BLACK COUNTRY WHEELS SCHOOL

DfE Registration Number 333/6003
Unique Reference Number 137571

Data Protection Policy (GDPR)

Adopted September 2013

Date of Last Review: September 2019

Next Review: September 2020

Company Registration No. 06608327 Registered Charity No. 1157795

Unit 3/4, Gainsborough Industrial Trading Estate,
Rufford Road, Stourbridge, DY9 7ND.
Telephone: 0121 522 3717

DATA PROTECTION (GDPR) POLICY

Introduction

Black Country Wheels School has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

Black Country Wheels School intentionally complies with the requirements and principles of the Data Protection Act 1998 and the Data Protection Bill 2017. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

This revised Policy complies with the GDPR (effective 25 May 2018) and attention is drawn to our revised Privacy Notice that is available on the school website.

Enquiries
Information about the school's Data Protection Policy is available via School Reception. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545 745, website www.gov.uk/data-protection/ .

Fair Obtaining and Processing of Information
Black Country Wheels 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 is held, the likely recipients of the data and the data subjects' 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.

"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.

Registered Purposes
The Data Protection Registration entries for the school are available for inspection, by appointment, via reception. Explanation of any codes and categories entered will be available at that time. Registered purposes covering the data held at the school are listed on the school's Privacy Notice. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Data Integrity

The school undertakes to ensure data integrity by the following methods:

Data Accuracy
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 computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects periodically so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the school will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally.

If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data Adequacy and Relevance
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 regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. As a minimum, this will be completed once every 12 months when printed data sheets are provided for checking and accuracy.

Time for Data Records
Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Headteacher/Proprietor to ensure that obsolete data is properly erased.

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 school's policy is that:

- 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 those Parents or Carers with Parental Responsibility.
- Requests from Parents with Parental Responsibility 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.

Processing Subject Access Requests
Requests for access must be made in writing.

Students, Parents or Staff may ask for a Data Subject Access Form available from the School Office. (Example at end of this Policy.) Completed forms should be submitted via reception for the attention of the Headteacher. Provided that there is sufficient information to process the request, an entry will be made in the School Records, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 30 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Note: In the case of any written request from a parent with Parental Responsibility 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.

Authorised Disclosures
The school will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the school's authorised officer 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 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 during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LA are IT liaison/data processing officers, for example in the LA, and are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, Tutors and welfare officers, data will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. The school will not disclose anything on students' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

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 school, 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 school's registered purposes.

Data and Computer Security

Black Country Wheels School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed).

Physical Security

Appropriate building security measures are in place, such as alarms, and deadlocks. Only authorised persons are allowed in the computer server rooms. Disks, tapes, pen-drives and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

Logical Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.

Procedural Security

In order to be given authorized access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Any queries or concerns about security of data in the school should in the first instance be referred to the Headteacher.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

The following pro-forma may be used to request access to personal data.

BLACK COUNTRY WHEELS SCHOOL

Access to Personal Data Request

Data Protection Act 1998 Section 7

Enquirer's Name: ……

Address: ……..

……

Contact details: ……..

Are you the person who is the subject of the records you are enquiring about (i.e. the " Data Subject")? YES/NO

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

Data Subject Declaration

I request that the 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 school.

I agree that the reply period will commence when I have supplied sufficient information to enable the school to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the dispatch 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) ……

Dated: ……

Please return completed form to reception, marked for the attention of the Headteacher.

GDPR – Our Responsibilities and Your Rights

We have a commitment to ensuring that personal data is processed in line with GDPR and relevant UK law and that all our employees conduct themselves in line with this and other related policies. Where third parties process data on our behalf, we will ensure that the third party takes the necessary measures to maintain our commitment to protecting personal data.

This policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

Anyone processing Data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly, lawfully, and in a transparent manner. (Fairness, Lawfulness and Transparency)

(b) Processed for specified, explicit and legitimate purposes and in an appropriate way. (Purpose Limitation)

(c) Adequate, relevant and limited to what is necessary for the stated purpose. (Data Minimisation)

(d) Kept accurate and up to date. (Accuracy)

(e) Not kept longer than necessary for the stated purpose. (Storage Limitation)

(f) Processed in a manner that ensures appropriate security of Data, Including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical or organisational measures. (Security, Integrity and Confidentiality)

(g) Not transferred to another country without appropriate safeguards being in place. (Transfer Limitation)

(h) Processed in line with Data Subjects' rights. (Data Subject's Rights and Requests)

We are responsible for and need to demonstrate compliance with the data protection principles listed above (Accountability).

GDPR allows processing of Data for specific purposes, which are where it is needed:

(a) for the performance of a contract, such as an employment contract

(b) to comply with a legal obligation

(c) in order to pursue our legitimate interests (or those of a third party)and where the interests and fundamental rights of the Data Subject do not override those interests

(d) to protect the Data Subject's vital interests

(e) in the public interest, or

(f) in situations where the Data Subject has given explicit consent.

We, as Data Controller, will only process Data on the basis of one or more of the lawful bases set out above. Where consent is required, it is only effective if freely given, specific, informed and unambiguous. The Data Subject must be able to withdraw consent easily at any time and any withdrawal will be promptly honoured.

Special Categories of Data and Criminal Convictions Data will only be processed with explicit consent of the Data Subject, unless the Data Controller can rely on one or more of the other lawful bases set out above, and any additional legal bases for processing specific to these types of data, details of which have been set out in an appropriate Privacy Notice issued to the Data Subject.

Data must be processed in line with Data Subjects' rights. Data Subjects have the following rights which apply in certain circumstances:

(a)The right to be informed about processing of Data.

(b)The right of access to their own Data.

(c)The right for any inaccuracies to be corrected (rectification).

(d)The right to have information deleted (erasure).

(e)The right to restrict the processing of Data.

(f)The right to portability.

(g)The right to object to the inclusion of Data.

(h)The right to regulate any automated decision-making and profiling of Data.

(i)The right to withdraw consent when the only legal basis for processing Data is consent.

(j)The right to be notified of a Data Breach which is likely to result in high risk to their rights and freedoms.

(k)The right to make a complaint to the Information Commissioner's Office or other supervisory authority.

Data Breach Protocol

Where a Data Breach is likely to result in a risk to the rights and freedoms of the individual(s) concerned, we will report it to the Information Commissioner's Office within 72 hours of us becoming aware of it, and it may be reported in more than one instalment.

Individuals will be informed directly if the breach is likely to result in a high risk to their rights and freedoms.

If the breach is sufficient to warrant notification to the public, we will do so without undue delay.

This Policy is subject to all other policies and protocols of Black Country Wheels School.