Data Protection Policy

Reviewed Sep 2018

1 Introduction

1.1 This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, the General Data Protection Regulations (GDPR) 2018 and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored or destroyed and irrespective of whether it is held in paper files or electronically.

1.2 This policy should be read in conjunction with the Safeguarding and Child Protection Policy. For the sake of clarity, any mention of the 'Al Haadiyah' or 'The School' includes staff.

1.3 Al Haadiyah needs to keep certain information about its staff, pupils and their parents to allow it to monitor performance, achievements and health and safety and seek to achieve its aims (as set out in the commitment statement). In so doing, the School will comply with the terms of the Data Protection Act 1998 and any associated legislation, to ensure personal data is treated in a manner that is fair and lawful. In summary, these state that personal data shall:

a. be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
b. be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose (such purposes are stated in the Trust's data protection Registration);
c. be adequate, relevant and not excessive for that purpose;
d. be accurate and kept up-to-date;
e. not be kept for longer than is necessary for that purpose;
f. be processed in accordance with the data subject's rights;
g. be kept safe from unauthorised access, accidental loss or destruction;
h. not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

1.3 Data Protection law is complex and the meaning of many of the terms used is often unclear to non-lawyers. Definitions of the main terms used are listed for reference purposes in an appendix to this Policy.

1.4 The School and all staff or others who process or use personal information on the School's behalf must ensure that they follow these principles at all times. In order to ensure that this happens, the school has adopted this data protection policy. Data protection statements will be included on any forms that are used to collect personal data.

2 Status of this Policy

2.1 This policy has been adopted by the Trustees and is a detailed statement of policy regarding one main area of information management. This policy is a condition of employment that staff will abide by the rules and policies made by the School from time to time. Any failure to follow the policy can, therefore, result in disciplinary proceedings.

3 The Data Controller and the Data Protection Compliance Officer

3.1 The School as a body is the Data Controller under the 1998 Act. However, the Data Protection Compliance Officer will deal with day to day matters. Any member of staff, pupil or any other individual who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with the Data Protection Compliance Officer.

4 Data Gathering

4.1 All personal data relating to staff, pupils or other people with who we have contact, whether held on computer or in paper files, are covered by the Act.

4.2 Only relevant personal data may be collected and the person from whom it is collected must be informed of the intended use of the data (only if that person is the data subject) and of any possible disclosures of that information which may be made.

4.3 Where we collect data which is of a more sensitive nature (for example details of medical conditions which pupils have and which the school needs to know about), the Trust will obtain the explicit consent from the parents in respect of its holding of that information.

5 Data Checking

5.1 The Trust and academies will issue regular reminders at the beginning of the academic year to staff and parents to ensure that personal data held is up-to-date and accurate.

6 Responsibilities of Staff

6.1 All staff are responsible for:

- checking that any information which they provide to the School in connection with their employment is accurate and up-to-date; and
- informing the School of any changes to information they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

7 Responsibility of Parents

7.1 Pupils and their parents should ensure that all personal information provided to the school is accurate and up-to-date. They should ensure that changes of address, etc. are notified to the school. The School cannot be held responsible for any errors unless the parent has informed the School of such changes. Subject to the above, any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, they will be informed of the corrected data.

8 Data Storage

8.1 Staff are responsible for ensuring that:

- any personal information held in respect of pupils is kept securely;
- the personal information is not disclosed either orally, in writing, electronically or by any other means accidentally or otherwise to any unauthorised third party.

8.2 Staff should note that any unauthorised disclosure will usually be a disciplinary matter.

8.3 Personal data should (in respect of manual data) be stored in a secure and safe manner. It should be kept in a locked filing cabinet, drawer or safe where it is inaccessible to anyone who does not have legitimate reason to view or process that data.

8.3 Electronic data should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up and if a copy is kept on a diskette or other removal storage media, that media must itself be kept in a locked filing cabinet, drawer or safe.

8.5 Computer work stations in administrative areas must be positioned so that they are not visible to casual observers waiting either in the office or waiting at reception or through any window which may permit unauthorised staff or visitors to view information on monitor screens.

9 Subject Access Requests

9.1 All people for whom the School holds personal information are entitled to:

a. know what information the school holds and processes about them and why;
b. know how to gain access to it;
c. understand the mechanisms used to keep the data up-to-date; and
d. know what the school is doing to comply with its obligations under the 1998 Act.
e. know who will see the information and who it is likely to be shared with

9.2 All people for whom the School holds personal information have a right under the 1998 Act to access personal data being kept about them either on computer or in paper. This is subject to certain exemptions. If a member of staff sees a written request from a data subject to see any or all personal data that the school holds about them, this should be treated as a subject access request and referred immediately to the Operations Director who will organise the Trust's response. The School will respond with 40 calendar days, as required by the 1998 Act. Focus-trust do not charge for any Subject Access Requests. Please note that the charges and timings of disclosures to pupils/parents of educational records are different (see 9.5 and 9.10 below).

9.3 The Data Protection Act gives all school pupils, regardless of age, the right of access to their school pupil records. Requests to see or receive copies of records should be made in writing to the Headteacher.

9.4 In addition to the right to be given a copy of the educational record, pupils are entitled to be given a description of the personal data which makes up the record, together with details of the purposes for which the data are processed, the sources of the data (if known) and individuals or organisations to which the data may have been disclosed.

9.5 A period of up to 15 school days are allowed in which to respond to a subject access request for educational records. (The equivalent period for other types of record is up to 40 calendar days). If asked to provide a hard copy of the record, a fee may be charged according to the number of pages. (See below for the scale of charges.) Pupils and parents may be asked for information to verify their identity if it is necessary, for instance in the case of former pupils who may not be currently known to the school. They may also be asked for information necessary to locate the data held about them. For instance, a former pupil may be asked to supply the dates between which he or she attended the school.

9.6 Only in exceptional cases will the School be able to withhold some of the information which is requested by a pupil. For example, information does not have to be disclosed by the school where that information might cause harm to the physical or mental health of the pupil or a third party. Also, information which may identify third parties (for example other pupils, although not teachers) is exempt from disclosure by the School. Information may also be withheld if in the particular case it would hinder the prevention and detection of crime or the prosecution or apprehension of offenders to provide it.

9.7 If pupils are incapable of understanding or exercising their own rights under the Data Protection Act (for instance because they are too young) parents can make subject access requests on their behalf.

9.8 If a pupil or parent feels that the school is ignoring the subject access request, is refusing to disclose the information or has not given full disclosure of the information, the matter may be referred to the Information Commissioner.

9.9 Parents have an independent right of access to pupil records (under the Education Pupil Information (England) Regulations 2000). Because of this, the pupils themselves have no right to prevent their parents from obtaining a copy of their school record.

Data Disclosures to Third Parties

10.1 Personal data will only be disclosed to organisations or individuals where the School has consent to do this, or where there is a legal requirement to make the disclosure without consent

10.2 When requests to disclose personal data are received by telephone, it is the legal responsibility of the school to ensure that the school is entitled to disclose the data and that the organisation is who it says it is. Therefore, such requests should be referred to the Operations Director who will normally ask for the request in writing.

10.3 A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later to be found to be inaccurate. This will also enable an audit trail to be created across the School.

10.4 Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

10.5 Routine consent issues are incorporated into the school's pupil and staff data gathering sheets to avoid the need for frequent similar requests for consent being made by the school. This will include information considered sensitive under the 1998 Act relating to particular health needs, such as allergies or medical conditions. The school will only use this information in the protection of the health and safety of the individual, but requires consent to process this data in the event of a medical emergency.

10.6 Therefore, any data gathering sheets that staff and pupils are required to complete will include a section requiring consent to process the applicant's personal data. A refusal to sign such a form will prevent the application from being processed.

11 Retention of data

11.1 Personal data will be retained for no longer than is necessary for the purpose for which it was collected. Standard retention times are necessary to meet various contractual requirements.

12 Disposal of data

12.1 Particular care must be taken with the disposal of personal data. Staff should be aware that the same standards should be applied to informal records, lists and printouts held by individual members of staff containing personal data as to records which are part of the formal Al Haadiyah records system. This material must not be disposed of in ordinary office waste paper bins. Personal data must be destroyed by secure methods such as shredding.

13 References

13.1 The provision of a reference will generally involve the disclosure of personal data. The School is responsible for references given in a corporate capacity. All staff references requested should be referred to the Headmaster of the School.

13.2 The School is not responsible for references given in a personal capacity. These must not be provided on School stationery and should be clearly marked as personal. The School will not provide subject access rights to confidential references written on behalf of the school about employees and sent to other organisations. This is a specific exemption allowed by the Act. The School recognises that once the reference is with the organisation to whom it was sent then no specific exemption from subject right access exists for the receiving organisation.

13.3 The School will normally provide subject right access to confidential references received about employees provided to the School by other organisations. However, the School may withhold information if it is likely to result in harm to the author or some other person or if it reveals information about another third party other than the previous supervisor or manager of the employee.

Title	Data Protection Policy
Aim	To state the Schools's policy and to outline the School's approach to data protection

Annex: Definitions in Data Protection Law

Data
Information processed by equipment (or intended to be processed by such equipment) or which is part of a relevant filing system or is an accessible record (including pupil records) or is other 'recorded information'.

Data subject
An individual who is the subject of personal data held by the school.

Personal data
Any information that identifies a living individual, including expressions of opinion, except that (Durant v FSA, 2003) courts have ruled that "mere mention of a data subject does not necessarily amount to personal data", if the person's personal, family, business or professional privacy is not compromised. (See also Schedule 2 and Sensitive Personal Data).

Processing data
Carrying out any operation with the data i.e. obtaining, recording, holding, disclosing or disposing).

Pupil Educational Records
Information held on a pupil, which must be disclosed within 15 school days of a written request addressed to the Principal by the pupil or parent.

Recorded information
Information recorded in any form, included structured information and unstructured information (where data is not organised by reference to individuals). From 1/1/05 unstructured information must be disclosed on request as well as structured information.

Rights of Data Subjects
The right to be given a description of their own personal data held by the school, why it is being held and to whom it may be disclosed. Also, he/she must be given within 40 days of a request, the information constituting the personal data and any information as to the source of the data. There is also the right to prevent any processing of personal data likely to cause unwarranted damage or distress. (See separate Subject Access Request Policy).

Refusal of Subject Access
A Subject Access Request can never be refused wholesale. The request must always be considered, and as much information as possible must be disclosed. Only certain information may be withheld if it falls under one of the exemptions.

Also the names of members of staff need not be disclosed if there is a likelihood that this will cause Physical or mental harm to the member of staff concerned.

Schedule 2
Regulates the processing of personal data which may be done only if one of the following apply: the data subject has consented to processing; processing is necessary to comply with a legal obligation on the school; processing is necessary to protect the "vital interests" of the data subject; processing is necessary to perform certain public interest activities; processing is necessary to pursue the legitimate interests of the school (e.g. CCTV cameras to prevent theft or malicious damage, etc.). In each case (except the first), the exception only applies where these interests outweigh the interests of the data subject.

Schedule 3
Sensitive personal data may only be processed if one of the Schedule 2 criteria (above) and one of the Schedule 3 criteria apply. Schedule 3 criteria include: the explicit* consent of the data subject; if it is absolutely necessary to protect the vital interests of the data subject or of a third party; for medical purposes; legal proceedings are pending; or for ethnic monitoring purposes.
*"Explicit" does not necessarily mean "written". It simply means that the data subject may make detailed statements about consent. So, a data subject may detail a particular type of information and say who it may be shared with, and may place a time limit on that sharing.

Sensitive Personal Data
Racial or ethnic origin; political opinions; religious or similar beliefs; physical or mental health; trade union membership; or data referring to the commission or alleged commission of an offence. (See also Schedules 2 and 3.)

Subject access request
A written request for personal data from the data subject. A subject access request for 'structured/unstructured personal data' must contain a description of the data.