1.Statement of intent

Outreach Rescue trading Company Ltd. is required to keep and process certain information about its staff members and customers in accordance with its legal obligations under the General Data Protection Regulation (GDPR).
The Company, from time to time, be required to share personal information about its staff or customers with other organisations, for Diploma and Certificate courses with the relevant awarding body (Coventry University) or other organisations.
This policy is in place to ensure all staff are aware of their responsibilities and outlines how the company will follow the 8 core principles of the Data Protection Act.
Organisational methods for keeping data secure are imperative, and Outreach Rescue Trading Company Ltd believes that it is good practice to keep clear practical policies, backed up by written procedures.
This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2. Scope of the Policy

The purpose of this policy is to ensure that the company, its comply with the provisions of the Data Protection Act 1998 when processing personal data. Any serious infringement of the Act will be treated seriously by the company and may be considered under disciplinary procedures.

This policy applies regardless of where the data is held, electronically or on paper, even if it is held on personally-owned equipment or outside company property.

The company is required to adhere to the eight principles of data protection as laid down by the Act. In accordance with those principles personal data shall be:

1. Processed fairly and lawfully
2. Processed for specified purposes only
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept longer than necessary
6. Processed in accordance with data subjects' rights
7. Processed and held securely
8. Not transferred outside the countries of the European Economic Area without adequate protection.

3. Responsibilities

[a] Company responsibilities

As the Data Controller the company is responsible for establishing policies and procedures in order to comply with the requirements of the Data Protection Act, and within the requirements of GDPR.

[b] Governance Team responsibilities

The Governance Team holds responsibility for:

The Companies Data Protection notification. Details of the companies' notification are published on the Information Commissioner's website. Anyone who is, or intends, processing personal data for purposes not included in the notification should seek advice from the Governance Team;

drawing up guidance, giving advice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information;

the appropriate compliance with subject access rights and ensuring that data is released in accordance with subject access legislation under the Data Protection Act 1998;

ensuring that any data protection breaches are resolved, catalogued and reported appropriately in a swift manner and in line with guidance from the Information Commissioner's Office;

investigating and responding to complaints regarding data protection including requests to cease processing personal data.

[c] Staff responsibilities

Staff members who process personal data about students, staff, applicants, alumni or any other individual must comply with the requirements of this policy.

Staff members must ensure that:

all personal data is kept securely;

no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;

personal data is kept in accordance with the Company retention schedule, and as required by law (ie.

any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Governance Team;

any data protection breaches are swiftly brought to the attention of the Governance Team and that they support the Governance Team in resolving breaches;

where there is uncertainty around a Data Protection matter advice is sought from the Governance Team.

When members of staff are responsible for supervising students doing work which involves the processing of personal information (for example in research projects), they must ensure that those students are aware of the Data Protection Principles, in particular, the requirement to obtain the data subject's consent where appropriate.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Governance Team.

[d] Third-Party Data Processors

Where external organisations are used to process personal data on behalf of the company, responsibility for the security and appropriate use of that data remains with the company.

Where a third-party data processor is used:

a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;

reasonable steps must be taken that such security measures are in place;

a written contract establishing what personal data will be processed and for what purpose must be set out;

a data processing agreement, available from the company, must be signed by both parties.

For further guidance about the use of third-party data processors please contact the administration team.

[e] Contractors

The Company is responsible for the use made of personal data by anyone working on its behalf. Contractors must ensure that they are appropriately vetted for the data they will be processing. In addition, managers should ensure that:

any personal data collected or processed in the course of work undertaken for the Company is kept securely and confidentially;

all personal data is returned to the Company on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed, and the notification given to the company in this regard;

the Company receives prior notification of any intent of disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;

any personal data made available by the company, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from the company;

all practical and reasonable steps are taken to ensure that contractors do not have access to any personal data beyond what is essential for the work to be carried out properly and safely.

[f] Customer responsibilities

Customers are responsible for:

familiarising themselves with the Data Protection Agreement provided when they register with the Company; ensuring that their personal data provided is accurate and up to date.

4. Data Retention policy

Type of Record	Retention Period	Reason for Length of Period
Personnel files including training records and notes of disciplinary and grievance hearings	5 years from the end of employment	References and potential litigation.
DBS certificate information	6 months after the recruitment or other relevant decision has been made	HMG Code of Practice on handling of DBS certificate information (14 November 2012)
Application forms/interview notes	At least 6 months from the date of the job advertisement	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	6 years from the date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from the date of the redundancies	Limitation Act 1980
Income Tax and NI Returns, including correspondence with tax office	At least 3 years after the end of the tax year to which the records related	Income Tax (Employment) Regulations 1993
Statutory Maternity and adoption Pay records and calculations	3 years after the end of the tax year in which the maternity period ends	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	3 years after the end of the tax year to which they relate	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Individual pension entitlement and contribution history	As long as there is a member or dependant liability	
Accident books, and records and reports of accidents	6 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985
Health Records	During employment	Management of Health and Safety at Work Regulations

Type of Record	Retention Period	Reason for Length of Period
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	Control of Substances Hazardous to Health Regulations 1999
Ionising Radiation Records	At least 50 years after last entry	Ionising Radiations Regulations 1985
Student records, including academic achievements and conduct	At least 6 years from the date that the student leaves, in case of litigation for negligence.	Limitation period for negligence.
	2 years from graduation / course completion for Exam scripts, as well as dissertations, portfolios and original compositions	Reasonable period to cater for student enquiries, which may need reference to examination scripts.
	At least 10 years for personal and academic references.	Permits institution to provide references for a reasonable length of time.
	Certain personal data may be held in perpetuity.	While personal and academic references may become 'stale', some data e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, data relating to him/her ceases to be personal data.
	Vocational Qualifications	2 years from the qualifications expiry date.
Moodle course data, including student online activity records and uploaded coursework	2 years from graduation / course completion.	Reasonable period to cater for student enquiries, which may

Type of Record	Retention Period	Reason for Length of Period
		need reference to multiple choice questions (MCQs).
Moodle course archives	A snapshot of Moodle to include individual course archives and a copy of the master MySQL database will be taken on or around 1st September annually and retained for 6 academic years. These snapshots will be stored offline.	Supplements (but does not replace) existing processes for the local archiving of assessed student work. Enables the company to respond to queries relating to user activity or behaviour through the interrogation of associated activity logs. Functions as a historic backup in the event of inadvertent or deliberate course removal or modification.
Details of programmes, courses, modules and units of study, including module descriptors ('current course materials')	At least 6 years after the student enrolled on those modules leaves	Module descriptors and programme specifications form part of the recognised learning that the student has completed. In the event of a challenge to the learning that the student has completed, details of past specifications need to be retained to support any enquiries or challenges.
Sampled assessments allowing for comparisons of standards over time to be made	In perpetuity	Benchmarking of practice requires historical samples to show trends and patterns
Assignments submitted to Turnitin	In perpetuity	Academic integrity is integral to academic teaching and research. Besides stressing its importance in education by, for example, teaching students to properly cite material, it is crucial to be able to inspect for cases of plagiarism. The large number of students enrolled in various programmes makes plagiarism detection software essential. The use of such

Type of Record	Retention Period	Reason for Length of Period
		plagiarism detection software forms part of the Regulations Governing Fraud and Plagiarism and the Teaching and Examination Regulations. Turnitin will not obtain ownership rights and is held to respect the intellectual property of the submitter.

5. Subject Access Requests

The Company is required to permit individuals to access their own personal data held by the company via a subject access request. Any individual wishing to exercise this right should do so in writing to the Administration Team and a charge may be made for this request. A standard form is available from the Administration Team, it is not however required.

The request should be made, in writing, e-mail is acceptable. If it is not possible to make a written request an exception for a verbal SAR can be made at the discretion of the Governance Team.

The company aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within the 40 calendar day limit set out in the Data Protection Act.

Individuals will not be entitled to access information to which any of the exemptions in the Act applies. However, only those specific pieces of information to which the exemption applies will be withheld and determining the application of exemptions will be made by the Governance Team.

A charge of £10 will be applied for collation of data unless waivered at the governance team's discretion.

6. Data protection breaches

Where a data protection breach occurs, or is suspected, it should be reported immediately to the Outreach Rescue Trading Company Ltd administration team by e-mail to:

enquiries@outreachrescue.com with the subject line 'Data Breach'.