Data Protection Policy

Date	Version	Edit and Agreed	Staff
2020	1	Y	HE, LK
2021	2	Y	HE, LK
2022	3	Y	HE, LK
2023	4	Y	HE, LK
2024	5	Y	HE, LK
2025	6	Y	HE, LK

Overview

Coast Tuition and Coast Tuition Community are committed to being transparent about how it processes personal data of its learners, workforce and meeting its data protection obligations. This Policy sets out the organisations commitment to data protection and individual rights and obligations in relation to personal data.

Data Protection Lead

The Data Protection Lead is the person with responsibility for data protection and compliance within the organisation. Questions about this policy, or requests for further information, should be directed to them.

The Data Protection Lead is:

Name: Helen Elcoate

Email Address: helen@coasttuition.co.uk

Phone Number: 07754270274

Data Protection Principles

Coast Tuition and Coast Tuition Community processes personal data in accordance with the following data protection principles. Personal data will:

- Be processed fairly, lawfully and transparently;
- Be collected and processed only for specified, explicit and legitimate purposes;
- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- Be accurate and kept up to date;
- Not be kept for longer than is necessary for the purposes in which it is processed; and
- Be processed securely.

Lawful Grounds for Processing

The lawful grounds for processing personal data are set out in Article 6 of the UK GDPR. At least one of these grounds must apply whenever personal data is processed:

a) Consent

The individual has given clear consent for their data to be processed for a specific purpose.

b) **Contractual Necessity**
The processing is necessary for the performance of a contract or to carry out specific tasks prior to entering into a contract.

c) **Legal Obligation Necessity**
The processing is necessary to comply with the law.

d) **Vital Interests Necessity**
The processing is necessary to protect the vital interests of the data subject or of another natural person.

e) **Public Task Necessity**
The processing is necessary so that you can perform an official function or task in the public interest and/or has a clear basis in law.

The lawful grounds for the personal data which Coast Tuition and Coast Tuition Community process is stated in the relevant privacy notice.

Personal Data

What is Personal Data?
Personal Data is defined by the UK GDPR as information which relates to a living person who can be identified or identifiable from the data, they are called the data subject.

This policy relates to all personal data whether it is stored electronically, on paper or in/ on any other materials.

Learners
We will process the following types of personal data:

- Personal information such as Name, address and date of birth
- Any data used to evaluate and consider the learners learning objectives such as exam results
- Parent/ carer contact details such as name, address, phone number and email address
- Attendance information
- Learner achievement records
- Learner registration records
- Photographs
- Any other category of personal data which may be collected from time to time

Employees
We will process the following types of personal data:

- Personal information such as name, address, phone number and email address.
- Payroll information which is National Insurance number, bank details, sex, and date of birth.
- Information collected through the recruitment process such as references, employment history and application forms.
- Information relating to disciplinary or grievance proceedings
- Training records
- Information relating to performance and behaviour at work.

- Emergency contact details
- Any other category of personal data which may be collected from time to time

What is Special Category Data?
Special Categories of Personal Data are types of personal data are types of personal data consisting of information about:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data
- Health
- Sex life and sexual orientation

Learners
We will process the following types of Special Category data:
- Education Health and Care Plan, if applicable
- Behavioural information
- Medical information
- Information relating to a disability
- Age, gender, nationality and ethnic origin
- Any information which would relate to Safeguarding

Employees
We will process the following types of Special Category data:
- Any sensitive information about employees health, is used to determine any reasonable adjustments to our processes to support you within employment.
- Past or current convictions where relevant due to the nature of the work we carry out with children and adults.
- Right to Work details
- Information about your gender, age and nationality.

What is Criminal Records Data?
Criminal records data applies to personal data relating to criminal convictions and offences, or related security measures.

This concept of criminal offence data includes the type of data about criminal allegations, proceedings or convictions.

We will process criminal records data in relation to the Disclosure and Barring Service for all employees working in regulated activity with children and vulnerable adults.

What is processing?
Processing means any operation which is performed on personal data such as:
- Collection, recording, organisation, structuring or storing;
- Adaption or alteration;
- Retrieval, consultation or use;

- Disclosure by transmission, dissemination or otherwise making available;
- Alignment or combination;
- Restriction, destruction, or erasure.

We will process personal data in line with our obligations under the UK GDPR and Data Protection Act 2018.

Accessing Personal Data
Employees shall only access personal data covered by this policy if they need it for their job role, or on behalf of the organisation and only if authorised to do so.

Sharing Personal Data

Learners
There will be times where we will need to share learner personal data with a School, Local Authority or regulatory bodies to carry out our legal obligations.

Employees
There will be times where we will need to share employee personal data with a School, Local Authority or regulatory body to carry out our legal obligations. We will also share employee personal data with relevant contractors where it is necessary as part of the employment contract.

For any personal data which is shared, we have the relevant data sharing agreements in place to protect your personal information.

Before sharing any data, employees must ensure that:
- They are allowed to share it
- That adequate security is in place to protect it
- The recipient is the correct recipient and they have the correct authority to process the data.

Data Security
Coast Tuition and Coast Tuition Community takes the security of personal data seriously. Everyone who works for, or on behalf of the organisation has responsibility for ensuring data is collected, stored and handled appropriately in line with this policy and relevant data protection legislation. We shall:

- Confidentially store paper records in a locked filing cabinet or drawers with restricted access.
- Ensure confidential paper records are not left in clear view anywhere with general access.
- Save digital data securely on the cloud which is regularly backed up externally.
- Only have access to documents which is relevant to the job role.
- Password protect all electronic devices to protect the information which is saved on the device.

- Where possible, ensure all electronic devices can be remotely blocked or deleted in case of loss or theft.
- Provide employees with their own secure login and individual password for electronic devices to be used by them only.
- Ensure documents containing personal data are password protected when sent by email, if there are unsecure servers between the sender and recipient.
- Blind copy email addresses when sending circular email messages to all learners or parent/carers to protect the recipients email addresses so that they are not disclosed to other recipients.
- Destroy any paper copies of data using a cross shredder when finished using it.
- Where personal information that could be considered confidential is taken off the premises, either electronically or paper, employees will take extra care to follow the same procedures e.g. lock and key. The person taking the data accepts full responsibility for the security of the data.
- Not save personal data on personal electronic devices.
- Report any breaches of personal data to the Data Protection lead as soon as possible.
- Where any deliberate or negligent breach of this policy occurs we may deal with this breach under the disciplinary policy.
- Remain confidential at all times when processing any personal data.

Some of the processing which Coast Tuition and Coast Tuition Community carries out may result in risks to privacy. Where processing would result in a high risk to individual rights and freedoms, the organisation will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks of individuals and the measures that can be put in place to mitigate those risks.

Data Breaches

A data breach is when a breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Examples of data breaches are *(this list is not exhaustive)*:

- Sending personal data to an incorrect recipient
- Loss of data where the individual is clearly identifiable
- Electronic devices containing personal data is lost or stolen
- Alteration of personal data without permission
- Access by unauthorised people
- Deliberate or accidental action (or inaction) by a person

If a data breach occurs, this must be reported to the Data Protection Lead as soon as possible. The Data Protection Lead will risk assess the incident to determine the appropriate action to be taken. If the incident could put the individual at significant risk of harm as a result of a data breach, the incident should be reported to the Information Commissioners Office (ICO) within 72 hours of the breach either taking place or the organisation being made aware.

All data breaches will be kept on an internal log, including those which are not reportable to the ICO, so that any decisions made to either report to the ICO or not are fully logged.

Data Subject Access Requests

Individuals can make a subject access request to find out what information the organisation holds on them. A data request should be made in writing, where possible, to the Data Protection Lead. Upon receipt, the Data Protection Lead will acknowledge your request and coordinate a response.

The organisation will have one calendar month, from the date of receipt, to respond to the request. If the request is complex, we may need to take extra time and can take up to extra two calendar months to respond.

There is no fee for making a Data Subject Access Request. However, if the request is manifestly unfounded or excessive, we may charge a reasonable administrative fee.

Data Subject Rights

Under the UK GDPR, individuals have the following rights:

The right to be informed – individuals have the right to be informed about the collection and use of personal information.

The right of access – individuals have the right to ask Coast Tuition and Coast Tuition Community for copies of their personal information.

The right to rectification – individuals have the right to ask for the correction of information which is believed to be inaccurate.

The right to erasure – individuals have the right to ask for personal information to be erased in certain circumstances.

The right to restrict processing – individuals have the right to ask for the restriction of processing of personal information in certain circumstances.

The right to object to processing – individuals have the right to object to the processing of personal information in certain circumstances.

The right to data portability – individuals have the right to ask that we transfer the personal information given to us to another organisation, or to the individual, in certain circumstances.

Any requests for the above, should be made to the Data Protection Lead.

Safeguarding

Coast Tuition and Coast Tuition Community understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping learners safe.

We will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a learner is shared with the relevant individuals or agencies proactively as soon as is reasonably possible.

We will aim to gain consent to share information where appropriate, however, will not endeavour to gain consent if to do so would place a learner at risk.

The organisation will manage all instances of data sharing for the purposes of keeping a learner safe in line with the Safeguarding Policy.

Retention Periods

Basic File Description	Relating to?	Retention Period
Pre-employment vetting information for successful candidates	Employees	Duration of employment + 6 years
Forms of Identity collected as part of enhanced DBS disclosure and Right to Work Checks	Employees	Duration of employment + 6 years
Employee File	Employees	Duration of employment + 6 years
Staff Training records in relation to children (e.g. safeguarding or other child related training)	Employees	Duration of employment + 40 years
Records relating to any allegation of a child protection nature against an employee	Employees	Until the persons retirement age or 10 years from the date of the allegation (whichever is longer)
Disciplinary Proceedings First Written Warning	Employees	Date of warning + 6 months
Disciplinary Proceedings Final Written Warning	Employees	Date of warning + 18 months
Payroll Data	Employees	Duration of employment + 6 years
Health and Safety Risk Assessments	Employees / Learners / Organisation	Life of risk assessment + 3 years *provided that a copy of the risk assessment is stored with the accident report if related to an incident*
Accident reporting records relating to individuals who are over the age of 18 at the time of the incident	Employees/ Learners	3 years after the last date of entry
Accident reporting records relating to individuals who	Learners	3 years after the last date of entry

Basic File Description	Relating to?	Retention Period
are under the age of 18 at the time of the incident		
Records relating to any reportable death, injury, disease, or dangerous occurrence (RIDDOR)	Employees/ Learners	Date of incident + 3 years
Control of Hazardous to Health (COSHH)	Employees/ Learners	Date of incident + 40 years
Fire precautions logbook	Organisation	Current year + 3 years
Employers' liability insurance certificate	Organisation	Closure of provision + 40 years
Annual Accounts	Organisation	Current year + 6 years
Maintenance log for all repairs	Organisation	Duration of the provision being in the building
Admissions Records	Learners	Duration of the learning plus 6 years
Unsuccessful Admissions	Learners	Until appeals process completed
Learner Education Record *(Primary age)*	Learners	Retain whilst the child remains at the provision
Learner Education Record *(Secondary age)*	Learners	Date of birth + 25 years
Examination results	Learners	Should be added to the learner file
Child protection information held on Learner file	Learners	Should be added to the learner file
Child protection information held on separate files	Learners	Date of Birth of the child + 25 years then review
Attendance registers	Learners	Every entry in the attendance register must be preserved for a period of 3 years after the date on which the entry was made.
Correspondence related to any absence *(authorised or unauthorised)*	Learners	Current academic year + 2 years
Special educational needs files, reviews and Education, Health and Care Plan, including advice and information provided to parents regarding educational needs and accessibility strategy	Learners	Date of birth + 31 years *(EHCP is valid until the individual reaches the age of 25 years – the retention period adds on 6 years from the end of the plan)*
Examination Results	Learners	Current year + 6 years

Basic File Description	Relating to?	Retention Period
Schemes of work	Learners	Current year + 1 year
Timetables	Learners	Current year + 1 year
Records books	Learners	Current year + 1 year