Data Protection Policy

May 2018

Policy Group: Data Protection, Security and Information
Policy Number: 5.1
Policy Title: Data Protection Policy
Author: Neil Whittaker
Date and Current Version: M a y 2 0 1 8
Review Date: M a y 2 0 1 9
Approved by: Gail Crossman

Introduction

This policy sets out how we at Learning Curve Group (the 'Company') 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.

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

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 or 01388 777 129.

Scope

In order to operate efficiently, Learning Curve Group has 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.

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, unauthorised 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, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
sensitive personal 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), genetics 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

Learning Curve Group 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 organisational measures to ensure that personal information are kept secure and protected against unauthorised 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 interests 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 privacy 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 Learning Curve Group's legal obligations or for the purposes of Learning Curve Group's legitimate interests; and one of the special conditions for processing sensitive personal information applies, e.g.:

1. the data subject has given 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 is necessary to protect the 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 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:

1. 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
2. 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.

Individual rights

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

1. to be informed about how, why and on what basis that information is processed—see the Company's data protection privacy notice;
2. 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 S Drive under Policies and Procedures;
3. to have data corrected if it is inaccurate or incomplete;
4. 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');
5. 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
6. 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 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, please refer to the Company's Information Security policy for more details [stored on the company S Drive under Policies and Procedures].

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

Please refer to the Company’s Data Breach Policy which can be found on stored on the company S Drive under Policies and Procedures.

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:

1. puts at risk the individuals whose personal information is being processed; and
2. carries the risk of significant civil and criminal sanctions for the individual and the Company; and
3. 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.