

# **BISHOP'S HATFIELD GIRLS' SCHOOL**

## **DATA PROTECTION POLICY**

<b>Date of last review:</b>	<b>Autumn Term 2018</b>
<b>Date of next review:</b>	<b>Autumn Term 2021</b>

**DATA PROTECTION POLICY**

**1. Policy statement and objectives**

- 1.1 The objectives of this Data Protection Policy are to ensure that Bishop's Hatfield Girls' School and its Governors and employees are informed about, and comply with, their obligations under the General Data Protection Regulation ("the GDPR") and other Data Protection legislation. It sets out the school 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.
- 1.2 The school is a Single Academy Trust and is the Data Controller for all the Personal Data processed by the Academy.
- 1.3 Everyone has rights with regard to how their personal information is handled. During the course of the school's activities, personal information will be processed about a number of different groups of people and it needs to be treated in an appropriate and lawful manner.
- 1.4 The type of information that the school may be required to handle include details of job applicants, current, past and prospective employees, pupils, parents / carers and other members of pupils' families, governors, members suppliers and other individuals related to educational or company activities. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the GDPR and other legislation. The GDPR imposes restrictions on how the information may be used.
- 1.5 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the GDPR may expose the school to enforcement action by the Information Commissioner's Office (ICO), including the risk of fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for employees. At the very least, a breach of the GDPR could damage the school's reputation and have serious consequences.

**2. Data Protection Officer**

- 2.1 The Data Protection Officer (the "DPO") is responsible for ensuring the school is compliant with the GDPR and with this policy. This post is held by Andrew North, Parent Governor, who may be contacted on [DPO@bishophatfield.herts.sch.uk](mailto:DPO@bishophatfield.herts.sch.uk) . In addition, the Business Manager acts as the Data Protection Manager (the "DPM") to support the DPO. Any questions or concerns about the operation of this policy should be referred in the first instance to the DPO.
- 2.2 The DPO and DPM will play a major role in embedding essential aspects of the GDPR into the school's culture, from ensuring the Data Protection principles are respected to preserving Data Subject rights, recording Data Processing activities and ensuring the security of processing.
- 2.3 The DPO should be involved, in a timely manner, in all issues relating to the protection of Personal Data. To do this, the school will provide the DPO with the necessary support and resources. These will include the following:
  - 2.3.1 senior management support;
  - 2.3.2 adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate and access to other services, such as HR, IT and security;

## Bishop's Hatfield Girls' School

- 2.3.3 official communication of the designation of the DPO to make known existence and function within the organisation;
  - 2.3.4 continuous training if required;
  - 2.3.5 access to external legal advice to advise the DPO on their responsibilities under this Data Protection Policy.
- 2.4 The DPO is responsible for ensuring that the school's Processing operations adequately safeguard Personal Data, in line with legal requirements. The school will ensure the independence of the DPO.
  - 2.5 The school will not instruct the DPO in respect of the carrying out of their tasks, such as how to investigate a complaint or what result should be achieved, in order to preserve their independence. The DPO will report directly to Governing Body to ensure they are aware of Data Protection issues.
  - 2.6 A DPO must not undertake other responsibilities for the school which would result in a conflict of interests with their role as DPO and the DPO cannot hold another position within the organisation that involves determining the purposes and means of processing Personal Data eg. Chief Financial Officer.
  - 2.7 In the light of this and in the event that the school decides to appoint an internal DPO, the school will take action in order to avoid conflicts of interests, including the drawing up of internal rules and safeguards to ensure the DPO role is not in conflict.
  - 2.8 If you consider that the policy has not been followed in respect of Personal Data about yourself or others you should raise the matter with the DPO.

### 3. Definition of terms

- 3.1 **Biometric Data** means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images;
- 3.2 **Consent** of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her;
- 3.3 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;
- 3.4 **Data Subjects** for the purpose of this policy include all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.
- 3.5 **Data Controllers** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
- 3.6 **Data Users** include employees, volunteers, trustees whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our Data Protection and security policies at all times;
- 3.7 **Data Processors** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

## Bishop's Hatfield Girls' School

- 3.8 **Parent** has the meaning given in the Education Act 1996 and includes any person having Parental responsibility or care of a child;
- 3.9 **Personal Data** means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- 3.10 **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;
- 3.11 **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR;
- 3.12 **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- 3.13 **Sensitive Personal Data** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, Biometric Data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- 4. Data Protection principles**
- 4.1 The School Leadership Team (SLT) will ensure that anyone processing Personal Data must comply with the enforceable principles of good practice. These provide that Personal Data must be:
- 4.1.1 processed lawfully, fairly and in a transparent manner in relation to individuals;
- 4.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- 4.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 4.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- 4.1.5 kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

## **Bishop's Hatfield Girls' School**

- 4.1.6 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. Processed lawfully, fairly and in a transparent manner**

- 5.1 The school will ensure that the processing of Personal Data is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told that the school is the Data Controller and the role of the DPO as well as the purpose for which the Data is to be processed, and the identities of anyone to whom the Data may be disclosed or transferred.
- 5.2 The school will ensure that Personal Data is processed lawfully, meeting the conditions required under GDPR:
  - 5.2.1 where we have the Consent of the Data Subject;
  - 5.2.2 where it is necessary for compliance with a legal obligation;
  - 5.2.3 where processing is necessary to protect the vital interests of the Data Subject or another person;
  - 5.2.4 where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- 5.3 The school will ensure that Personal Data is only processed for the specific purposes notified to the Data Subject when the Data was first collected, or for any other purposes specifically permitted by the Act. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the Data is processed, the Data Subject must be informed of the new purpose before any processing occurs.
- 5.4 Sensitive Personal Data
  - 5.4.1 The school will be processing Sensitive Personal Data about our stakeholders and recognises that the law states that this type of Data needs more protection.
  - 5.4.2 When Sensitive Personal Data is being processed, as well as establishing a lawful basis, a separate condition for processing it must be met. In most cases the this will be:
    - 5.4.2.1 the Data Subject's explicit Consent to the processing of such Data has been obtained
    - 5.4.2.2 processing is necessary for reasons of substantial public interest, on the basis of law which shall be proportionate to the aim pursued, where the school respects the essence of the right to Data Protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
    - 5.4.2.3 processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;
    - 5.4.2.4 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field

of employment law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

- 5.4.3 The school recognises that in addition to Sensitive Personal Data, it will also likely process information about stakeholders which is confidential in nature, for example, information about family circumstances, child protection or safeguarding issues. Appropriate safeguards will be implemented for such information, even if it does not meet the legal definition of Sensitive Personal Data.

## 5.5 Biometric Data

- 5.5.1 The school processes Biometric Data as part of an automated biometric recognition system for cashless catering. Biometric Data is a type of Sensitive Personal Data.
- 5.5.2 The school will obtain the written Consent of at least one Parent before the Data is taken from the pupil and used as part of an automated biometric recognition system. The school will not process the Biometric Data if a pupil under 18 years of age where:
  - 5.5.2.1 the child (whether verbally or non-verbally) objects or refuses to participate in the Processing of their Biometric Data;
  - 5.5.2.2 no Parent has Consented in writing to the processing; or a Parent has objected in writing to such processing, even if another Parent has given written Consent.
- 5.5.3 The school will provide reasonable alternative means of accessing services for those staff and pupils who will not be using an automated biometric recognition system. The school will comply with any guidance or advice issued by the Department for Education on the use of Biometric Data from time to time.
- 5.5.4 The school will obtain the explicit Consent of staff, Governors or other Data Subjects before processing their Biometric Data.

## 5.6 Criminal convictions and offences

- 5.6.1 The school will Process Data about criminal convictions or offences as a result of pre-vetting checks on staff and Governors prior to appointment, or due to information that may be acquired during the course of their employment or appointment.
- 5.6.2 In addition, from time to time the school may acquire information about criminal convictions or offences involving pupils or their parents. This information is not routinely collected and is only likely to be processed in specific circumstances, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter.
- 5.6.3 Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the Data secure.

## 5.7 Transparency

- 5.7.1 The school will ensure Data Subjects are informed about how their Personal Data will be processed when it is collected in order to maintain transparency through the publication of a Privacy Notice for Parents and Pupils and also for Staff and Governors.

## **Bishop's Hatfield Girls' School**

5.7.2 School staff are expected to use other appropriate and proportionate methods to tell individuals how their Personal Data is being processed, if Personal Data is being processed in a way that is not envisaged by our privacy notices and / or at the point when individuals are asked to provide their Personal Data. For example, where people are asked to complete forms requiring them to provide their Personal Data.

5.7.3 The school will ensure that privacy notices are concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

### **5.8 Consent**

5.8.1 Consent is not the only lawful basis and there are likely to be many circumstances when the school processes Personal Data and the justification for doing so is based on a lawful basis other than Consent.

5.8.2 A Data Subject Consents to processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so the school will not assume consent on the basis of silence, pre-ticked boxes or inactivity. If Consent is given in a document which deals with other matters, then the Consent will be kept separate from those other matters.

5.8.3 In the event that a pupil is aged under 13, the school will obtain Consent from the parent(s). In the event that we require Consent for processing Personal Data about pupils aged 13 or over, we will require the Consent of the pupil although, the school will make the parents aware of this process. When relying on Consent, the school will make sure that the child understands what they are consenting to, and we will not exploit any imbalance in power in the relationship.

5.8.4 The school will ensure that Data Subjects can easily withdraw Consent to processing at any time by writing to the school, and withdrawal will be promptly honoured.

5.8.5 Evidence and records of Consent will be maintained so that the school can demonstrate compliance with Consent requirements.

## **6. Specified, explicit and legitimate purposes**

6.1 Personal Data will only be collected to the extent that it is required for the specific purpose notified to the Data Subject, for example, in the Privacy Notice or at the point of collecting the Personal Data.

6.2 The school will be clear with Data Subjects about why their Personal Data is being collected and how it will be Processed. The school will not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless the Data Subject has been informed and they have consented.

## **7. Adequate, relevant and limited to what is necessary**

7.1 The school will ensure that the Personal Data collected is adequate to enable performance of key functions and that the information is relevant and limited to what is necessary.

7.2 In order to ensure compliance with this principle, SLT will ensure staff check records at appropriate intervals for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of Data.

7.3 School staff must also give due consideration to any forms stakeholders are asked to complete and consider whether all the information is required. The school will endeavour to collect Personal Data

## **Bishop's Hatfield Girls' School**

that is needed to operate as a business function only and will ensure that any Personal Data collected is adequate and relevant for the intended purposes.

- 7.4 The school will implement measures to ensure that Personal Data is processed on a 'need to know' basis. This means that the only members of staff or governors who need to know Personal Data about a Data Subject will be given access to it and no more information than is necessary for the relevant purpose will be shared.
- 7.5 When Personal Data is no longer needed for specified purposes, it will be deleted or anonymised in accordance with the school's Data Retention guidelines.

### **8. Accurate and, where necessary, kept up to date**

- 8.1 Personal Data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and staff will need to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date Data should be destroyed.
- 8.2 If a Data Subject informs the school of a change of circumstances their records will be updated as soon as is practicable.
- 8.3 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, the school will try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Data Protection Officer for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the Information Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.
- 8.4 Notwithstanding paragraph 8.3, a Data Subject continues to have rights under the GDPR and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out in paragraph 8.3 has been followed.

### **9. Data to be kept for no longer than is necessary**

- 9.1 Personal Data should not be kept longer than is necessary for the purpose for which it is held. This means that Data should be destroyed or erased from school systems when it is no longer required.
- 9.2 It is the duty of the DPO, after taking appropriate guidance for legal considerations, to ensure that obsolete Data is properly erased. The school has a Retention Policy for all Data, see Appendix 1.

### **10. Data will be Processed in a manner that ensures appropriate security of the Personal Data**

- 10.1 School staff should take steps to ensure that appropriate security measures are taken to avoid unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.
- 10.2 The school will develop, implement and maintain safeguards appropriate to its size, scope, and available resources, the amount of Personal Data held and identified risks (including use of encryption and Pseudonymisation where applicable). The DPO will evaluate and test the effectiveness of those safeguards to ensure security of processing of Personal Data from time to time.
- 10.3 Staff are responsible for protecting the Personal Data held and must implement reasonable and appropriate security measures to prevent unlawful or unauthorised processing of Personal Data and



## Bishop's Hatfield Girls' School

against the accidental loss of, or damage to, Personal Data. Staff must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

- 10.4 The school will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Staff and governors must follow all these procedures and technologies and must comply with all applicable aspects of our data policies and not attempt to circumvent the administrative, physical and technical safeguards implemented and maintained in accordance with the GDPR to protect Personal Data.
- 10.5 For the purpose of the school, Data Security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:
  - 10.5.1 **Confidentiality** means that only people who are authorised to use the Data can access it.
  - 10.5.2 **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed.
  - 10.5.3 **Availability** means that authorised users should be able to access the Data if they need it for authorised purposes.
- 10.6 It is the responsibility of all members of staff and governors to work together to ensure that the Personal Data held is kept secure and staff should identify and report any practices that do not meet these standards so that action can be taken by SLT to address any weaknesses. Anyone who has any comments or concerns about security should notify the DPM or DPO.
- 10.7 Please see our Data Security Policy in appendix 2 for details for the arrangements in place to keep Personal Data secure.
- 10.8 All staff, governors and onsite contractors will be expected to sign an Acceptable Use Agreement each year.

## 11. Processing in line with Data Subjects' rights

- 11.1 The school will uphold the rights of Data Subjects when handling their Personal Data. These include rights to:
  - 11.1.1 withdraw Consent to Processing at any time;
  - 11.1.2 receive certain information about the Data Controller's processing activities;
  - 11.1.3 request access to their Personal Data that we hold;
  - 11.1.4 prevent our use of their Personal Data for direct marketing purposes;
  - 11.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate Data or to complete incomplete Data;
  - 11.1.6 restrict or challenge Processing of their data;
  - 11.1.7 prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
  - 11.1.8 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

## **Bishop's Hatfield Girls' School**

- 11.1.9 make a complaint to the supervisory authority (the ICO); and
- 11.1.10 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

11.2 The school will verify the identity of an individual requesting Data under any of the rights listed above as set out in the school's Subject Access Request Policy. Members of staff should not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

11.3 It should be noted that the Education (Pupil Information) (England) Regulations 2005 do not apply to academies so the rights available to Parents in those Regulations to access their child's educational records are not applicable to the school. Instead, requests from Parents for Personal Data about their child must be dealt with under the GDPR (as outlined above). This is without prejudice to the obligation on the school in the Education Regulations 2014 to provide an annual report of each registered pupil's progress and attainment in the main subject areas taught to every Parent (unless they agree otherwise in writing).

## **12. Providing information over the telephone**

12.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by the school whilst also applying common sense to the particular circumstances. In particular they should:

- 12.1.1 Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- 12.1.2 Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- 12.1.3 Refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

## **13. Authorised disclosures**

13.1 The school will only disclose Data about individuals if one of the lawful bases apply.

13.2 Only authorised and trained staff are allowed to make external disclosures of Personal Data. The school will regularly share Personal Data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

- 13.2.1 Local Authorities
- 13.2.2 the Department for Education /the Education & Skills Funding Agency
- 13.2.3 the Disclosure and Barring Service
- 13.2.4 the Teaching Regulation Agency
- 13.2.5 the Teachers' Pension Service
- 13.2.6 the Local Government Pension Scheme which is administered by LPFA
- 13.2.7 Serco payroll and HR

## **Bishop's Hatfield Girls' School**

- 13.2.8 HfL
- 13.2.9 RM Education / IT provider
- 13.2.10 HMRC
- 13.2.11 the Police or other law enforcement agencies
- 13.2.12 professional advisors including Stone King and Hillier Hopkins LLP
- 13.2.13 occupational health advisors
- 13.2.14 exam boards;
- 13.2.15 the Joint Council for Qualifications;
- 13.2.16 NHS health professionals including educational psychologists and school nurses;
- 13.2.17 Education Welfare Officers;
- 13.2.18 Courts, if ordered to do so;
- 13.2.19 Prevent teams in accordance with the Prevent Duty on schools;
- 13.2.20 other schools, for example, if there is a managed move and the school has Consent to share information in these circumstances;
- 13.2.21 confidential waste collection companies.

- 13.3 Some of the organisations with whom the school shares Personal Data may also be Data Controllers in their own right in which case both the school and the external organisation may be jointly liable in the event of any Data Breaches.
- 13.4 Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. When information is shared in one-off circumstances staff must keep a record of the decision and the reasons for sharing information.
- 13.5 All Data Sharing Agreements will be retained in a central file and will be reviewed by the Data Protection Officer.
- 13.6 The school will ensure that a written contract is in place with every external Data Processors which must include specific clauses relating to the way in which the Data is processed ("GDPR clauses"). Personal Data may only be transferred to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves. Should the external organisation wish to include clauses which allocate risk to the school, staff should contact the DPO for guidance.

## **14. Reporting a Personal Data Breach**

- 14.1 A notifiable Personal Data Breach must be reported to the ICO without undue delay and where feasible within 72 hours, unless the Data Breach is unlikely to result in a risk to the individuals. School staff and governors should ensure that the Data Breach is advised to the DPO and DPM immediately in accordance with the school's Data Breach Policy in Appendix 3.

**15. Accountability**

- 15.1 The school will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with Data Protection principles. The school is responsible for, and must be able to demonstrate, compliance with the Data Protection principles.
- 15.2 The governors must ensure that the school has adequate resources and controls in place to ensure and to document GDPR compliance including:
  - 15.2.1 appointing a suitably qualified DPO and an executive team accountable for Data Privacy;
  - 15.2.2 implementing Privacy by Design when processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where Processing presents a high risk to rights and freedoms of Data Subjects;
  - 15.2.3 integrating Data Protection into internal documents including this Data Protection Policy, related policies and Privacy Notices;
  - 15.2.4 regularly training staff on GDPR, this Data Protection Policy, related policies and Data Protection matters including, for example, Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches. The school should maintain a record of training attendance by staff; and
  - 15.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

**16. Record keeping**

- 16.1 The school will keep full and accurate records of all our Data Processing activities including records of Data Subjects' Consents and procedures for obtaining Consents.
- 16.2 These records should include a list of all data held by staff in the form of an annual Data Audit.

**17. Privacy By Design and Data Protection Impact Assessment (DPIA)**

- 17.1 The school will implement Privacy by Design measures when processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with Data Privacy principles.
- 17.2 SLT will ensure that where the school processes Personal Data, there will be an assessment of what Privacy by Design measures can be implemented, taking account the data involved, the likely risks and the practical challenges or costs associated with implementation.
- 17.3 When implementing a major new system or business change program, a member of SLT will conduct a DPIA and discuss the findings with the DPO to ensure data is processed and stored appropriately.
- 17.4 A DPIA must include:
  - 17.4.1 a description of the processing, its purposes and the school's legitimate interests if appropriate;
  - 17.4.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;
  - 17.4.3 an assessment of the risk to individuals; and the risk mitigation measures in place.

## **Bishop's Hatfield Girls' School**

### **18. CCTV**

- 18.1 The school uses external CCTV to protect the buildings and assets and to protect all members of the school community.
- 18.2 The school will maintain the CCTV system and hold data according to the CCTV Policy, see Appendix 4.

### **19. Subject Access Request**

- 19.1 Should a Data Subject or their parent request access to their data through a "Subject Access Request", then the school will follow the Subject Access Request Policy, see Appendix 5. The DPO and the DPM must be informed of SARs immediately as the school as a time limit for response (one month).

### **20. Policy Review**

- 20.1 It is the responsibility of the governors to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be reported to the DPO.
- 20.2 The school will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives and will review the Policy at least every 2 years.

### **21. Enquiries**

- 21.1 Further information about the school's Data Protection Policy is available from the DPO.
- 21.2 General information about the Act can be obtained from the Information Commissioner's Office: [www.ico.gov.uk](http://www.ico.gov.uk)

## **Appendices:**

- 1. Data Retention Policy [https://drive.google.com/open?id=1-IPsn\\_vcsRgNpy7pN2KA82a2yIKSSsNOWEA4s0nndvw](https://drive.google.com/open?id=1-IPsn_vcsRgNpy7pN2KA82a2yIKSSsNOWEA4s0nndvw)
- 2. Data Security Policy <https://drive.google.com/open?id=1Q-grG8Exrzxcn0wFhaW4yXoMujlhF9RR6AX8zqliRg0>
- 3. Data Breach Policy [https://drive.google.com/open?id=1bcvf2cpb3LcJr\\_VCuT99IA7wuJ7hdjZu4Zv9DRrH7i4](https://drive.google.com/open?id=1bcvf2cpb3LcJr_VCuT99IA7wuJ7hdjZu4Zv9DRrH7i4)
- 4. CCTV Policy [https://drive.google.com/open?id=1K6A2Q2tUPxvxtCX7t-uOYncXVOpP8GwzL9h\\_gluOX8o](https://drive.google.com/open?id=1K6A2Q2tUPxvxtCX7t-uOYncXVOpP8GwzL9h_gluOX8o)
- 5. Subject Access Request Policy <https://drive.google.com/open?id=1oW-pl3vNtCJymljDYW1SMY4TD6al3a5TJ2psgwvn15A>