

Bhaktivedanta Manor Primary School



Data Protection Policy

Lead	Name	Approval Date	Date to Be Reviewed
Headteacher	W Harrison	May 18, 2018	May 2020
Governing Body	Members	May 21, 2018	May 2020

Bhaktivedanta Manor School

Data Protection Policy

Statement of Policy

Bhaktivedanta Manor School collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations. This policy should be used in conjunction with the school's Acceptable Use of the Internet Use Policy.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. It also takes into account the expected provisions of the General Data Protection Regulation, which is new legislation due to come into force on 25 May 2018. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Changes to data protection legislation (GDPR, May 2018) will be monitored and implemented in order to remain compliant with all requirements.

The legal bases for processing data are as follows –

(a) Consent: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.

(c) Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations).

The members of staff responsible for data protection are mainly the Headteacher and the school administrator. However all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document. The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

- 1) Personal data shall be processed fairly and lawfully;
- 2) Personal data shall be obtained only for one or more specified and lawful purposes;
- 3) Personal data shall be adequate, relevant and not excessive;
- 4) Personal data shall be accurate and where necessary, kept up to date;
- 5) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
- 6) Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
- 7) Personal data shall be kept secure i.e. protected by an appropriate degree of security;
- 8) Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

General Policy

Bhaktivedanta Manor School is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared (see exemptions in Appendix 2)
- Check the quality and the accuracy of the information it holds. The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staffs are aware of and understand our policies and procedures.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. The policy review will be undertaken by the Headteacher, or nominated representative. The next review will take place in May 2020.

Contacts

If you have any enquires in relation to this policy, please contact the Headteacher who is the appointed Data Protection Officer for any subject access request. Please send an email with such requests to headteacher@bvmschool.co.uk with title of the email clearly marked as a subject access request.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

Appendix 1 – Bhaktivedanta Manor School procedures for responding to subject access requests made under the Data Protection Act 1998.

Rights of access to information

Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Headteacher (headteacher@bvmschool.co.uk). If the initial request does not clearly identify the information required, then further enquiries will be made. All requests should be clearly marked as subject access requests.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- birth/ marriage certificate
- P45/P60
- credit card or mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 13 or above) and the nature of the request. Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights. For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Therefore most subject access requests from parents of pupils at this school will not be granted without the express permission of the pupil. Parents at this school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, bearing in mind guidance issued from time to time from the Information Commissioner's Office.

4. The response time for subject access requests we will respond within a month. However the month will not commence until after clarification of information is sought (if needed).

5. The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

6. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the month statutory timescale.

7. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

8. If there are concerns over the disclosure of information then additional advice should be sought.

9. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

10. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

11. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies /procedures then please contact the Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

Appendix 2 - Privacy Notice -How we use pupil information

Why do we collect and use pupil information?

We collect and use pupil information under [Article 6, GDPR “Processing shall be lawful only if and to the extent that at least one of the following applies a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes and c) processing is necessary for **compliance with a legal obligation** to which the controller is subject.

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so (see list below).

We share pupils’ data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information about Individual Pupils) (England) Regulations 2013.

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Medical information (such as name of GP, relevant medical conditions)
- Attendance information (number of absence, absence reasons)
- Behavioural information (such as behaviour incidents, exclusions)
- Assessment information (such as national curriculum assessments)
- Special educational needs information
- School history (such as where pupils go when they leave us)

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Retaining pupil data

We hold pupil educational records until they leave the school, after which they are transferred to the next school the pupil attends. We retain your child's personal data for up to 3 years after your child leaves the school, or until our next Ofsted inspection (after the child leaves school). Medication records and accident records are kept for longer according to legal requirements. In some instances (child protection, or other support service referrals) we are obliged to keep your data for longer if it is necessary to comply with legal requirements.

Admission registers are retained permanently and school registers are retained whilst the pupils are still at school and for three years after the last date on the register and then destroyed.

Storing pupil data

Personal data will be stored in a secure and safe manner. Electronic data will be protected by standard password and firewall systems operated by the school. 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 with particular attention paid to the need for security of sensitive personal data.

Who do we share pupil information with?

Data may be disclosed to the following third parties without consent:

- Other schools - If a pupil transfers from Bhaktivedanta Manor School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.
- Examination authorities - This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.
- Health authorities - As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.
- Police and courts - If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered. Personal data will only be disclosed to Police Officers if they are able to supply a WA170 form which notifies of a specific, legitimate need to have access to specific personal data. This form is the agreed procedure between Hertfordshire City Council and Metropolitan Police.
- Social workers and support agencies - In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- Educational division - Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.
- Right to be Forgotten - Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

We also provide pupil level personal data to third party organisations which supply services to us for which the provision of the data is essential for the service to be provided. Decisions on whether to release this data are subject to a robust approval process, including the arrangements in place to store and handle the data.

Parents

We retain parent information (i.e. contact details) for as long as we retain the child's records. We use this information to communicate about the school, classes, and students. Parents will be blind copied into all email correspondence and their details won't be shared beyond the school administration and staff, including transportation, and those who run after school clubs (in case of an emergency).

Staff

We keep staff records until the records are no longer relevant to the purpose they were collected. As per ISKCON Child Protection Office (CPO) regulations regarding safeguarding in ISKCON institutions, the school (after seeking permission from the member of staff) will send details of any new member of staff to be checked against CPO records. Staff records are kept for a period of up to 7 years for auditing purposes by International Society For Krishna Consciousness Bhaktivedanta Manor Finance and Human Resources.

After a member of staff leaves we will keep records that allow us to provide references. Personal data which no longer has a purpose will be removed from our records.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to

<https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Review Date: May 2018

This policy will be reviewed on or before the following date: May 2020