BLUE LION

TRAINING ACADEMY

DATA PROTECTION & PRIVACY POLICY AND PROCEDURE

DOCUMENT HISTORY

Version	Issued	Reason for Revision	Created by	Approved by
V1	Sept 2019	Initial release	Harj Dhanjal	Harj Dhanjal
V2	May 2020	COVID-19 Update	Harj Dhanjal	Harj Dhanjal
V3	June 2021	Updated in line with new QMS	Harj Dhanjal	Geeta Dhanjal
V4	Jan 2023	Updated new title	Harj Dhanjal	Harj Dhanjal

This Policy and Procedure document has been approved by the CEO / Director and is signed on release to the BLQMS on monday.com as per the version control status in the above table:	

CONTENTS

DATA PRIVACY POLICY AND PROCEDURE

Blue Lion Training Academy Limited (the 'Organisation') aims to provide defect-free products and services to its customers on time and within budget, we aim to audit our policies and procedures to drive continuous improvement.

The terms data protection and data privacy are often used interchangeably, but there is an important difference between the two. Data privacy defines who has access to data, while data protection provides tools and policies to restrict access to the data.

We cover both aspects within this document.

We are committed to ensuring that all personal data handled by us will be processed according to legally compliant standards of data protection and data security. We will meet UK GDPR and Data Protection Act 2018 requirements in relation to data sharing and data protection.

We need to process certain information about employers, learners, staff, and other individuals it has dealings with, for administrative purposes for example: recruitment, payment to staff, administering courses and training, to record training progress, to comply with our legal obligations to funding bodies and government.

To comply with the law, information about individuals will be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

We confirm for the purposes of the data protection laws 2018, that our data controller of personal data subjects using our services. This means that we determine the purposes for which, and the manner in which, your personal data is processed.

The purpose of this procedure is to help us achieve our data protection and data security aims by:

1. Notifying our data subjects using our services of the types of personal information that we may hold about them, and what we do with that information through the privacy policy. (Appendix 1)
2. Setting out the rules on data protection and the legal conditions that must be satisfied when we collect, receive, handle, process, transfer and store personal data and ensuring everyone understand our rules and the legal standards; and
3. Clarifying the responsibilities and duties of staff in respect of data protection and data security.

For the purposes of this procedure:

1. **Criminal records** data means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.
2. **Data protection laws** means all applicable laws relating to the processing of Personal Data, including, for the period during which it is in force, the UK General Data Protection Regulation.
3. **Data subject** means the individual to whom the personal data relates.
4. Personal data means any information that relates to an individual who can be identified from that

information.

5. **Processing** means any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.
6. **Special categories of personal data** mean information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

DATA PROTECTION PRINCIPLES

Staff whose work involves using personal data relating to data subjects must comply with this policy and with the following data protection principles which require that personal information is:

- Processed lawfully, fairly and in a transparent manner. We must always have a lawful basis to process personal data, as set out in the data protection laws. Personal data may be processed as necessary to perform a contract with the data subject, to comply with a legal obligation which the data controller is the subject of, or for the legitimate interest of the data controller or the party to whom the data is disclosed. The data subject must be told who controls the information, the purpose(s) for which we are processing the information and to whom it may be disclosed.
- Collected only for specified, explicit and legitimate purposes. Personal data will not be collected for one purpose and then used for another. If we want to change the way we use personal data, we will first tell the data subject.
- Processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing. We will only collect personal data to the extent required for the specific purpose notified to the data subject.
- We will take all reasonable steps to ensure that information that is inaccurate is rectified or deleted without delay. Checks to personal data will be made when collected and regular checks must be made afterwards. We will make reasonable efforts to rectify or erase inaccurate information.
- Kept only for the period necessary for processing. Information will not be kept longer than it is needed, and we will take all reasonable steps to delete information when we no longer need it.
- Secure, and appropriate measures are adopted by to us to ensure as such.

WHO IS RESPONSIBLE FOR DATA PROTECTION AND DATA SECURITY?

Maintaining appropriate standards of data protection and data security is a collective task shared between all staff at Blue Lion Training Academy Limited and the data subject. This procedure and the rules contained in it apply to all staff, irrespective of seniority, tenure and working hours, including all employees, directors and consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (Staff), learners our customers, suppliers and other third parties.

Questions about this policy, or requests for further information, should be directed to:
Data Protection – email: info@bluelionta.com

Everyone has personal responsibility to ensure compliance with this policy, to handle all personal data consistently with the principles set out here and to ensure that measures are taken to protect the data security. Directors and staff have special responsibility for leading by example and monitoring and enforcing compliance.

The Data Protection must be notified via email if this policy has not been followed, or if it is suspected this policy has not been followed, as soon as reasonably practicable via info@bluelionta.com

Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal. Significant or deliberate breaches, such as accessing staff or customer personal data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

WHAT PERSONAL DATA AND ACTIVITIES ARE COVERED BY THIS PROCEDURE?

This procedure covers personal data:

- Which relates to a natural living individual who can be identified either from that information in isolation or by reading it together with other information we possess.
- Is stored electronically or on paper in a filing system.
- In the form of statements of opinion as well as facts.
- Which relates to data subjects (present, past or future) or to any other individual whose personal data we handle or control.
- Which we obtain, is provided to us, which we hold or store, organise, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy.

This personal data is subject to the legal safeguards set out in the data protection laws.

WHAT PERSONAL DATA DO WE PROCESS ABOUT STAFF?

We collect personal data about you which:

- You provide or we gather before or during your employment or engagement with us.
- Is provided by third parties, such as references or information from suppliers or another party that we do business with; or
- is in the public domain.

The types of personal data that we may collect, store and use about you include records relating to your:

- Home address, contact details and contact details for your next of kin.
- Recruitment (including your application form or curriculum vitae, references received and details of your qualifications).
- Pay records, national insurance number and details of taxes and any employment benefits such as

pension and health insurance (including details of any claims made).
- Telephone, email, internet, fax or instant messenger use.
- Performance and any disciplinary matters, grievances, complaints or concerns in which you are involved.

WHAT PERSONAL DATA DO WE PROCESS ABOUT LEARNERS?

We collect personal data about you which:

- You provide or we gather before or during your apprenticeship or adult learning with us;
    - such as references or information from your employer,
    - qualifications and results from prior learning.

- The types of personal data that we may collect, store and use about you include records relating to your:
    - home address, contact details and contact details for your next of kin,
    - your application form or curriculum vitae, references, qualifications,
    - telephone, email,
    - complaints or concerns in which you are involved.

SENSITIVE PERSONAL DATA

We may from time to time need to process sensitive personal information (sometimes referred to as 'special categories of personal data').

We will only process sensitive personal information if:

- we have a lawful basis for doing so, e.g. it is necessary for the performance of the data subject's contract; and
- one of the following special conditions for processing personal information applies:
    i. the data subject has given explicit consent.
    ii. the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject.
    iii. the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
    iv. processing relates to personal data which are manifestly made public by the data subject.
    v. the processing is necessary for the external auditing or defence or legal claims; or
    vi. the processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, the data subject must notify the Data Protection Officer of the proposed processing, in order for the Data Protection Officer to assess whether the processing complies with the criteria noted above.

Sensitive personal information will not be processed until the assessment above has taken place and the individual has been properly informed of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

CRIMINAL RECORDS INFORMATION

Criminal records information will be processed in accordance with our Safer Recruitment Policy and Procedure.

HOW WE USE YOUR PERSONAL DATA

We will tell you the reasons for processing your personal data, how we use such information and the legal basis for processing in our privacy notice. We will not process data subject personal information for any other reason.

In general, we will use information to carry out our business, to administer your employment or engagement and to deal with any problems or concerns you may have, including, but not limited to:

- **Address Lists:** to compile and circulate lists of home address and contact details, to contact you outside working hours.
- **Sickness records:** to maintain a record of your sickness absence and copies of any doctor's notes or other documents supplied to us in connection with your health, to inform your colleagues and others that you are absent through sickness, as reasonably necessary to manage your absence, to deal with unacceptably high or suspicious sickness absence, to inform reviewers for appraisal purposes of your sickness absence level, to publish internally aggregated, anonymous details of sickness absence levels.
- **Monitoring IT systems:** to monitor your use of e-mails, internet, telephone and fax, computer or other communications or IT resources.
- **Disciplinary, grievance or legal matters:** in connection with any disciplinary, grievance, legal, regulatory or compliance matters or proceedings that may involve you.
- **Performance Reviews:** to carry out performance reviews.
- **Equal Opportunities Monitoring:** to conduct monitoring for equal opportunities purposes and to publish anonymised, aggregated information about the breakdown of the Employer's workforce.

ACCURACY AND RELEVANCE

We will:

- Ensure that any personal data processed is up to date, accurate, adequate, relevant and not excessive, given the purpose for which it was collected.
- Not process personal data obtained for one purpose for any other purpose, unless you agree to this or reasonably expect this.

If you consider that any information held about you is inaccurate or out of date, then you should tell the Data Protection Officer. If they agree that the information is inaccurate or out of date, then they will correct it promptly. If they do not agree with the correction, then they will note your comments.

ESFA

As an ESFA provider, we must hold evidence to assure ESFA that we are using ESFA funding appropriately.

When our contract with ESFA ends, we will ensure our learner records are transferred to ESFA if required and all other records are either securely destroyed if they have reached their retention period or retained by Blue Lion TA until their destruction date is reached.

What is the minimum that should be kept?

As a minimum we will keep a learner file for each learner. It will contain:

- Evidence about the learner, e.g. proof of identify.
- Evidence of eligibility for funding.
- Evidence of qualifications/course studied and achieved.

How should files be stored?

It is recommended by the ESFA that learner files should be stored electronically. Electronic data records and documents should be stored in secure off-site cloud-based servers that meet accepted security standards and legal requirements so can be relied upon for audit purposes (including ISO 27001).

However, if records are kept in paper-format they should be stored in individual wallets, one wallet per learner per academic year. All paper records should be stored in secure, lockable, fireproof, non-portable storage containers and access should be strictly controlled and limited to staff that need to access the records.

It is recommended that learner files should be stored in electronic systems or paper wallets that contains the following information:

- learner's surname, first name
- course studied
- academic year
- ESF contract number (if applicable)
- destruction date (6 years from date study ended, or 31/12/2030 if ESF-funded)

Transfer of records

If the learner moves to a new provider or the contract is terminated, Blue Lion Training Academy will

- retain their learner file as per retention periods see diagram below. The new provider will gather new evidence for the learner.
- Transfer their portfolio so they can continue their course with the new provider.

If the learner file needs to be transferred back to ESFA, the ESFA record transfer agreement will be used.

Retention of records

Learner files should be retained securely for 6 years from Financial Year End after end of course or until 31/12/2030 if ESF-funded provision.

Type of record	Retention period	Action
Learner records: • **Details of learner** • **Course studied** • **Learner eligibility**	6 years from Financial Year End after last payment made	Destroy records older than 7 years. List all remaining records with full name, course studied & course dates.
'Live' Portfolios (paper and electronic)*	2 years from end of course	Destroy records older than 2 years. List all remaining records with full name, course studied & course dates.
Certificates	N/A - send to learner	Return all certificates to awarding body if not sent to learner.
European Social Fund (ESF)	For the 2007-13 ESF Programme this is expected to be until at least 31 December 2022. For the For the 2014-20 ESF Programme until at least 31 December 2030.	Destroy records if past destruction date. List all remaining records with full name, course studied and course dates. **Note**: check the DWP - ESF guidance before destroying any paperwork in case the destruction date has changed.
Corporate records: • **HR records** • **Finance records** • **Contract records**	Retain as per statutory guidance provided by Companies House and HMRC on a company's record keeping requirements	

INDIVIDUAL RIGHTS

You have the following rights in relation to your personal data.

Subject access requests: You have the right to make a subject access request. If you make a subject access request, we will tell you:

- Whether or not your personal data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from you.
- To whom your personal data is or may be disclosed.
- For how long your personal data is stored (or how that period is decided).
- Your rights of rectification or erasure of data, or to restrict or object to processing.
- Your right to right to complain to the Information Commissioner if you think we have failed to comply with your data protection rights; and

we will provide you with a copy of the personal data undergoing processing. This will normally be via email To make a subject access request, contact us by email: info@bluelionta.com

We may need to ask for proof of identification before your request can be processed. We will let you know if we need to verify your identity and the documents we require.

We will normally respond to your request within 28 days from the date your request is received. In some cases, e.g. where there is a large amount of personal data being processed, we may respond within 3 months of the date your request is received. We will write to you within 28 days of receiving your original request if this is the case.

If your request is manifestly unfounded or excessive, we are not obliged to comply with it.

OTHER RIGHTS:

You have a number of other rights in relation to your personal data. You can require us to:

- Rectify inaccurate data.
- Stop processing or erase data that is no longer necessary for the purposes of processing.
- Stop processing or erase data if your interests override our legitimate grounds for processing the data (where we rely on our legitimate interests as a reason for processing data).
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override legitimate grounds for processing the data.

To request that we take any of these steps, please send the request to info@bluelionta.com

DATA SECURITY

We will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Maintaining data security means making sure that:

- Only people who are authorised to use the information can access it.
- Where possible, personal data is encrypted.
- Information is accurate and suitable for the purpose for which it is processed; and
- authorised persons can access information if they need it for authorised purposes.

By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.

Personal information must not be transferred to any person to process (e.g. while performing services for us on or our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

Security procedures include:

- Any desk or cupboard containing confidential information must be kept locked.
- Computers should be locked with a strong password that is changed regularly or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.

The Data Protection Officer must approve of any cloud used to store data.

- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing sensitive personal data must be approved and strict permissions provided.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up on an external hard drive.

Telephone Precautions.

Particular care must be taken by Staff who deal with telephone enquiries to avoid inappropriate disclosures. In particular:

- the identity of any telephone caller must be verified before any personal information is disclosed;
    - if the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing;
    - do not allow callers to bully you into disclosing information. In case of any problems or

uncertainty, contact the Director

Methods of disposal.

Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

Additional measures to ensure data security include personal and sensitive should not be left in in trays or on desks or public places, anyone who sees any personal data visible should report it immediately.

DATA BREACHES

If we discover that there has been a breach of data subject's personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery.

If the breach is likely to result in a high risk to your rights and freedoms, we will tell affected individuals that there has been a breach and provide them with more information about its likely consequences and the mitigation measures it has taken.

Every 2 years register is updated with ICO: Information Commissioners office. The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Membership number is: ZA743617 **(See Appendix 2)**

INDIVIDUAL RESPONSIBILITIES

Data Subjects are responsible for helping us keep their personal data up to date.

Data Subjects should let Blue Lion TA know if personal data provided to the us changes, e.g. if you move house or change your bank details.

Our Staff may have access to the personal data of other Staff members and of our customers in the course of the employment. Where this is the case, we rely on Staff members to help meet its data protection obligations to Staff and to customers.

Individuals who have access to personal data are required:

- to access only personal data that they have authority to access and only for authorised purposes;
- not to disclose personal data except to individuals (whether inside or outside of the company) who have appropriate authorisation;
- to keep personal data secure (e.g. by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from

our premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

- not to store personal data on local drives or on personal devices that are used for work purposes.

TRAINING

We will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this procedure or responding to subject access requests under this procedure will receive additional training to help them understand their duties and how to comply with them.

BLUE LION TRAINING ACADEMY PRIVACY POLICY

WHO WE ARE: Our website address is: https://bluelionta.com

WHAT PERSONAL DATA WE COLLECT AND WHY WE COLLECT IT

COMMENTS

When visitors leave comments on the site we collect the data shown in the comments form, and also the visitor's IP address and browser user agent string to help spam detection.

An anonymized string created from your email address (also called a hash) may be provided to the Gravatar service to see if you are using it. The Gravatar service privacy policy is available here: https://automattic.com/privacy/. After approval of your comment, your profile picture is visible to the public in the context of your comment.

MEDIA

If you upload images to the website, you should avoid uploading images with embedded location data (EXIF GPS) included. Visitors to the website can download and extract any location data from images on the website.

CONTACT FORMS

COOKIES

If you leave a comment on our site you may opt-in to saving your name, email address and website in cookies. These are for your convenience so that you do not have to fill in your details again when you leave another comment. These cookies will last for one year.

If you visit our login page, we will set a temporary cookie to determine if your browser accepts cookies. This cookie contains no personal data and is discarded when you close your browser.

When you log in, we will also set up several cookies to save your login information and your screen display choices. Login cookies last for two days, and screen options cookies last for a year. If you select "Remember Me", your login will persist for two weeks. If you log out of your account, the login cookies will be removed.

If you edit or publish an article, an additional cookie will be saved in your browser. This cookie includes no personal data and simply indicates the post ID of the article you just edited. It expires after 1 day.

EMBEDDED CONTENT FROM OTHER WEBSITES

Articles on this site may include embedded content (e.g. videos, images, articles, etc.). Embedded content from other websites behaves in the exact same way as if the visitor has visited the other website.

These websites may collect data about you, use cookies, embed additional third-party tracking, and monitor your interaction with that embedded content, including tracking your interaction with the embedded content if you have an account and are logged in to that website.

ANALYTICS

WHO WE SHARE YOUR DATA WITH - HOW LONG WE RETAIN YOUR DATA

If you leave a comment, the comment and its metadata are retained indefinitely. This is so we can recognize and approve any follow-up comments automatically instead of holding them in a moderation queue.

For users that register on our website (if any), we also store the personal information they provide in their user profile. All users can see, edit, or delete their personal information at any time (except they cannot change their username). Website administrators can also see and edit that information.

WHAT RIGHTS YOU HAVE OVER YOUR DATA

If you have an account on this site, or have left comments, you can request to receive an exported file of the personal data we hold about you, including any data you have provided to us. You can also request that we erase any personal data we hold about you. This does not include any data we are obliged to keep for administrative, legal, or security purposes.

APPENDIX 2: ICO CERTIFICATE

ico.
Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

Certificate

Organisation Name:

Blue Lion Training Academy Limited

Reference number:

ZA743617

Tier:

Tier 1

Start date:

31 March 2020

End date:

30 March 2023

Data Protection Officer

Get in touch!

Visit us online...

www.BlueLionTA.com

Call us...

01332 738625

Email us...

info@BlueLionTA.com

Find us...

Blue Lion Training Academy Limited

Ground Floor, 13 Mallard Way

Pride Park,

Derby.

DE24 8GX

BLUE LION

TRAINING ACADEMY