The Blue Coat School

DATA PROTECTION POLICY

Approved by the Governors' Safeguarding, Health and Safety Committee

Signed: _____

(H Andrews – Chair of Safeguarding, Health and Safety Committee)

Date:_____

This Data Protection Policy was devised by the Bursar and the Estates & Operations Manager in consultation with the Headmaster and the Director of Marketing & Admissions.

Date of Next Review: Trinity 2027

The Blue Coat School Birmingham Limited

DATA PROTECTION POLICY

1. INTRODUCTION

1.1
The Blue Coat School complies with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. As part of its activities, the School collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, suppliers and other third parties. All staff have a part to play in ensuring the School complies with its legal obligations in respect of personal data, whether that personal data is sensitive or routine.

1.2
This Policy sets out the School's expectations and procedures with respect to processing any personal data collected from data subjects including staff, parents and pupils. Accidental breaches will happen and may not be a disciplinary issue, but any breach of this Policy may result in disciplinary action.

1.3
All staff have a responsibility to handle the personal data with which they come into contact fairly, lawfully, responsibly and securely and in accordance with all relevant School policies and procedures. In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the Employment Manual and other School policies including: ICT Acceptable Use Policy; Privacy Notice for Staff; Privacy Notice for Parents of Younger Pupils and Privacy Notice for Parents; Information Security Policy; Information and Records Retention Policy; Staff Code of Conduct; Safeguarding and Child Protection Policy and Guidance for Staff on the Use of Photographs and Videos of Pupils by the School.

1.4
This Policy applies to all staff working at the School (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, governors, contractors, agency staff, work experience students and volunteers.

2. DEFINITIONS

2.1 Personal Data

2.1.1
Personal Data (or Personal Information) is information which relates to a living person who can be identified either from that information, or from other information that is available. Personal data can be as simple as a person's name and address. It might be found on a computer database; in a file, such as a pupil report; in a register or contract of employment; pupils' exercise books; mark books; health records; and email correspondence. Personal data might also be found in documents such as a report about a child protection incident; a record about disciplinary action taken against a member of staff; photographs of pupils; an audio recording of a job interview or disciplinary hearing; contact details and other personal information held about pupils, parents and staff and their families; contact details of a member of the public who is enquiring about placing their child at the School; financial records of a parent; information about a pupil's performance and an opinion about a parent or colleague in an email.

2.2 Sensitive Personal Data

2.2.1
The School may process special category data and criminal offence data where necessary and where a lawful basis and additional condition for processing applies under the UK GDPR and Data Protection Act 2018. Special category and criminal offence data may include:

- Safeguarding or child protection matters;
- Serious or confidential medical conditions;

- Special educational needs;
- Financial matters including parent and staff bank details;
- An individual's racial or ethnic origin;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Trade Union membership;
- Physical or mental health or condition;
- Sex life including sexual orientation;
- Actual or alleged criminal activity; and
- Serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved).

2.3 Processing

Processing includes everything that is done in relation to personal data including using, disclosing, copying and storing personal data.

3. PRINCIPLES

3.1

The School will only process personal data where it has a lawful basis for doing so under the UK GDPR. Where the School processes special category data, it will also identify an additional condition for processing. Where criminal offence data is processed, the School will ensure that the processing is authorised by law and subject to appropriate safeguards.

The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by all staff. These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

4. STAFF RESPONSIBILITIES

4.1

All staff have a responsibility to handle the personal data with which they come into contact fairly, lawfully, responsibly and securely and in accordance with all relevant School policies and procedures. Responsible processing also extends to the creation and generation of new personal data and records which should always be done fairly, lawfully, responsibly and securely.

4.1.1

Staff will receive appropriate data protection training on induction and at regular intervals thereafter.

4.1.2

The School will maintain appropriate records of data protection training, personal data breaches, data protection requests, Data Protection Impact Assessments and other compliance activity.

4.1.3

Staff are expected to complete required data protection training and to follow the School's data protection policies, procedures and guidance when handling personal data.

4.2
Personal data must only be processed for the following purposes:

- Ensuring that the School provides a safe and secure environment;
- Providing pastoral care;
- Providing education and learning for the pupils;
- Providing additional activities for pupils and parents;
- Protecting and promoting the School's interests and objectives;
- Safeguarding and promoting the welfare of the pupils; and
- Fulfilling the School's contractual and other legal obligations.

4.3 Record-keeping

4.3.1
It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform a member of SLT if they believe that their personal data is inaccurate or untrue or if they are dissatisfied with the information in any way. Staff are also required to record the personal data of colleagues, pupils and their parents in an accurate, professional and appropriate manner.

4.3.2
Staff should be aware of the rights set out in Section 5 below, whereby any individuals about whom they record information in emails and notes on School business may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. Staff must ensure that they record every document or email in such a way that they would be able to stand by it if the person about whom it was recorded were to see it.

4.4 Avoiding, mitigating and reporting data breaches

4.4.1

The School will assess all personal data breaches. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the School will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Where the breach is likely to result in a high risk to individuals, the School will also notify affected individuals without undue delay.

The School will keep a record of any personal data breaches, regardless of whether or not the ICO has been informed. Staff must notify the Estates & Operations Manager, who is the Data Protection Officer, if they become aware of a personal data breach. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but the School always needs to know about them to make a decision.

5. RIGHTS OF INDIVIDUALS

5.1
In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by the School. This is known as the 'subject access right' (or the right to make 'subject access requests') which should be made to the Bursar. The School will deal with any such requests within one calendar month of receipt, unless an extension applies.

5.2
Individuals also have legal rights to:

- require the School to correct the personal data held about them if it is inaccurate;
- request that the School erases their personal data (in certain circumstances);
- request that the School restricts its data processing activities (in certain circumstances);
- receive from the School the personal data held about them for the purpose of transmitting it in a commonly used format to another data controller;

- object, on grounds relating to their particular situation, to any of the School's particular processing activities where the individual feels this has a disproportionate impact on them; and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where the School is relying on it for processing their personal data.

5.3
Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply.

6. DATA SECURITY: ONLINE AND DIGITAL

6.1
The School ensures that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. These measures include:

- using school systems rather than personal email/accounts;
- password security and MFA where applicable;
- locking screens when not situated at your device;
- secure storage of paper records;
- secure disposal/shredding;
- encrypted transfer of sensitive documents;
- restrictions on using personal devices;
- checking email recipients before sending;
- reporting lost devices immediately;
- password protecting documents;
- not downloading pupil/staff data unnecessarily.

7. PROCESSING OF CREDIT CARD DATA

7.1
The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. Guidance from the Bursar is available on the use of credit cards.

8. INTERNATIONAL TRANSFERS OF PERSONAL DATA

8.1
The School maintains a record of when it transfers personal data outside of the UK and what safeguard or derogation is relied on under the UK GDPR. The Bursar is responsible for maintaining this record.

8.2
Staff are required to speak to the Bursar before transferring personal data outside of the UK so that the School can ensure compliance with the international transfer provisions in the UK GDPR.

9. SHARING DATA WITH THIRD PARTIES

9.1

Where the School uses third-party suppliers or processors to process personal data on its behalf, the School will ensure that appropriate due diligence is carried out and that suitable contractual terms and data protection safeguards are in place.

9.2

Staff, Governors and parents must consult the Bursar before introducing or using any new system, software, platform, app or third-party service which involves the processing of personal data obtained by, or processed on behalf of, the School.

9.3

Where processing is likely to result in a high risk to individuals, including pupils, parents, staff or other members of the School community, the School will complete a Data Protection Impact Assessment before the processing begins.

9.4

The School will keep appropriate records of its data protection due diligence, supplier arrangements and Data Protection Impact Assessments.

10. MONITORING AND POLICY REVIEW

10.1

The Policy will be reviewed annually to ensure that it complies with statutory requirements and to ensure that any changes in practices are accurately reflected. It should be read in conjunction with other whole school policies as outlined above. It will be presented to the Governors' Safeguarding and Health and Safety Committee for approval in the Trinity Term. The minutes of this meeting will be presented to the Governors.