

Data Protection Policy

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 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 living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
- "**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

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. Information about the use of personal data is

printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

3. Registered purposes

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 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 (Information Commissioner's Office) website. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

4. Data accuracy

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. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

5. Data adequacy and relevance

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. Length of time

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.

7. Subject access

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a student, the Academy's policy is as follows:

- Requests from students will be processed as any subject access request as outlined below and the copy will be given directly to the student unless it is clear that the student does not understand the nature of the request.
- Requests from students who do not appear to understand the nature of the request will be referred to their parents.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

8. Processing subject access requests

- 8.1 Requests for access must be made in writing.
- 8.2 Students, parents or staff may ask for a Data Subject Access form, available from reception. Completed forms should be submitted to Person responsible for DP. 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. student 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.

9. Authorised disclosures

- 9.1 The Academy will, in general, only disclose data about individuals with their consent. However there are circumstances under which the Academy's authorised officers may need to disclose data without explicit consent for that occasion. These circumstances are strictly limited to:
- Student data disclosed to authorised recipients related to education and administration necessary for the Academy to perform its statutory duties and obligations.
 - Student data disclosed to authorised recipients in respect of their child's health, safety and welfare.

- Student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the Academy.
- Staff data disclosed to relevant authorities, e.g. in respect of payroll and administrative matters.
- Only authorised and trained staff are allowed to make external disclosures of personal data.
- Data will only be made available within the Academy where the person requesting the information is a professional legitimately working within the Academy who **needs to know** the information in order to do their work. The Academy will not disclose anything on a student's record which would be likely to cause serious harm to his/her physical or mental health or that of anyone else - including anything which suggests that the student is, or have been, either the subject of or at risk of child abuse.

9.2 Definitions:

- A **legal disclosure** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the Academy, provided that the purpose of that information has been registered.
- An **illegal disclosure** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the Academy's registered purposes.

10. Data and computer security

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 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.

11. Biometric Data

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

12. CCTV

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

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:	22 November 2011
Reviewed and reapproved:	6 May 2014
Date of next review:	May 2016