Policy A21 – Data Protection including EYFS

(Review every year)

Date	Reviewed by	Date approved SMT	Date approved Governors	Next review date
June 2021	P Oldroyd	22.6.21	Category 3 Policy for 23.06.21 Court Meeting	May 2022 for June 2022 Bridewell Court Meeting
May 2022	T Goddings	14.06.22	Category 1 Policy for 23.06.21 Court Meeting	May 2023 for June 2023 Bridewell Court Meeting
May 2023	T Goddings	06.06.23	Category 1 Policy for 21st June 2023 Court Meeting	May 2024 for June 2024 Bridewell Court Meeting

Category definitions
1. policies where there have been no changes 2. policies containing minor changes of a factual nature 3. policies which contain significant changes or are new and require thorough reading

Contents

1. Introduction

This Data Protection Policy ("Policy") regulates and details the way in which Barrow Hills obtains, uses, holds, transfers and processes personal data and sensitive personal data (as defined in parts 2 and 7 of this policy) about individuals, and ensures that all employees know the rules for protecting personal data.

This Policy also describes individuals' rights in relation to their personal data processed by the school.

The school has practices in place in relation to their handling of personal data to ensure that they are acting in accordance with UK laws and other relevant regulatory guidance. The most notable legislation in this area is the UK Data Protection Act 2018 which is the UK implementation of the General Data Protection Regulation (GDPR).

The school will comply with the principles of the Data Protection Act to ensure that all data is:

- Fairly and lawfully processed
- Processed only for lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without consent and adequate protection

The school will also comply with these further rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

At all times, the school will endeavour to ensure that it has a legal basis for the processing of personal information.

Tina Goddings is the school's Data Protection Controller and can be contacted via cmg@barrowhills.org if anyone has any queries concerning this policy.

2. Personal Data

"Personal data" is any information about a living person, such as name and address and date of birth, which allows that living person to be identified from that information and which relates to them.

Examples of personal data which may be used by the school in its day-to-day business include employee, pupil, parent and customer details, such as names, addresses, telephone numbers and other contact details, such as email addresses and mobile numbers, CVs, performance reviews, photographs, payroll and salary information. This could affect job applicants, direct employees, temporary staff, volunteers, parents, pupils, individual consultants or contractors and visitors.

Personal data may also be relevant to unincorporated suppliers or customers, such as a sole trader business or partnership, or inquirers or complainants, and to individual contacts at third parties, customers and leads, even in respect of work contact details, such as their direct line or mobile number, or information entered about them in any management system.

The definition of personal data also includes opinions about a person, and appraisals about or statements of intent regarding them.

The laws governing how the school can use personal data apply whether the personal data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word processed document) or in structured paper records (for example, in paper files, card indices or filing cabinets).

3. Processing of personal data & Audits

The school uses or processes personal data, including sensitive personal data, see section 7, on a range of individuals for a multitude of business purposes. Such individuals may include staff and contractors, pupils and parents, alumni, business contacts, customers and prospects, job applicants and former employees, and the person whose personal data is used by the school is known as "the data subject".

When the school collects, stores, uses, discloses, updates or deletes or destroys personal data, this is called "processing". All processing is regulated by the Data Protection Act and must meet certain conditions to be carried out lawfully.

Personal data and sensitive personal data are held securely by the school and staff are regularly briefed by the ICT department and via the ICT policies on appropriate and safe data management.

4. Legislation and Information Commissioner's Office

Data protection laws are enforced in the UK by the Information Commissioner's Office (ICO). The ICO may investigate concerns and complaints, may audit the school's use or processing of personal data and may take action against the school and in some cases individuals for breach of these laws. Action may include making the school pay a fine and/or stopping the use by the school of the personal data, which may prevent it from carrying on its business. There is also the risk of negative publicity.

5. Transparency and personal data

The school is entrusted to use the personal data of individuals on the basis that the proposed use is transparent, expected and clearly defined. Accordingly, one of the main data protection obligations requires the school to process personal data fairly.

In addition, use of personal data must be lawful. In practice, this means that the school will comply with at least one of the following conditions when processing personal data:

- the individual to whom the personal data relates has consented to the processing;
- the processing is necessary for the performance of a contract between the school and the individual or to enter into that contract at the individual's request;
- the processing is necessary to comply with a legal obligation placed on the school;
- the processing is necessary to protect a vital interest of the individual where there is an imminent risk to their life or of serious harm to them otherwise;
- the processing is necessary to pursue the legitimate interest of the school or a proposed recipient of the personal data but where on balance, this would not involve disproportionate harm to the individual.

Use of personal data should meet one or more of these conditions. If there are any concerns about this, it is proposed to use personal data for additional purposes or new reasons for using personal data are contemplated, reliance on these conditions must be discussed in the first instance with the Data Protection Controller prior to being relied upon.

All new personal data processing activities and projects involving the use of personal data must be approved prior to being started as there are complex exemptions and other lawful reasons for processing which may apply. For example, if someone provides their details as a contact, it will not be possible to start sending them marketing emails unless that is covered in an appropriate notice and consent from that individual.

In addition, the school ensures its personal data is accurate and up to date. Some personal data may change from time to time, such as addresses and contact details, bank accounts and the place of employment. It is important to keep current records up to date. The school takes care to update records promptly and correctly.

6. Privacy Notices

When an individual gives the school any personal data about him or herself, the school will make sure the individual knows:

- who is responsible for the processing of their personal data;
- for what purposes the school will process the personal data provided to it;
- sufficient details about any proposed disclosures/transfers of their personal data to third parties, including any cross border transfers;
- the rights that the individual has in respect of their personal data;
- any other information that the individual should receive to ensure the processing carried out is within his/her reasonable expectations, retention periods for instance;
- who to contact to discuss or raise any personal data issue.

The school does this by providing this information is known as providing a "privacy notice". Before collecting personal data, staff at the school will give individuals providing those details

appropriate privacy notices. These may be embedded in contracts, or on websites or form part of application or other forms. The school will inform individuals about the processing of their personal data before or at the time the data is collected. The information contained in its privacy notices will be concise and easily accessible and written in clear and plain language.

The school will only process personal data in a manner and for purposes consistent with the relevant privacy notice(s) already provided to an individual. Personal data should not be collected for one purpose and then used for a second purpose unless that is also set out in the relevant notice.

7. Sensitive personal data

"Special category personal data", sometimes called "sensitive personal data", is personal data about a person's race or ethnicity, their health, their sexual preference, the medical information, their religious beliefs, their political views, trade union membership or information accusing an individual of any crime, or about any criminal prosecution against them, and the decision of the court and any punishment. The Data Protection Controller can provide further information on what is, and the handling of, Special Category Data.

Special Category personal data should not be collected or used unless essential. It must be treated as strictly confidential. Extra care must be taken with it and it must be kept more securely. In addition to the normal requirements for lawful use of any personal data such details should not be used without the explicit prior consent of the individual, which has to be clear, unambiguous and voluntary.

The school does not seek to obtain Special Category personal data unless:

- the individual concerned agrees in writing that we may do so, on the basis of a full understanding of why the school is collecting the data
- the school needs to do so to meet its obligations or exercise its rights under any relevant laws;
- in circumstances such as where the processing is necessary to either safeguard or protect the vital interests of the individual concerned

Special Category personal data should be collected and used as little as possible and be subject to more limited and strictly need to know access and used subject to greater security measures than other personal data.

8. Employee Obligations

All school staff should be aware of their obligations and comply at all times with this Policy.

All staff must ensure that personal data collected by them must be appropriate to and sufficient for the relevant purpose for which it is collected but not excessive for that purpose. Use of personal data should be minimised. Where staff are dealing with pupil and parent data already collected by the school, on Engage for example, the individual concerned will have given consent on joining the school for the processing of their personal data for the purposes of running the school.

All staff involved in the processing of personal information will:

- Read and understand this policy
- Use strong passwords
- Only keep information as long as necessary

Staff should not download personal data onto personally owned devices unless absolutely necessary. In such cases, the personal data should be deleted from the personal device as soon as is practicable after use.

9. Data retention & School Archives

Personal data must be stored securely and not be kept for any longer than required. Some records have to be retained for minimum periods by law, such as records on employee payments and their taxation under tax laws.

As a general rule, when personal data is no longer needed for the purposes for which it was collected, this personal data will be securely and permanently destroyed as soon as practicable.

The school maintains a school archive of historical interest. This means that some data that is used for research purposes and that is compatible with the purposes for which the data was originally collected may be kept indefinitely if the relevant conditions apply. These are that the data is not processed to support decisions about individuals, and that substantial damage or substantial distress is not likely to be caused to any data subject.

10. The Right to Information, the Right to Erasure and Subject Access Requests

Individuals have certain rights in relation to their personal data:

- the right to obtain information, what personal data, from where, used for what purposes and shared with which recipients, about personal data held about themselves and to obtain copies of such personal data (Subject Access Request);
- the right to prevent processing of personal data for direct marketing purposes;
- the right to object to and stop certain processing of personal data where it is likely to cause substantial unwarranted harm or distress;
- the right to have personal data corrected;
- the right to compensation for any damage or distress suffered from any breach;
- the right to be informed of automated decision making about them.

If any member of school staff receives such a request or demand from an individual, they must promptly inform the Data Protection Controller.

Individuals are also allowed to withdraw their consent where this is not required for the school's legitimate interests to the school's use of their personal data at any time. If a school employee receives such a withdrawal of consent, they must promptly inform the Data Protection Controller.

If anyone at the school receives a request to stop sending marketing materials, direct marketing communications of that type to that individual must be stopped as soon as possible.

All users including staff, parents and pupils have the right under the Data Protection Act to request to see the personal information that Barrow Hills keeps on them and this includes paper

based records. They will need to make a Subject Access request in writing to the Head who can arrange for the information to be copied, once the identity of the person requesting the information has been confirmed. Some information is exempt from the right of access; such as details of a third party or disclosure of another individual.

11. Data Security

The school endeavours to keep all personal data secure by protecting data against being accessed by other companies or individuals, for example, via hacking, from being corrupted (data corruption) or being lost or stolen. This applies to personal data in IT systems, emails and attachments and paper files. The Director of ICT is responsible for the security of all data stored on the school network and ensuring that all staff are trained appropriately following the law.

School staff must comply with the school's security procedures whenever processing personal data. The school is dependent upon all employees to help keep personal data secure. Employees must only access and use personal data they are individually authorised to access and use and which is needed for a specific task within their school role.

School employees who work away from the school's premises must comply with any additional procedures and guidelines issued by the school for home working and/or offsite working. Extra care is needed to secure personal data in such cases, particularly sensitive personal data.

The school also recognises that adequate security is important where it arranges for Third Parties to process personal data on its behalf, such as when outsourcing services to service providers, who process personal data on behalf of the school as a result ("a Data Processor"). The school remains liable for those service providers and their treatment of the personal data.

12. Disclosing personal data to Third Parties and Overseas Transfers

A disclosure of personal data is a form of processing. That means that the rules described above for fair and lawful use have to be satisfied. The school will not disclose personal data to a Third Party without first checking the disclosure is lawful and proportionate.

There are some exceptions to deal with disclosures, such as those requested lawfully by police where the information is necessary to prevent or detect a crime. Any request for personal data about an individual from government, police or other similar bodies or from journalists or other investigators should be passed immediately to the Data Protection Controller.

All aspects of child protection and safeguarding override any considerations of the GDPR.

From time to time the school may pass pupil personal data including sensitive personal data where appropriate to third parties where lawful to do so, including local authorities, other public authorities, independent school bodies such as the Independent Schools Inspectorate and the Independent Schools Council, health professionals and the school's professional advisers, who will process the data:

- to enable the relevant authorities to monitor the school's performance;
- to compile statistical information (normally used on an anonymous basis);
- to secure funding for the school and where relevant, on behalf of individual pupils
- to safeguard pupils' welfare and provide appropriate pastoral and where relevant, medical and dental care for pupils;

- where specifically requested by pupils and/or their parents or guardians;
- where necessary in connection with learning and extra-curricular activities undertaken by pupils;
- to enable pupils to take part in national and other assessments and to monitor pupils' progress and educational needs;
- to obtain appropriate professional advice and insurance for the school;
- where a reference or other information about a pupil or ex-pupil is requested by another educational establishment or employer to whom they have applied
- otherwise where reasonably necessary for the operation of the school.

Unlawful disclosure risks placing the school in breach of several obligations under data protection legislation. Special care is needed with telephone requests for information, often used by unauthorised parties to 'blag' or obtain personal data to which they are not entitled. School employees must be certain of the identity of the person with whom they are dealing, ideally have a written request for information from them and ensure any disclosures are justified and authorised in advance.

There are special rules on whether personal data can be transferred to another country. Within the EU, there are restrictions on the transfer of personal data outside the European Economic Area (EEA). Such a transfer can happen, for example, where personal data is emailed outside the EEA, where the school IT servers are hosted outside the EEA, or where there is remote on screen access from outside the EEA to personal data stored in an IT system within the EEA. This is to make sure the personal data remains safeguarded and that the individuals concerned do not lose the protection and rights they have under local law in respect of their personal data when transferred.

Actual or likely transfers of personal data to outside the EEA, especially of sensitive personal data, should be clearly set out in the privacy notices described in the fair use section of this Policy (section 5) above so that such transfers are expected by the affected individuals.

13. Development, Marketing and Fundraising

As with other types of Processing, the use of personal data for marketing and fundraising purposes must satisfy the fair and lawful use requirements set out above. This means information notices must be given, and a lawful reason for processing has to be satisfied. Typically, this will have to be consent based.

Personal data should not be used to contact individuals for marketing purposes by email, text or similar unless the individual has consented to marketing use. Individuals have a right to decline postal marketing and to object to any fundraising. Where marketing or fundraising is to be by email, text or similar electronic means, normally individual consent is needed and must clearly cover marketing by that communication method. Special rules apply as to when consent is needed and how consent is obtained, for example, whether individuals can "opt out" of or "opt in" to receiving marketing, depending on the type of marketing contemplated and the means of communication with the individual. Any objections to marketing or requests to unsubscribe must be dealt with properly and promptly.

School employees should liaise with the Data Protection Controller about any marketing or fundraising plans regarding compliance with regulation on Data Protection.