the whole process is entirely anonymised.

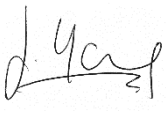
__unam
Saves the user's navigation on the website including what pages have been viewed and how long the browser has been used to view each page.
9 months

Most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, including how to see what cookies have been set and how to manage and delete them, visit **www.allaboutcookies.org**.

Further Information, Links and Your Rights

As an individual whose personal data is processed by Oxford Professional Education Group you have these rights (**https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr)**. If, at any time, you want to verify, update or amend your personal data please email support@oxfordpeg.com

You also have the right to lodge a complaint about our processing with the UK's Information Commissioner's Office (**ICO).**

Signed: 

Date: January 2022