LEARNING CURVE GROUP

DATA PROTECTION POLICY

Policy Group: Data Protection, Security and Information Policy

Effective: May 20

Approved: Gail Crossman

Responsible officer Neil Whittaker

Next renew due: May 21

Ref no.: 5.1

GUIDANCE

Values | Vision | Tone of Voice

Values

Vision

Transforming lives through learning

Tone of voice

Our tone of voice takes its direct influence from our core values.

We are passionate about people and learners and are driven to get the best out of everyone by getting to understand them. We are caring and supportive, as well as being determined and strive for growth. We talk with purpose and enthusiasm in a way that connects and empowers people.

Innovation is at the heart of Learning Curve Group and we're always thinking about what's next!

SUMMARY CHANGES

Date	Page	Details of amendments
May 2020		**Reflect LHAA**

I. INTRODUCTION

Learning Curve Group is one of the largest training providers in the UK, providing education and training nationally. In October 2018 Profound Services Ltd and Northern Care Training Ltd joined Learning Curve Group and later in 2020 the London Hairdressing Apprenticeship Academy and the London Beauty Therapy Academy joined the family.

Glossary:
Learning Curve Group (LCG)
Profound Services (PS)
Northern Care Training (NCT)
London Hairdressing Apprenticeship Academy (LHAA)
London Beauty Therapy Academy (LBTA)

This policy meets the legal requirements of General Data Protection Regulations 2018 and the Data Protection Act 2018

Reason for policy

To ensure we comply with the required government legislation.

Applies to:

In order to operate efficiently, we have to collect and use personal information and this policy applies to the personal information of:

- Job applicants
- Current and former staff, including employees, temporary and agency workers, associates, contractors, volunteers, apprentices
- Learners, service users, customers
- Relatives of any of the forgoing: and
- Suppliers

II. Policy

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

The policy does not form of the formal contract of employment, but it is a condition of engagement that employers, workers, contractors and associates abide by the rules and policies made. Any failures to follow the policy can therefore result in disciplinary.

The Director of Marketing & Communications is responsible for data protection compliance within Learning Curve Group. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Director of Marketing & Communications on data.protection@learningcurvegroup.co.uk , dataprotection@LHAA.co.uk or 01388 777 129.

We regard the lawful and correct treatment of personal information as very important to our successful operations and to maintaining confidence between the Company and those with who it carries out business. We will ensure that we treat personal information lawfully and correctly.

Personal information will be handled and dealt with properly however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

As part of our commitment to data protection, we will review and update this policy regularly in accordance with our data protection obligations. We may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

Definitions

Criminal records information – means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;

Data breach – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal information;

Data subject – means the individual to whom the personal information relates;

Personal information – (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

Processing information – means obtaining, recording, organizing, storing, amending, retrieving, disclosing and / or destroying information, or using or doing anything with it;

Sensitive information – (sometimes known as ' special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

The principles of data protection

We will comply with the following data protection principles when processing personal information:

1. We will process information fairly, lawfully and in a transparent manner;
2. We will collect personal information for specified, explicit and legitimate purposes only, and will not process it in any manner incompatible with those legitimate purposes;
3. We will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
4. We will keep accurate and up to date personal information and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay.
5. We will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
6. We will take appropriate technical and organizational measures to ensure that personal information are kept secure and protected against unauthorized or unlawful processing, and against accidental loss, destruction or damage.

Basis for processing personal information

In relation to any processing activity we will, before the processing starts for the first time and then regularly while it continues review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

1. That the data subject has consented to the processing;
2. That the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. that the processing is necessary for compliance with a legal obligation to which the Company is subject;
4. That the processing is necessary for the protection of the vital interests of the data subject or another natural person; or
5. that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see below.

Except where the processing is based on consent, we will:

1. satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
2. document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
3. include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
4. where sensitive personal information is processed, also identify a lawful special condition for processing that information (see below), and document it; and
5. where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

1. Conduct a legitimate interest assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
2. If the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA)
3. Keep the LIA under review, and repeat it if circumstances change; and
4. Include information about our legitimate interests in our relevant notice(s)

Sensitive personal information

The Company may from time to time need to process sensitive personal information. We will only process sensitive personal information if we have a lawful basis for doing so as set out above, eg it is necessary for the performance of the employment contract, to comply with our legal obligations or

for the purposes our legitimate interests; and one of the special conditions for processing sensitive personal information applies, e.g.:

1. The data subject has given explicit consent;
2. The processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;
3. The processing relates to personal data subject's vital interests, and the data subject is physically incapable of giving consent;
4. Processing relates to personal data which are manifestly made public by the data subject;
5. The processing is necessary for the establishment, exercise or defence of legal claims; or
6. The processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, staff must notify the Director of Marketing & Communications of the proposed processing, in order that the Director of Marketing & Communications may assess whether the processing complies with the criteria noted above.

Sensitive personal information will not be processed until:

1. The assessment above has taken place; and
2. The individual has been properly informed (by the way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

During the recruitment process: the HR department will ensure that (except where the law permits otherwise):

1. During the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g. race or ethnic origin, trade union membership or health;
2. If sensitive personal information is received, e.g. the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;
3. Any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;
4. 'Right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;
5. We will only ask health questions once an offer of employment has been made.

During employment: the HR department will process:

- Health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits; and
- Sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting.

Documentation and records

We will keep written records of processing activities, including:

1. The name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and Data Protection Officer);
2. The purposes of the processing;
3. A description of the categories of individuals and categories of personal data;
4. Categories of recipients of personal data;
5. Where possible, retention schedules; and
6. Where possible, a description of technical and organisational security measures.

If we process sensitive personal information or criminal records information, we will keep written records of:

1. The relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
2. The lawful basis for our processing; and
3. Whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

We will conduct regular reviews of the personal information we process and update our documentation accordingly.

Privacy notice

The Company will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language and our full notices is currently on our website alongside a guide on how we use cookies.

We take your privacy very seriously and would request you read this privacy policy carefully as it contains important information on who we are and how and why we collect, store, use and share your personal data. It also explains your rights in relation to your personal data and how to contact us or supervisory authorities in the event you have a complaint.

When we use your personal data, we are regulated under the General Data Protection Regulation (GDPR) which applies across the European Union (including in the United Kingdom) and we are responsible as 'controller' of that personal data for the purposes of the GDPR. Our use of your personal data is subject to us offering our services to you, your consent, the GDPR, other relevant UK and EU legislation.

Individual rights

You (in common with other data subjects) have the following rights in relation to your personal information:

- To be informed about how, why and on what basis that information is processed—see the Company's data protection privacy notice;
- To obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request—see the Company's subject access request policy stored on the company J Drive under Policies and Procedures;
- To have data corrected if it is inaccurate or incomplete;
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

If you wish to exercise any of the rights above, please contact the Director of Marketing & Communications.

Individual obligations

Individuals are responsible for helping the Company keep their personal information up to date. You should let the HR department know if the information you have provided to the Company changes, for example if you move to a new house or change details of the bank or building society account to which you are paid.

You may have access to the personal information of other members of staff, workers, learners, service users, customers and suppliers etc. of the Company in the course of your employment or engagement. If so, the Company expects you to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

1. Only access the personal information that you have authority to access, and only for authorised purposes;
2. Only allow other Company staff to access personal information if they have appropriate authorisation;
3. Only allow individuals who are not Company staff to access personal information if you have specific authority to do so from the Director of Marketing & Communications;
4. Keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Company's [information security policy] stored on the company S Drive under Policies and Procedures;
5. Not remove personal information, or devices containing personal information (or which can

be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

6. Not store personal information on local drives or on personal devices that are used for work purposes.

You should contact the Director of Marketing & Communications if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

1. Processing of personal data or sensitive personal information without a lawful basis for its Processing being met;
2. Any data breach as set out below;
3. access to personal information without the proper authorisation;
4. Personal information not kept or deleted securely;
5. Removal of personal information, or devices containing personal information (or which can be used to access it), from the Company's premises without appropriate security measures being in place;
6. Any other breach of this policy or of any of the data protection principles set out in above.

Information security

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

International transfers

The Company will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

Storage and retention of personal information

Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow the Company's records retention policy [stored on the company S Drive under Policies and Procedures] which set out the relevant retention period. Where there is any uncertainty, staff should consult the Director of Marketing & Communications.

Disposing of Data

Data will be disposed of through either confidential shredding using an external contractor or purging from the company servers.

Where computer equipment is disposed of, all data shall be removed and storage media such as hard disks, Tablets, iPads and USB memory sticks will be "electronically" shredded or a similar procedure to ensure that data can't be "reclaimed".

Data breaches

The Company takes every care in protecting the personal information it holds and avoiding risks which could lead to a compromise of security and a potential data protect breach. Compromised security and/or data breaches can result in harm to the individual(s) involved, reputational damage

to the Company, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

Training

The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests, will receive additional training to help them understand their duties and how to comply with them.

Consequences of failing to comply

The Company takes compliance with this policy very seriously. Failure to comply with the policy:

- Puts at risk the individuals whose personal information is being processed; and
- Carries the risk of significant civil and criminal sanctions for the individual and the Company; and
- May, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Director of Marketing & Communications.

Privacy Notice
Statement

Key terms

It would be helpful to start by explaining some key terms used in this policy:

We, us, our	Learning Curve Group (a trading name of Learning Curve (NE) Group Limited) is a company registered in England and Wales with company number 08616453. Our registered address is at Unit 1-10 Dunelm Rise, Durhamgate, Spennymoor, County Durham, DL16 6FS. The London Hairdressing Apprenticeship Academy Limited (LHAA) 07710651 and their subsidiary, the London Beauty Training Academy Limited (LBTA) 10359923.
Our data protection officer	The Director of Marketing & Communications is responsible for data protection compliance within Learning Curve Group. If you have any questions or comments about the content of this policy or if you need further information, you can contact the Director of Marketing & Communications: By telephone: 01388 777 129 or Email: data.protection@learningcurvegroup.co.uk Email: dataprotection@LHAA.co.uk
Personal data	Any information relating to an identified or identifiable individual
Special category personal data	Personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership Genetic and biometric data Data concerning health, sex life or sexual orientation

#

Personal data we collect about you

The table below sets out the personal data we will or may collect in the course of providing our services to you.

Personal data we will collect	Personal data we may collect
1. Learners	
Your name, address and telephone number Information to enable us to check and verify your identity, e.g. your date of birth or passport details	Your racial or ethnic origin, gender and sexual orientation, religious or similar beliefs for internal equal opportunities monitoring

Personal data we will collect	Personal data we may collect
1. Learners	
Electronic contact details, e.g. your email address and mobile phone number Your National Insurance and tax details to enable us to determine government funding eligibility Your nationality and immigration status to determine government funding eligibility Details of your spouse/partner and dependants or other family members to determine government funding eligibility and for next of kin purposes Your employment status to enable us to determine government funding eligibility Emergency contact information	Health/learning difficulties/disabilities Household situation Prior attainment / previous qualifications Specific employer data (e.g. employer name, weekly hours, job title etc) Bank details (e.g. for bursary payments where applicable) Destination tracking information after completing learning (further training/employment)

2. Job Applicants/Seekers	
Your name, address and telephone number Information to enable us to check and verify your identity, e.g. your date of birth or passport details Electronic contact details, e.g. your email address and mobile phone number Your National Insurance and tax details Your nationality and immigration status to determine work permit requirements etc. Details of your spouse/partner and dependants or other family members for next of kin purposes Your previous employment records including, where relevant, records relating to sickness and attendance, performance, disciplinary, conduct and grievances	Your racial or ethnic origin, gender and sexual orientation, religious or similar beliefs for internal equal opportunities monitoring Your medical records

This personal data is required to enable us to provide our services to you. If you do not provide personal data we ask for, it may delay or prevent us from providing services to you.

How your personal data is collected

We collect most of this information from you directly. However, we may also collect information:

- from a third party with your consent, e.g.:
- consultants and other professionals (schools/colleges);
- your employer;
- Learning Records Service (LRS (e.g. Unique Learner Reference / Number (URL/URN), ESFA etc)
- via our website—we use cookies on our website (for more information on cookies, please see our cookies policy (link)

- via our information technology (IT) systems, e.g.:
- e-Assessor portal
- automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, email and instant messaging systems;

How and why we use your personal data

Under data protection law, we can only use your personal data if we have a proper reason for doing so, e.g.:

- for the performance of our contract with you or to take steps at your request before entering into a contract;
- to comply with our legal and regulatory obligations;
- for our legitimate interests or those of a third party; or
- where you have given consent.

A legitimate interest is when we have a business or commercial reason to use your information, so long as this is not overridden by your own rights and interests.

The table below explains what we use (process) your personal data for and our reasons for doing so:

What we use your personal data for	**Our reasons**
To provide educational services to you	For the performance of our contract with you or to take steps at your request before entering into a contract
To provide recruitment services to you	For the performance of our agreement with you or to take steps at your request before entering into a contract
Conducting checks to identify our clients and verify their identity	To comply with our legal and regulatory obligations
Gathering and providing information required by or relating to audits, enquiries or investigations by regulatory bodies	To comply with our legal and regulatory obligations
Ensuring business policies are adhered to, eg policies covering security and internet use	For our legitimate interests or those of a third party, i.e. to make sure we are following our own internal procedures so we can deliver the best service to you

Operational reasons, such as improving efficiency, training and quality control	For our legitimate interests or those of a third party, i.e. to be as efficient as we can so we can deliver the best service for you at the best price
Preventing unauthorised access and modifications to systems	For our legitimate interests or those of a third party, i.e. to prevent and detect activity that could be damaging for us and for you To comply with our legal and regulatory obligations

What we use your personal data for	**Our reasons**
Updating client records	For the performance of our contract with you or to take steps at your request before entering into a contract To comply with our legal and regulatory obligations For our legitimate interests or those of a third party, e.g. making sure that we can keep in touch with our clients about existing and new services
Ensuring safe working practices, staff administration and assessments	To comply with our legal and regulatory obligations For our legitimate interests or those of a third party, e.g. to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you
Marketing our services to: —existing and former clients; —third parties who have previously expressed an interest in our services; —third parties with whom we have had no previous dealings.	For our legitimate interests or those of a third party, ie to promote our business to existing and former clients
External audits and quality checks, e.g. for….	For our legitimate interests or a those of a third party, i.e. to maintain our accreditations so we can demonstrate we operate at the highest standards To comply with our legal and regulatory obligations
Safeguarding concerns	To comply with our legal and regulatory obligations

The above table does not apply to special category personal data, which we will only process with your explicit consent.

Marketing

We may use your personal data to send you information (by email, text message, telephone or post) about our services, new courses and new services**.**

We have a legitimate interest in processing your personal data for marketing purposes (see above '**How and why we use your personal data**'). This means we do not usually need your consent to market to you. However, where consent is needed, we will ask for this consent separately and clearly.

We will always treat your personal data with the utmost respect and never sell or share it with other organisations for marketing purposes.

You have the right to opt out of receiving promotional communications at any time by:

- contacting us by emailing unsubscribe@learningcurvegroup.co.uk
- using the 'unsubscribe' link in emails or 'STOP' number in texts

We may ask you to confirm or update your marketing preferences if you instruct us to provide further services in the future, or if there are changes in the law, regulation, or the structure of our business.

Who we share your personal data with?

We routinely share personal data with:

- Employers;
- Government funding agencies (including the Apprenticeship Service where applicable)
- FE Providers/Colleges
- our group companies;
- our insurers and brokers;
- external auditors, eg in relation to ISO accreditations and the audit of our accounts;
- external service suppliers, representatives and agents that we use to make our business more efficient, eg marketing agencies, document collation or analysis suppliers;
- End Point Assessment Organisations (EPAO);
- Software suppliers (e.g. Smart Assessor, Advanced etc);
- Awarding Organisations for certification.

We only allow our service providers to handle your personal data if we are satisfied, they take appropriate measures to protect your personal data. We also impose contractual obligations on service providers relating to ensure they can only use your personal data to provide services to us and to you.

We may disclose and exchange information with law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations.

We may also need to share some personal data with other parties, such as potential buyers of some or all of our business or during a re-structuring. Usually, information will be anonymised, but this may not always be possible. The recipient of the information will be bound by confidentiality obligations.

We will not share your personal data with any other third party.

Where your personal data is held

Information may be held at our offices and those of our third-party agencies, service providers, representatives and agents as described above (see '**Who we share your personal data with**').

How long your personal data will be kept

We will keep your personal data after we have finished providing our services to you. We will do so for one of these reasons:

- to respond to any questions or complaints made by you or on your behalf;
- to show that we treated you fairly;
- to keep records required by law and/or funding criteria.

We will not retain your data for longer than necessary for the purposes set out in this policy. Different retention periods apply for different types of data.

When it is no longer necessary to retain your personal data, we will delete or anonymise it.

Your rights

You have the following rights, which you can exercise free of charge:

Access	The right to be provided with a copy of your personal data
Rectification	The right to require us to correct any mistakes in your personal data
To be forgotten	The right to require us to delete your personal data—in certain situations. Please contact us directly if you wish to discuss this further.
Restriction of processing	The right to require us to restrict processing of your personal data—in certain circumstances, eg if you contest the accuracy of the data

Data portability	The right to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party—in certain situations
To object	The right to object: —at any time to your personal data being processed for direct marketing (including profiling); —in certain other situations to our continued processing of your personal data, eg processing carried out for the purpose of our legitimate interests.
Not to be subject to automated individual decision-making	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you

For further information on each of those rights, including the circumstances in which they apply, please contact us or see the guidance from the UK Information Commissioner's Office (ICO) on individuals rights under the General Data Protection Regulation (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/).

If you would like to exercise any of those rights, please:

- **[**complete a data subject request form—available on our website at [*insert link*]; or
- email, call or write to us —see below: '**How to contact us**'; and
- let us have enough information to identify you *(e.g. your full name, address and learner reference number (if applicable))*;
- let us have proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill); and
- let us know what right you want to exercise and the information to which your request relates.

Keeping your personal data secure

We have appropriate security measures to prevent personal data from being accidentally lost or used or accessed unlawfully. We limit access to your personal data to those who have a genuine business need to access it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

How to complain

We hope that we can resolve any query or concern you may raise about our use of your information.

The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority, in particular in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in the UK is the Information Commissioner who may be contacted at https://ico.org.uk/concerns or telephone: [*0303 123 1113*].

Changes to this privacy policy

This privacy policy was published in May 2018 and last updated on May 2020.

We may change this privacy policy from time to time.

How to contact us

Please contact us by post, email or telephone if you have any questions about this privacy policy or the information we hold about you. Our contact details are shown below:

Our Data Protection Officer's contact details

FAO The Director of Marketing & Communications

Dunelm Rise, Unit 8-10

Durhamgate,

Spennymoor,

DL16 6FS

data.protection@learningcurvegroup.co.uk
dataprotection@LHaa.co.uk

01388 777 129

Cookies Guide

What are cookies?

Our website uses cookies. A cookie is a small text file which is stored on your computer, tablet or phone when you visit a website. These cookies allow us to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and also allows us to improve our
website.

There are two main types of cookie:

- session cookies—these are deleted when you finish browsing a website and are not stored on your computer longer than this

- persistent cookies—these are stored on your computer after you have finished using a website so that the website provider can remember your preferences the next time you use it

Cookies can be set by the website you have browsed, i.e. the website displayed in the uniform resource locator (URL) window. These are called first party cookies. Third party cookies are set by a website other than the one you are browsing.

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.

How do we use cookies?

The table below shows what cookies we use and why.

Type of cookie	**Why do we use this cookie?**

Session cookies And **Persistent cookies**	We use cookies to help provide services, provide a secure online environment, to provide a better online experience, to manage your browsing session, to monitor our website performance, to help make the website more relevant to you and to compile statistics to help us improve our website and services we offer.

Consent

If you continue to use our website, we will assume that you are happy to receive all cookies from our website. However, if you would prefer to change your cookie settings, you can do so at any time—see below:

'Controlling our use of cookies'.

Controlling our use of cookies

Most browsers automatically accept cookies unless you change your internet browser settings. If you wish to restrict, block or delete the cookies which are set by any websites, you can generally do this through your browser settings. These settings are usually found in the 'options' or 'preferences' menu of your internet
browser.

If you set your internet browser preferences to block all cookies, you may not be able to access all or parts of our site.

If you delete cookies relating to this website, we will not remember things about you, including your cookie preferences, and you will be treated as a first-time visitor the next time you visit the site.

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.

Queries

If you have any questions or comments regarding this Cookies policy, please email data.protection@learningcurvegroup.co.uk
dataprotection@LHAA.co.uk

Appendix

The policy and procedures within this document cover Tees Valley ESF NEET ESFA-15032.