THE JCB ACADEMY

Data Protection Policy

June 2020

1. General

1.1 The JCB Academy (the academy) is registered with the Information Commissioners Office (ICO) as a “Data Controller” and its registration number is Z1690581.

1.2 The academy will often handle and store information about an identifiable, living person and is therefore legally obliged to protect that information under the Data Protection Act. The academy is committed to processing data in accordance with its responsibilities under Article 5 of the General Data Protection Regulation (GDPR) under which the academy must:

- Fairly and lawfully process the data.
- Process for limited purposes.
- Process data that is adequate, relevant and not excessive.
- Ensure the data processed is accurate.
- Ensure the data is not kept longer than necessary.
- Ensure the data is in accordance with the data subject's rights.
- Secure the data.
- Not transfer data to other countries without adequate protection.

1.3 Definitions:

- "**processing**" means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.
- "**data subject**" means an individual who is the subject of personal data or the person to whom the information relates.
- "**personal data**" means data, which relates to a natural identifiable individual whether directly or indirectly.
- "**parent**" has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

2. Fair obtaining and processing

2.1 The academy undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection. The purposes for which data is held, the likely recipients of the data and the data subject's right of access, are stated in the academy privacy policies which are accessible through its website.

3. Registered purposes

3.1 The Data Protection Registration entries for the academy are available for inspection, by appointment, at reception. Explanation of any codes and categories entered is available from the Data Protection Officer (DPO) who is the person nominated to deal with data protection issues in the academy. Registered purposes covering the data are held on the ICO's website. The academy will not use personal information beyond the reasons stated in its privacy policies. In the unlikely event that there is a need to use data for a different reason than originally stated, the academy will contact the individual concerned for their consent.

4. Data accuracy

4.1 Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the academy of a change of circumstances their record will be updated as soon as is practicable.

5. Data adequacy and relevance

5.1 Data held about data subjects will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the academy will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

6. Retention

6.1 Data held about data subjects will not be kept for longer than necessary for the purposes registered. It is the duty of the academy to ensure that obsolete data is properly erased in line with its data retention policy.

7. Subject access

7.1 Individual data subjects have the right to:

- Be informed on why the academy collects, processes and holds data. This is listed in the academy's privacy policies.
- Request access to a copy of the records the academy holds on them.
- Object to processing that is likely to cause or is causing distress.
- Prevent direct marketing.

- Object to decisions being made by automated means.
- Have inaccurate personal data rectified, blocked, erased or destroyed and claim compensation for damages caused by a breach of the Act.

8. Processing subject access requests

8.1 Requests for access must be made in writing.

8.2 Learners, parents or staff may make a Data Subject Access request by contacting office@jcbacdemy.com. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access register, showing the date of receipt, the data subject's name, the name and address of requester, the type of data required (e.g. learner record, personnel record) and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

8.3 In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

8.4 The following information can be requested:

- Whether any data is being processed.
- A description of the personal data, the reasons it is being processed, and whether it will be given to any other organisation or people.
- A copy of the information comprising the data; and details of the source of the data (where this is available).

9. Authorised disclosures

9.1 The academy will not share information about individuals with anyone without consent unless the law and its policies allows it to do so. Further details are listed in the academy's privacy notices.

10. Data and computer security

10.1 The academy undertakes to ensure security of personal data by the following general methods:

- All staff within the academy have agreed to the ICT Acceptable Use Policy which states they must not disclose their password to anyone else.
- All computers that the academy provides require users to authenticate with a username and password to gain access.
- The academy provides a "guest wireless" which provides visitors to a segregated part of the network which provides a means of access to the internet.
- The servers in which all personal data about data subjects is stored are controlled by card access, which limits access to authorised personnel only.
- All computers administered by the academy have up to date anti-virus software installed.
- All personal data is protected by security groups which allows only those that require access to view it.
- The academy uses data encryption software to encrypt hard drives and portable memory used off site.

11. Biometric data

11.1 The academy uses a biometric fingerprint system for the cashless catering and follow-me printing facilities. The biometric information collected will be only obtained by formal consent and will not be used in conjunction with any other biometric system without the data subject's consent.

12. CCTV

12.1 The academy operates a 24 hour CCTV monitoring system which records and archives for 30 days. Access to the system is restricted to authorised personnel only. All CCTV footage is stored in a secure location that has security card access and is only removed from the system in the case of an investigation.

13. Physical security

13.1 Appropriate building security measures are in place, e.g. alarms, deadlocks and CCTV. Only authorised personnel are allowed into the computer room. Disks and printouts are locked away securely when not in use. Visitors to the academy are required to sign in and out at reception, to wear identification badges whilst in the academy and are, where appropriate, accompanied.

Date of approval by Governing Body: 6 May 2014
Reviewed and reapproved: 15 June 2018
Reviewed and reapproved: 17 June 2020