



GDPR POLICY

Babel School of Dance

For the Attention of:

All Staff

Produced by:

Sara Ridley

Approved by:

Directors / Management

Date of Publication:

August 2020

Date of review:

August 2025



Our Mission Statement

To instill a lifelong passion and love for dance

Our Values

Children First - placing the children at the centre of all we do

Empowering - enabling all in a caring environment to achieve their full potential

Excellence - a culture of creativity and aspiration

Diversity - celebrating diversity and inclusivity as a key to our success

Integrity - honesty and openness at the heart of dance school life

Respect - showing fairness, courtesy and mutual respect

GDPR Policy Contents

1. Overview	4
2. About This Policy	4
3. Definitions.....	4
4. The Babel School of Dances' Personnel's General Obligations	5
5. Data Protection Principles	6
6. Lawful Use of Personal Data	6
7. Transparent Processing – Privacy Notices	6
8. Data Quality	7
9. Personal Data Must Not Be Kept For Longer Than Needed.....	8
10. Data Security	8
11. Data Breach	8
12. Appointing Contractors Who Access the Dance School's Personal Data	9
13. Individuals' Rights	10
14. Marketing & Consent.....	11
15. Automated Decision Making and Profiling	12
16. Data Protection Impact Assessments (DPIA)	13
17. Transferring Personal Data to a Country Outside the EEA.....	13
18. Scope & Limitations	14
19. Responsibilities	14
20. Privacy Notice & Website.....	14
21. Complaints Management Process.....	15
22. Data Sharing Agreements.....	15
23. Records Management Policy	15
24. Monitoring & Review	15
25. Supporting Documents	15

1. Overview

- 1.1 The Babel School of Dance's reputation and future growth are dependent on the way the School manages and protect Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of all teachers, staff, volunteers and parents/guardians within the school.
- 1.2 As an organisation that collects, uses and stores Personal Data about its employees, employers, suppliers (sole traders, partnerships or individuals within companies), students, parents and visitors, the school recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the School's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.
- 1.3 The School has implemented this Data Protection Policy to ensure all School Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the school and will provide for a successful working and learning environment for all.
- 1.4 School Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any member of the School Personnel's contract of employment and the School reserves the right to change this Policy at any time. All members of School Personnel are obliged to comply with this Policy at all times.
- 1.5 If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the School's compliance with this Policy.

2. About This Policy

- 2.1 This Policy (and the other policies and documents referred to in it) sets out the basis on which the School will collect and use Personal Data either where the School collects it from individuals itself, or where it is provided to the School by third parties.
- 2.2 It also sets out rules on how the School handles uses, transfers and stores Personal Data. It applies to all Personal Data stored electronically, in paper form, or otherwise.

3. Definitions

- 3.1 **School** – The Babel School of Dance.
- 3.2 **School Personnel** – Any School employee or contractor who accesses any of the School's Personal Data and will include employees, contractors, and temporary personnel hired to work on behalf of the School.
- 3.3 **Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.
- 3.4 **Data Protection Laws** – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

- 3.5 **Data Protection Officer** – Our Data Protection Officer is Sara Ridley and can be contacted at: 01753 544560 or by email at babeldance83@gmail.com
- 3.6 **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.
- 3.7 **ICO** – the Information Commissioner’s Office, the UK’s data protection regulator.
- 3.8 **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the School has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.
- 3.9 **Personal Data** – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address IP address and also more sensitive types of data such as genetic data and religious beliefs. These more sensitive types of data are called “Special Categories of Personal Data” and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

- 3.10 **Processor** – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller.
- A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfillment services.
- 3.11 **Special Categories of Personal Data** – Personal Data that reveals a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

4. The Babel School of Dances' Personnel's General Obligations

- 4.1 All School Personnel must comply with this policy.
- 4.2 School Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.
- 4.3 School Personnel must not release or disclose any Personal Data:
outside the School; or

inside the School to School Personnel not authorised to access the Personal Data, without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

- 4.4 School Personnel must take all reasonable steps to ensure there is no unauthorised access to Personal Data whether by other School Personnel who are not authorised to see such Personal Data or by people outside the School

5. Data Protection Principles

- 5.1 When using Personal Data, Data Protection Laws require that the School complies with the following principles. These principles require Personal Data to be:
- 5.1.1 processed lawfully, fairly and in a transparent manner;
 - 5.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - 5.1.3 adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
 - 5.1.4 accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
 - 5.1.5 kept for no longer than is necessary for the purposes for which it is being processed; and
 - 5.1.6 processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 5.2 These principles are considered in more detail in the remainder of this Policy.
- 5.3 In addition to complying with the above requirements the School also has to demonstrate in writing that it complies with them. The School has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the School can demonstrate its compliance

6. Lawful use of Personal Data

- 6.1 In order to collect and/or use Personal Data lawfully the School needs to be able to show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds [<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing>].
- 6.2 In addition when the School collects and/or uses Special Categories of Personal Data, the School has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions [<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data>].
- 6.3 The School has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 6.1 and 6.2.

- 6.4 In most cases the legal grounds for the School processing Personal Data is because
- the processing is necessary for the School to perform its contract with an Individual or
 - the processing is necessary for the School to comply with a legal obligation; or
 - the processing is necessary for the performance of a task carried out in the public interest.
 - the processing is necessary for the health / safety of the Individual and thus processed under vital interest.
 - otherwise we will seek the Individual's consent to process their Personal Data for a particular purpose.
- 6.5 The School sets out the legal grounds for processing in the privacy notices on its website and in the enrolment form for students.
- 6.6 If the School changes how it uses Personal Data, the School needs to update this record and may also need to notify Individuals about the change. If School Personnel therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply

7. Transparent Processing – Privacy Notices

- 7.1 Where the School collects Personal Data directly from Individuals, the School will inform them about how the School uses their Personal Data. This is in a privacy notice. The School has adopted the following privacy notices: General Privacy Notice, Privacy Notice for Parents and Students, Privacy Notice for Staff.
- If the School receives Personal Data about an Individual from other sources, the School will provide the Individual with a privacy notice about how the School will use their Personal Data.
- 7.2 This will be provided as soon as reasonably possible and in any event within one month.
- If the School changes how it uses Personal Data, the School may need to notify Individuals about the change. If School Personnel therefore intend to change how they use Personal Data they must notify the Data Protection Officer who will decide whether the School
- 7.3 Personnel's intended use requires amendments to be made to the privacy notices and any other controls which need to apply

8. Data Quality – ensuring the use of accurate, up to date and relevant personal data

- 8.1 Data Protection Laws require that the School only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice and as set out in the School's record of how it uses Personal Data. The School is also
- 8.2 required to ensure that the Personal Data the School holds is accurate and kept up to date. All School Personnel that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.
- 8.3 All School Personnel that obtain Personal Data from sources outside the School shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and

limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require School Personnel to independently check the Personal Data obtained.

- 8.4 In order to maintain the quality of Personal Data, all School Personnel that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the School must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).
- 8.5 The School recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The School has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the School responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents

9. Personal Data Must Not Be Kept For Longer Than Needed

- 9.1 Data Protection Laws require that the School does not keep Personal Data longer than is necessary for the purpose or purposes for which the School collected it. The School has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the School, the reasons for those retention periods and how the School securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.
- 9.2 If School Personnel feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if School Personnel have any questions about this Policy or the School's Personal Data retention practices, they should contact the Data Protection Officer for guidance.
- 9.3

10. Data Security

- 10.1 The School takes information security very seriously and the School has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The School has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

11. Data Breach

- 11.1 Whilst the School takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and School Personnel must comply with the School's Data Breach Notification Policy. Please see the relevant policy for examples of what can be a Personal Data breach. School Personnel need to comply with in the event of Personal Data breaches.

- 11.2 Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.
- 11.3 There are three main types of Personal Data breach which are as follows:
- 11.3.1 **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a School Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people “blagging” access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
 - 11.3.2 **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and
 - 11.3.3 **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

12. Appointing Contractors Who Access The School's Personal Data

- 12.1 If the School appoints a contractor who is a Processor of the School's Personal Data, Data Protection Laws require that the School only appoints them where the School has carried out sufficient due diligence and only where the School has appropriate contracts in place.
- 12.2 One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.
- 12.3 Any contract where an organisation appoints a Processor must be in writing.
- 12.4 You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.
- 12.5 GDPR requires the contract with a Processor to contain the following obligations as a minimum:
- 12.5.1 to only act on the written instructions of the Controller;
 - 12.5.2 to not export Personal Data without the Controller's instruction;
 - 12.5.3 to ensure staff are subject to confidentiality obligations;
 - 12.5.4 to take appropriate security measures;

- 12.5.5 to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
 - 12.5.6 to keep the Personal Data secure and assist the Controller to do so;
 - 12.5.7 to assist with the notification of Data Breaches and Data Protection Impact Assessments;
 - 12.5.8 to assist with subject access/individuals rights;
 - 12.5.9 to delete/return all Personal Data as requested at the end of the contract;
 - 12.5.10 to submit to audits and provide information about the processing; and
 - 12.5.11 to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.
- 12.6 In addition the contract should set out:
- 12.6.1 The subject-matter and duration of the processing;
 - 12.6.2 the nature and purpose of the processing;
 - 12.6.3 the type of Personal Data and categories of individuals; and
 - 12.6.4 the obligations and rights of the Controller

13. Individuals' Rights

- 13.1 GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced. It is extremely important that the Schools plan how they will handle these requests under GDPR.
- 13.2 The different types of rights of individuals are reflected in this section.
- 13.3 **Subject Access Requests**
- 13.3.1 Individuals have the right under the GDPR to ask School to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right but additional information has to be provided and the timescale for providing it has been reduced from 40 days to one month (with a possible extension if it is a complex request). In addition, you will no longer be able to charge a fee for complying with the request.
- 13.3.2 Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.
- 13.4 **Right of Erasure (Right to be Forgotten)**
- 13.4.1 This is a limited right for individuals to request the erasure of Personal Data concerning them where:
- the use of the Personal Data is no longer necessary;
 - their consent is withdrawn and there is no other legal ground for the processing;

- the individual objects to the processing and there are no overriding legitimate grounds for the processing;
- the Personal Data has been unlawfully processed; and
- the Personal Data has to be erased for compliance with a legal obligation.

13.4.2 In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

13.5 Right of Data Portability

13.5.1 An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine readable format where:

- the processing is based on consent or on a contract; and
- the processing is carried out by automated means

13.5.2 This right isn't the same as subject access and is intended to give individuals a subset of their data.

13.6 The Right of Rectification and Restriction

13.6.1 Finally, individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

13.7 The School will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Laws, and will ensure that it allows Individuals to exercise their rights in accordance with the School's Rights of Individuals Policy and Rights of Individuals Procedure. Please familiarise yourself with these documents as they contain important obligations which School Personnel need to comply with in relation to the rights of Individuals over their Personal Data

14. Marketing and Consent

14.1 The School will sometimes contact Individuals to send them marketing or to promote the School. Where the School carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

14.2 Marketing consists of any advertising or marketing communication that is directed to particular individuals. When the School undertake any direct marketing it will ensure that:

14.2.1 It provides appropriate detail to individuals in our privacy notices, including for example whether profiling takes place; and

14.2.2 it will operate on an 'opt-in' basis when seeking consent to continue receiving direct marketing communications.

14.3 The School also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection.

14.4 Alternatively, the School may be able to market using a "soft opt in" if the following conditions were met:

- 14.4.1 contact details have been obtained in the course of a sale (or negotiations for a sale);
- 14.4.2 the School are marketing its own similar services; and
- 14.4.3 the School gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

15. Automated Decision Making and Profiling

- 15.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

Automated Decision Making happens where the School makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and

Profiling happens where the School automatically uses Personal Data to evaluate certain things about an Individual.

- 15.2 Any Automated Decision Making or Profiling which the School carries out can only be done once the School is confident that it is complying with Data Protection Laws. If School Personnel therefore wish to carry out any Automated Decision Making or Profiling School Personnel must inform the Data Protection Officer.
- 15.3 School Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.
- 15.4 The School does not carry out Automated Decision Making or Profiling in relation to its employees

16. Data Protection Impact Assessment (DPIA)

- 16.1 The GDPR introduce a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (“**DPIA**”). A DPIA should be started as early as practically possible in the design of a new product/service/process. The process is designed to:
 - 16.1.1 describe the collection and use of Personal Data;
 - 16.1.2 assess its necessity and its proportionality in relation to the purposes;
 - 16.1.3 assess the risks to the rights and freedoms of individuals; and
 - 16.1.4 the measures to address the risks.
- 16.2 A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The ICO’s standard DPIA template is available from www.ico.org.uk.
- 16.3 Where a DPIA reveals risks which are not appropriately mitigated the ICO will be consulted.

- 16.4 Where the School is launching or proposing to adopt a new process, product or service which involves Personal Data, the School needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The School needs to carry out a DPIA at an early stage in the process so that the School can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.
- 16.5 Situations where the School may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):
- 16.5.1 large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;
 - 16.5.2 large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or
 - 16.5.3 systematic monitoring of public areas on a large scale e.g. CCTV cameras.
- 16.6 All DPIAs must be reviewed and approved by the Data Protection Officer

17. Transferring Personal Data to a Country Outside the EEA

- 17.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be thought about whenever the School appoints a supplier outside the EEA or the School appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.
- 17.2 So that the School can ensure it is compliant with Data Protection Laws School Personnel must not export Personal Data unless it has been approved by the Data Protection Officer.
- 17.3 School Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer

18. Scope and Limitations

- 18.1 The policy covers all aspects of personal data that is identifiable.
- 18.2 **Retention of Records**
- 18.2.1 The School has a legal requirement to hold data for a range of reasons and is a requirement of certain legal bodies including but not limited Government Funding Organisations and the HMRC.
 - 18.2.2 The Data Retention Policy states what data the School holds and how long each different type of data will be kept for.
 - 18.2.3 At the end of the retention period the data will be disposed of securely following the School procedures.

18.3 **Photography**

18.3.1 Photography for any other purpose other than ID badges or Staff posters will require explicit consent from individuals and parents/guardians for under 16's

18.3.2 Consent will be obtained during the enrolment process

18.3.3 The marketing team and associated contractors will get explicit consent for any marketing activities

18.3.4 Staff undertaking trips or visits will obtain a list of students who have consented to having their photo taken.

18.3.5 As part of open events and general photography, signs must be clearly visible and guidelines followed

18.4 **Financial Data**

18.4.1 Financial Data, particularly credit card payments will be taken securely to comply with the Payment Card Industry Security Standard (PCI)

19. **Responsibilities**

19.1 It is the responsibility of all staff to ensure that all data within the School is held in accordance with GPDR guidance.

19.2 The School Management are responsible for ensuring that there is the required policy and framework in place to ensure the school is compliant with GDPR.

19.3 The Data Protection Officer is responsible for developing the policies, ongoing monitoring of compliance with GDPR in school, recording any breaches and raising awareness across the school to support compliance.

19.4 There are specific areas of the school that hold personal data and the responsibilities for each area and person responsible for ensuring compliance and control of data in each of these areas:-

19.4.1 Human Resources (Staff Data) - School Principal

19.4.2 Student Information (Student Data) - School Principal

19.4.3 Examinations (Student Data) - Exams Co-ordinators

19.4.4 Competitions (Student Data) - Competitions Co-ordinator

20. **Privacy Notice and Website**

20.1 The School will publish and update via its website, the School's Privacy notices and the Policies relating to data protection.

20.2 Students and Staff when starting at the School will have seen the Schools data protection statement and have the option of opting in or giving consent for any items not covered by a legal requirement to process

21 Complaints Management Process

- 21.1 The complaints management process is that any individual can in the first instance complain to the Principal, by emailing babeldance83@gmail.com
- 21.2 If they believe that the complaint has not been resolved successfully and wish to escalate the complaint then students and parents can use the School's complaints procedure, which can be found on the School website. Staff will use the complaints procedure by contacting the Principal.

24. Records Management Policy

- 24.1 The Records management policy shows the responsibilities of staff and areas for the recording, usage, storage and disposal of personal data across the school.

25. Monitoring and Review

- 25.1 The compliance of the policy and regular review will be undertaken in a number of ways to mitigate the risk of data breaches.
- 25.1.1 Log of all data protection requests and breaches to be held by the Data Protection officer

26. Supporting Documents

- Guidance for staff
- Breach Procedure
- Dealing with Subject Access request for data disclosing to parents
- Disposal of Data
- Records Management Policy
- Subject Access Request Form
- Subject Access Removal Form
- Privacy and Fair Processing Statements / Notices Data Sharing Policy and Agreement
- Data Sharing Log
- Data Retention Policy
- Encryption Policy
- Information Asset Register
- Digital Images Procedures
- Data Privacy Impact Assessment Process (DPIA)
- Third Party Subject Access Request Guidelines
- In addition the School will maintain and update its contract with third parties to ensure that they reflect this policy

