The Blue Coat School

DATA PROTECTION POLICY

Date of Next Review: Trinity 2019

This Data Protection Policy was devised by the Director of External Relations in consultation with the Senior Leadership Team and other colleagues in the School.

The Blue Coat School Birmingham Limited

DATA PROTECTION POLICY

1. INTRODUCTION

1.1
The Blue Coat School complies with the requirements of the General Data Protection Regulation (GDPR) (May 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 Pupils and Parents; Information Security Policy; Record 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, contractor, agency staff, work experience students and volunteers.

2. DEFINITIONS

2.1 Personal Data

2.1.1
Personal Data (or Personal Information) Information is information which relates to a living person who can be identified either from that information, or from the information that is available. Personal data can be as simple as a person' 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 Critical Personal Data

2.2.1
Critical Personal Data includes:

- Information concerning child protection matters;
- Information about serious or confidential medical conditions and information about special educational needs;
- Information concerning 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);

- Financial information (for example about parents and staff);
- Physical or mental health or condition;
- Information relating to actual or alleged criminal activity.

2.2 Processing

2.2.1
Processing includes everything that is done in relation to personal data including using, disclosing, copying and storing personal data.

3. PRINCIPLES

3.1
The 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.

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.

4.2
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 report breaches of personal data which risk an impact to individuals to the Information Commissioner's Office (ICO) within 72 hours. The School will also notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. 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 Bursar 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 promptly.

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.

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. MONITORING AND POLICY REVIEW

8.1
The Policy will be reviewed at least 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.