



AL-HIJRAH SCHOOL DATA PROTECTION POLICY

Al-Hijrah
Secondary School
مدرسة الهجرة الثانوية

1 General

- 1.1 The Data Protection Act 1998 came into force on 1 March 2000 and superseded the Data Protection Act 1984. The purpose of the Act is to protect the rights and privacy of individuals, and to ensure that data about them are not processed without their knowledge and are processed with their consent wherever possible.
- 1.2 Al-Hijrah School is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.
- 1.3 All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.
- 1.4 Information on the processes used to comply with this policy can be obtained from the appointed Data Controller, the Finance Manager. General information about the Data Protection Act can be obtained from the Data Protection Commissioner

2 Obtaining and Processing Data

- 2.1 The School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access.
- 2.2 Processing Data means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.
- 2.3 A Data Subject is an individual who is the subject of personal data or the person to whom the information relates.
- 2.4 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 too are names and photographs if published electronically or manually.

Cherrywood Centre Burbidge Road Bordesley Green Birmingham B9 4US Phone +44(0)121 773 5466 Fax +44(0)121 773 9676

Web www.al-hijrah.bham.sch.uk Email finance@al-hijrah.bham.sch.uk

Dcsf No. 3304334



Specialist Schools
and Academies Trust
EXCELLENCE AND DIVERSITY



- 2.5 A Parent as defined in the Education Act 1996 includes any person having parental responsibility or care of a child.

3 Data Integrity

3.1 The School undertakes to ensure data integrity. In order to comply with the requirements of the Data Protection Act 1998, the School undertakes to ensure:

- Personal data must be processed fairly and lawfully;
- Personal data must be obtained only for one or more specified and lawful purposes and it must not be processed in a way that is incompatible with that purpose or those purposes;
- Personal data must be adequate, relevant and not excessive;
- Personal data must be accurate and, where necessary, kept up to date;
- Personal data must not be kept for longer than is necessary for its purpose;
- Personal data must be processed in accordance with the rights of the data subjects;
- Appropriate technical and organisational measures must be taken against accidental loss, destruction and damage to personal data;
- Personal data must not be transferred to a country or territory outside the European Union, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

3.2 Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their data will be updated as soon as is practicable. A printout of data will be provided to data subjects periodically so they can check accuracy and make any amendments.

3.3 Where a data subject challenges the accuracy of their data, the School will immediately mark the data as potentially inaccurate. In the case of any dispute, the School will attempt to resolve the issue informally. Unresolved disputes will be referred to the School Governors for their judgment. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the potentially inaccurate status will remain and all disclosures of the affected data will contain both versions of the information.

3.4 Data held about people 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 School will check records periodically for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

3.5 Sensitive Personal Data of data subjects held by the School may include:

- addresses of residence and/or telephone numbers;

- racial or ethnic origin;
- political beliefs;
- religious beliefs or beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- commission or alleged commission of any offence;
- any proceedings for any offence committed or alleged, the disposal of such proceedings or the sentence of any court in such proceedings.

4 Data Subject Access

- 4.1 The Data Protection Act 1998 extends 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. A standard subject access request is a request in writing in accordance with the guidelines issued by the Data Commissioner. An example of such a request is given as an appendix to this policy.
- 4.2 Requests from members of School staff will be processed as any standard subject access request. The copy will be given directly to the requesting staff member.
- 4.3 Requests from students will be processed as any subject access request and the copy will be given directly to the student.
- 4.4 Requests from students who do not appear to understand the nature of the request will be referred to their parents.
- 4.5 Requests from parents in respect of their own child will be processed as standard subject access requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided in accordance with any existing Education (Student Information) Regulations.

- 4.6 The School operates a CCTV monitoring system around its properties. The function of this system is to assist in the detection and deterrence of crime and to assist the Police and civil authorities in the event of a major emergency. The system will be operated in such a way as to safeguard people's right to privacy.

The School is considered the copyright owner of all such images. Recorded images will normally be preserved for a period determined by School Facilities Management. After this period, if they are not needed for evidential purposes, the recording media will be re-used. If required for evidential purposes, they will be retained for as long as is necessary to the prosecution of the case.

5 Authorised Disclosures of Data

- 5.1 The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the Data Controller may need to disclose data without explicit consent for that occasion.
- 5.2 Such circumstances are fully listed on the Data Protection Register as held by both the School Data Controller and the Data Protection Commissioner, but include the following as an example:
- Student data disclosed to authorised recipients related to education and administration necessary for the school 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 School;
 - Staff data disclosed to relevant authorities, e.g.: in respect of payroll and administrative matters;
 - Unavoidable disclosures, for example to an engineer or an LA member during maintenance of a computer system. Such people will be contractually bound not to disclose personal data.
- 5.3 Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the School by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who needs to know the information in order to do their work. The School will not disclose any data which would be likely to cause serious harm to a Data Subject's health or that of anyone else.
- 5.4 For the purposes of complying with, and ratifying, the requirements of the Data Protection Act 1998:
- A Legal Disclosure is the release of data to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered;
 - An Illegal Disclosure is the release of data to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.
 - In the event that a request for data is made by an official body outside the School's registered purposes, full documentation of the purpose for the request will be gained, along with a statement of non-disclosure, before any such data is released.

6 Data and Computer Security

- 6.1 The School undertakes to ensure security of personal data held on computers by a number of methods.
- 6.2 Physical security of data includes appropriate building security such as alarms, window bars, deadlocks and computer hardware cable locks. Network servers are locked in unspecified areas, accessible only by authorised personnel. Visitors to the School are required to sign in and out, to wear identification badges whilst in the School and are, where appropriate, accompanied.
- 6.3 Sensitive data will be encrypted according to its level of confidentiality and reviewed periodically. This includes information held on a portable device. Specialist technical advice may be sought if necessary to recover data.
- 6.4 Multiple levels of software security are applied to all computers within the School that contain or can access personal data. Such data can only be accessed by authorised users. Encrypted backups of all data, including security profiles, are taken regularly and stored securely.
- 6.5 Computers used for accessing personal data will be programmed with automated screen locks if left idle so that data cannot be viewed by casual passers-by.
- 6.6 In order to be given authorised access to the School network, staff undergo a Criminal Records Bureau vetting procedure and sign a confidentiality agreement as part of their employment contract.
- 6.7 Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data.
- 6.8 Any queries or concerns about security of data in the school should in the first instance be referred to the Data Controller, Finance Manager.

7 Publication of Data

- 7.1 Data that is normally held in the public domain is exempt from Data Protection legislation.
- 7.2 The following data may be included in authorised electronic and manual publications without notice:
 - names of members of staff with appropriate contact details;
 - names and photographs of the School Board of Governors;
 - names and photographs of the Senior Leadership Team.
- 7.3 Student details or images, either of individuals or small groups, will not normally be displayed in electronic or manual publications without explicit

consent of the parent of the student involved. However, images of large groups, where it would not be practicable to approach each person individually, may be used as deemed appropriate by the Data Controller-Finance Manager.

- 7.4 Student details or images created by people or organisations outside of the School, such as a media representative at an event, are considered exempt from this policy.

8 Disposal of Data

- 8.1 The School undertakes to ensure that all personal data stored either electronically or manually under the guidelines of this policy will not be held for longer than necessary for its purpose.
- 8.2 Beyond the life of its purpose, such data will be destroyed in such a manner so that it cannot be retrieved at a later date by either the School or any other individual.
- 8.3 In the case of electronic data, all copies will be deleted and overwritten with new data. Backup copies will be overwritten with new data.
- 8.4 In the case of manually data, all copies will be shredded.

Review of the Policy:

Date Policy Approved

Signed by Chair of Governors.....

Next Review Date.....

APPENDIX

ACCESS TO PERSONAL DATA REQUEST

DATA PROTECTION ACT 1998 Section 7.

Enquirer's Surname.....

Enquirer's Fore Names.....

Enquirer's Address

.....
.....
.....
.....

Enquirer's Postcode

Telephone Number

Are you the person who is the subject of the records you are enquiring about YES / NO

(i.e. the "Data Subject")?

If NO,

Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?

YES / NO

If YES,

Name of child or children about whose personal data records you are Enquiring

.....
.....
.....
.....

Description of Concern / Area of Concern

Description of Information or Topic(s) Requested (In your own words)

Additional information.

Please despatch Reply to: (if different from enquirer's details as stated on this form)

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that Al-Hijrah School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the Al-Hijrah School.

I agree that the reply period will commence when I have supplied sufficient information to enable Al-Hijrah School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent).....

Name of "Data Subject" (or Subject's Parent)
(PRINTED).....

Date