DATA PROTECTION POLICY

Approved by Governing Body October 2018

Review Timetable: 3 years

Renewal Date: October 2021

Status of Policy:

• This policy takes account of the changes to Data Protection as a result of the new GDPR (General Data Protection Regulations) that take effect from October 2018.

• This policy also builds upon previous Data Protection legislation, including the Data Protection Act (DPA) 1998, Environmental Regulations (EIR) and Freedom of Information Act (FOIA).

Scope:

• This Policy covers the School's acquisition, handling and disposal of the personal and sensitive personal data it hold on all Staff, including temporary staff, agency workers, volunteers, parents and pupils. It also applies to Governors and contractors. It explains the School's general approach to data protection which is to ensure that individual's personal data and information is protected and appropriately processed and provides practical guidance which will help to ensure that the School complies with the Data Protection Act 1998 (the Act) and anticipates the General Data Protection Regulations 2018 (GDPR) which become law on 25th May 2018.

1. INTRODUCTION

1.1 The new GDPR requirements set out a new responsibility for schools to inform parents, staff and any other stakeholders about how they are using personal data and who it is shared with.

1.2 Personal data is defined as any information held about a person, whether it is on paper, held electronically or held as a visual image, which can identify the individual in any way. Even if the information does not use an individual's name, but identifies the individual using a number for example (with a separate list matching the individual to that number) such information is still deemed to be personal.

1.3 By their very nature, schools hold a considerable volume of information and data to enable them to carry out their statutory provision of services, as well as the day-to-day tasks associated with caring for young people in the absence of their parents. The vast majority of this data is held by, or on, computer-based systems. Other data is held in on-site paper-based systems. This policy relates to all such data, whatever its purpose.

1.4 Some personal data is recognised as being particularly sensitive. This relates to information gathered about:

- Race or ethnic origin
- Political or religious beliefs
- Trades Union membership
- Physical or mental health
- Sexual orientation
- Criminal records

1.5

1.5 Organisations are expected to take even greater care with sensitive personal data, as it has the potential to be used against an individual in a discriminatory way.

2. THE PURPOSE OF THE GDPR

2.1 The GDPR requirements are there to provide individuals with protection related to the activity of processing their personal data in any way.

2.2 The term 'processing' covers virtually any activity which can take place using personal data, including obtaining, holding, recording or carrying out any other activity using it.

2.3 The legal documentation refers to the individual whose data is held as the 'data subject', but for the purposes of this document the term 'individual' is used.

2.4 The legal documentation refers to the organisation who holds the documentation as the 'Data Controller' as they are the party that makes decisions about how the

information is kept, how it is protected and how it is shared. Any third party with whom the data is shared as known legally as the 'Data Processor'. For the avoidance of confusion, within this document the term 'school' is used instead of 'Data Controller' and 'Third Party' is used instead of 'Data Processor'.

2.5 The School (as Data Controller) must ensure that any processing of personal data for which they are responsible – even if this is carried out by a third party - complies with the GDPR Act. Failure to do so risks enforcement action, fines and possible prosecution.

2.6 The School has appointed the Headteacher, Evelyn Chua, and Assistant Headteacher, Eva Valverde, as its Data Protection Officers, responsible for day to day compliance with this Policy. They can be contacted at Hampden Gurney Primary by telephone on 020 7723 7482 or email: head@hampdengurney.co.uk or senco@hampdengurney.co.uk

2.7 The School's duties under the Act apply throughout the period of processing personal data – as do the rights of individuals in respect of that personal data i.e. from the moment the data is obtained until the time when the data has been returned, deleted or destroyed. The duties also extend to the way that personal data is disposed of when no longer required, as the data must be disposed of securely and in a way which does not prejudice the interests of the individuals concerned.

3. APPLICATION

3.1 This policy exists in order to enforce the 8 Data Protection Principles, to ensure that personal data shall be:

I. Processed fairly and lawfully;
II. Used for one or more specified and lawful purpose (and shall not be further processed in any manner incompatible with that original purpose or purposes);
III. Requested so that it is adequate, relevant and not excessive in relation to the purpose or purposes required;
IV. Accurate – and where necessary, kept up to date;
V. Retained for no longer than is absolutely necessary for the original purpose;
VI. Processed in accordance with the rights of the individual in relation to the GDPR Act;
VII. Kept securely, with appropriate measures taken against unauthorised or unlawful access and accidental loss, damage or destruction;
VIII. Kept within the EU.

4. FAIR & LAWFUL PROCESSING (principle one)

4.1 It is a legal requirement that the School has legitimate grounds for collecting and using all the personal data that they collect.

4.2 The School must not use the data in ways that could have unjustified adverse effects on the individuals concerned.

4.3 The School must be transparent about why the information is being collected; how it

will be used; and (if appropriate) whether any Third Party will be involved in processing the data. (This should be set out in a Privacy Notice or similar e.g. ''How we use your information'.)

4.4 The School must only handle personal data in ways that the individual could reasonably expect.

4.5 The School must not do anything unlawful with the data they hold.

4.6 The School must ensure that any breach of confidence is prevented, unless the situation relates to a Safeguarding matter in relation to the safety or wellbeing of a child.

4.7 The School must prevent any breach of the Human Rights Act 1998, which includes the right to respect for private and family life, home and correspondence.

5. PROCESSING FOR A SPECIFIED PURPOSE (principle two)

5.1 The requirement for a specified purpose is there to ensure that organisations are open and transparent about why they need the information they are asking for and what they intend to do with it.

5.2 The school must issue a Privacy Notice, setting out what information they collect, in what form, how it is stored and what it is used for. It must also state where, if applicable, any Third Party is involved.

5.3 While a Privacy Notice is a requirement, it is unlikely that all parents and staff will make themselves familiar with this document and so it is good practice to ensure that any document issued to parents or staff in order to collect information makes it clear at that point what the purpose for the collection is, whether it will be shared and with whom.

5.4 The School has a duty to ensure that any Third Party is not in breach of GDPR requirements.

6. ADEQUATE & APPROPRIATE PROCESSING (principle three)

6.1 This requirement is there to ensure that schools have all the information to fulfil their statutory duties and their duties on behalf of the absent parent (e.g. in a medical emergency) but also to avoid the collection of unnecessary information.

6.2 Some information is required by the Department for Education (DFE) by law and schools are obliged to collect it from parents and to share it with the department. This should be made clear to parents at the point where the information is collected.

6.3 Other information is requested by the DFE, but is optional and parents are not obliged to disclose it. This should also be made clear to parents.

6.4 Organisations are expected to ensure that they collect only the information that is necessary to fulfil the identified purpose and to avoid what can be construed as excessive data collection.

7. ACCURATE PROCESSING (principle four)

7.1 The School is obliged to take reasonable steps to ensure that the personal data they hold is accurate. Some of the information held comes directly from parents and so it is reasonable to assume it is accurate, although care should be taken to ensure the information has been recorded accurately by the school. It may be advisable to check some information however, such as date of birth, by asking to see the Birth Certificate as children start school. (The school would then check a box to say that the certificate has been seen rather than keep a copy on file.)

7.2 The School must decide which personal data needs to be updated and how often. It will be critical, for example, that parent contact details are kept up to date for use in an emergency.

7.3 The School will not be deemed to have breached this principle, even where the information is subsequently proven inaccurate, as long as they have:

- accurately recorded information provided by the individual concerned, or by another individual or organisation; and,
- taken reasonable steps in the circumstances to ensure the accuracy of the information; and,
- made it clear where the individual has challenged the accuracy of the information.

7.4 If an individual challenges the School that their personal data is not accurate, the School should consider whether the information is in fact accurate and, if it is not, should delete or correct it. Sometimes the individual may be able to provide convincing documentary evidence that, for example, a date of birth has been recorded incorrectly. In other circumstances, the school may need to carry out its own further checks.

8. RETENTION OF PERSONAL DATA (principle five)

8.1 This principle requires organisations to retain personal data no longer than is necessary for the purpose it was obtained for. Ensuring personal data is disposed of when no longer needed will, of course, reduce the risk that it will become inaccurate, out of date or irrelevant.

8.2 In order to ensure that data is not retained for longer than necessary, it will be important for schools to:

- review the length of time that personal data is currently retained;
- consider the purpose or purposes for holding the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and

• update, archive or securely delete information if it goes out of date

8.3 It is obvious that discarding personal data too soon would be likely to disadvantage the School and, quite possibly, inconvenience the people the information is about as well.
8.4 However, it is equally true that keeping personal data for too long will cause problems. The issues are:
• there is an increased risk that the information will go out of date (breaching principle four);
• as time passes it becomes more difficult to ensure that information is accurate (breaching principle four);
• there is an increased risk that it will be deemed that the School is holding excessive amounts of information e.g. if the pupil has left the school (breaching principle three);
• even though you may no longer need the personal data, you must still make sure it is held securely (in order to comply with principle ten);
• you must also be willing and able to respond to subject access requests for any personal data you hold (principle six) – this will be more time-consuming if you are holding more data than you need.

8.5 In order to comply with this principle, it is expected that the School will carry out an annual review in order to ensure that they identify which data can now be removed.

8.6 The Data Protection Act does provide that personal data can be held for historical, statistical or research purposes. If this is the case it may be kept indefinitely, as long as it is not used in connection with decisions affecting particular individuals, or in a way that is likely to cause damage or distress. This does not mean that the information may be kept forever – it should be deleted when it is no longer needed for historical, statistical or research purposes. This could relate to documents that have historical value, such as School Registers, School Log Books, School Photographs and similar, relating back to the early years of the school's existence.

8.7 The Data Protection Act also provides that personal data can be held for legal reasons, for example relating to possible claims against the organisation. This would relate to some financial documents, some recruitment documents, accident forms, accident books, Health & Safety investigations and matters relating to SEND/Safeguarding provision.

8.8 If the School determines that some personal data may be required for legal reasons but is not required actively, it can be archived. The School must be aware that there is still the obligation to adhere to all the principles for Data Protection set out in this policy and that there is still an obligation to use such data in the case of a Subject Access Request.

8.9 The School staff responsible for deleting an individual's personal data must understand that this means the complete removal of their data, guaranteeing that it

cannot be retrieved e.g. from a physical waste basket or from an electronic one.

8.10 The ICO will accept that an organisation has deleted an individual's data if:
• it is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
• it does not give any other organisation access to that personal data;
• it surrounds the personal data with appropriate technical and organisational security; and
• it commits to permanent deletion of the information as and when this becomes possible

9.0 THE RIGHTS OF THE INDIVIDUAL (principle six)
9.1 The Data Protection Act guarantees individuals certain rights. These are:

• a right of access to a copy of the information comprised in their personal data;
• a right to object to processing that is likely to cause or is causing damage or distress;
• a right to prevent processing for direct marketing;
• a right to object to decisions being taken by automated means;
• a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
• a right to claim compensation for damages caused by a breach of the Act.

9.2 Where an individual exerts their right to access the information held on them, this is known as a Subject Access Request. That individual can be charged the statutory fee of £10 (except where this relates to a pupil's educational record – see paragraph 9.11 below) and they can be asked for this payment in advance. They are then entitled to be:

• told whether any personal data is being processed (by that organisation or by a Third Party on their behalf);
• given a description of the personal data, the reasons it is being processed, and whether it will be/has been given to any other organisations or people;
• given a copy of the information comprising the data; and given details of the source of the data (where this is available).

9.3 In most cases the school must respond to a Subject Access Request promptly and in any event within 40 calendar days of receiving it (except where it relates to a pupil – see paragraph 9.11 below).

9.4 It is important to note that an individual does not have to state that their request is a Subject Access Request – if it is clear that an individual is asking to see their personal data, then the request should be treated as a Subject Access Request even if this has not been stated.

9.5 Equally, if the request is sent to the wrong person, the School is still obliged to meet the requirements of a Subject Access Request, so it is important that all school

administrators who handle mail understand the importance of any such request, however it is worded.

9.6 The Data Protection Act specifies that a Subject Access Request relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted while the request is being dealt with. So it would be reasonable for a school to supply information that is held at the point of sending out the response, even if this is different to that held when the request was received.

9.7 It is important to note, however, that it is not acceptable to amend or delete any data if this would not otherwise have occurred. For organisations subject to Freedom of Information legislation, it is an offence to make such an amendment with the intention of preventing its disclosure.

9.8 Organisations are obliged to explain any coded information that is held that would not normally be understood to the individual making the request, but there is no expectation to give any further explanations or translations into any other language.

9.10 The Data Protection Act specifies that personal data belongs only to the individual whom it relates to – this includes in the case of children and young people. A parent only has the right to make a Subject Access Request where the pupil is not deemed to be able to understand their own personal data or where the pupil has given their consent for the request. In England, there is no statutory age at which a child is deemed to be mature enough to make their own requests, but in Scotland, this is deemed to be any child over the age of 12 years. Hampden Gurney School no pupils will be deemed responsible for making their own Subject Access Requests as all pupils are under the age of 12 years old. The following points will also be taken into consideration when granting a request relating to a child:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data being requested;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child;
- any consequences of allowing those with parental responsibility access to the child's or young person's information (this is particularly important if there have been allegations of abuse or ill treatment);
- any detriment to the child if individuals with parental responsibility cannot access this information; and
- any views the child has on whether their parents should have access to information about them.

9.11 If a Subject Access Request is made for information containing, in whole or in part, a pupil's 'educational record', a response must be provided within 15 school days. The

maximum amount that may be charged depends on the number of pages of information to be supplied.

9.12 If a Third Party makes a request on behalf of an individual, it is reasonable (and good practice) to seek confirmation from the individual that the Third Party has their permission to make the request.
9.13 Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. The Act says you do not have to comply with the request if to do so would mean disclosing information about another individual who can be identified from that information, except where:

- the other individual has consented to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without that individual's consent.

9.14 The Data Protection Act does not define what constitutes unreasonable requests, nor does it limit the number of subject access requests an individual can make to any organisation. However, it does allow some discretion when dealing with requests that are made at unreasonable intervals. The Act says that there is no obligation to comply with an identical or similar request to one that has already been dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones.

9.15 An individual does have the right, under the Act, to challenge the personal data that an organisation holds on the basis that it has the potential (or already has) caused unwarranted substantial damage of distress. A written response to such a challenge must be given within 21 calendar days, stating whether the specified information is to be removed or not. It is for the organisation to determine whether or not the data does have this potential, however an appropriate guide would be:

- substantial damage would be financial loss or physical harm; and
- substantial distress would be a level of upset, or emotional or mental pain, that goes beyond annoyance or irritation, strong dislike, or a feeling that the processing is morally abhorrent.

9.16 If an individual suffers damage because the School has breached the Act, they are entitled to claim compensation. This right can only be enforced through the courts. The Act allows an organisation to defend a claim for compensation on the basis that all reasonable care was taken, in the circumstances, to avoid the breach.

10. SECURITY (principle seven)
10.1 The Data Protection Acts states that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss of, destruction or, or damage to, personal data. In practice, this means that organisations must have appropriate security to prevent the personal

data held being accidentally or deliberately compromised. In particular, there is a need to:

- design and organise any security to fit the nature of the personal data being held and the harm that may result from a security breach;
- be clear about who, in the School is responsible for ensuring information security;
- make sure that the right physical and technical security is in place, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively, ensuring that this is reported as appropriate to the Information Commissioner.

10.2 It is important to note that as well as the potential for distress or fraud that results in any breach of security relating to and individual's personal data, there is also the potential for huge reputational damage to the individual school and to the Trust as a whole.

10.3 It is important to understand that the requirements of the Data Protection Act go beyond the way information is stored or transmitted. The seventh principle relates to the security of every aspect of the processing of personal data. This means that the security measures put in place should seek to ensure that:

- only authorised people can access, alter, disclose or destroy personal data;
- those people only act within the scope of their authority; and
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

10.4 The Trust will carry out a regular Data Protection Risk Assessment to review the nature and extent of its premises and computer systems across all academies and the central office site. This will reflect on:

- the number of staff involved in processing data;
- the extent of their access to the personal data;
- the electronic systems in place for storing personal data;
- the systems in place for storing hard-copy personal data; and
- personal data held or used by a third party on behalf of individual or the School as a whole (under the Data Protection Act you are responsible for ensuring that any data processor also has appropriate security).

10.5 As part of its Data Protection Risk Assessment, the School will identify who is the named individual responsible for overseeing Data Protection. The staff will take the lead in carrying out the Risk Assessment process. Particular attention will be given to co-ordinating with lead individuals for IT in each academy, whose roles will link closely with the work required for appropriate Data Protection.

10.6 It is vital that relevant staff in each school understand the importance of protecting personal data; that they are familiar with this policy and other procedural expectations relating to the security of information; and that they put the appropriate security procedures into practice. This should form a key part of the induction and ongoing training for all administrative and IT staff and should include:

- the organisation's duties under the Data Protection Act and restrictions on the use of personal data;
- the responsibilities of individual staff members for protecting personal data, including the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, information without authority;
- the proper procedures to use to identify callers;
- the dangers of people trying to obtain personal data by deception (for example, by pretending to be the person whom the information is about or by making "phishing" attacks) or by seeking to persuade staff to alter information when they should not do so; and
- any restrictions the organisation places on the personal use of its computers by staff or on the transfer of information beyond the premises (to avoid, for example, virus infection, spam or loss).

10.7 There is also an expectation that the School will follow appropriate procedures in ensuring that those staff given responsibility for handling personal data are trustworthy and reliable.

10.8 In the School there is a requirement to ensure that physical security is appropriate. The named Data Protection individual should liaise as appropriate with senior leaders and site staff to ensure that the following potential risks are being appropriately managed:

- doors
- locks
- windows
- alarms
- external lighting
- CCTV (where appropriate)
- access for visitors
- disposal of paper waste
- storage of portable equipment
- electrical testing
- electrical surge protection

10.9 There is also a requirement to ensure that electronic safety is being well managed, including:

- the use of encryption for any portable devices

- the use of robust and regularly updated passwords to protect access to electronic equipment
- the use of secure 'cloud' storage space
- the prevention of accidental viewing of sensitive information
- the disposal of old electronic equipment
- network security
- firewalls
- protection from cyber attack
- handling suspicious emails or attachments

10.10 When tendering for IT services across the School, the effective management of these security measures will play a key role in the selection of an IT provider.

10.11 If, in spite of all prevention measures in place, a breach of security takes place, the following points provide some guidance about action to be taken:

a) Containment and recovery – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.
b) Assessing the risks – assess any risks associated with the breach, as these are likely to affect what to do once the breach has been contained. In particular, assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen again.
c) Notification of breaches – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. Be clear about who needs to be notified and why. Consider notifying the individuals concerned; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.
d) Evaluation and response – it is important that an investigation into the causes of the breach takes place and also an evaluation of the effectiveness of organisation's response to it. If necessary, policies and procedures should then be amended accordingly.

11. WITHIN THE EEA (principle eight)
11.1 The Act requires that personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The EEA countries are:

Austria
Belgium
Bulgaria
Croatia
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
United Kingdom

11.2 This principle, in relation to schools, relates to two main aspects:
a) the transfer of personal data about pupils (their educational record) to countries not within the EEA; and
b) the storage of electronic data in the 'cloud' where servers are not sited within the EEA.

11.3 The ICO has identified the following countries as having adequate protection:
Andorra
Argentina
Faroe Islands
Guernsey
Isle of Man
Israel
Jersey
New Zealand
Switzerland
Uruguay

11.4 In relation to the transfer of a pupil's educational record to a country not identified in 11.2 or 11.3 above, this can still take place if the school is satisfied that in the particular circumstances there is an adequate level of protection for the rights of the individuals concerned.

11.5 The Act requires a risk assessment to determine whether there is adequate protection for the rights of individuals, in all the circumstances of the transfer. This is known as an assessment of adequacy. To assess adequacy, you should look at:

- the nature of the personal data being transferred;
- the country or territory of origin of the information in question;
- the country or territory of final destination of that information;
- how the data will be used and for how long; and
- the security measures to be taken in respect of the personal data in the country or territory where the data will be received.

11.6 If the assessment of these 'general adequacy' criteria concludes that, in the particular circumstances, the risks associated with the transfer are low, then the school may go ahead with the transfer. If the opposite is concluded, arrangements should be made with the individual to transfer their data in person, so that it remains under their personal control as they travel abroad.

12 COMPLAINTS

12.1 If a member of the public is concerned about the information rights practices of the School, it is an expectation that the organisation handles its own complaints.

12.2 At Hampden Gurney School, we expect any complaints about Data Protection to be referred to the individual responsible for Data Protection at Hampden Gurney, even though most complaints will need to be responded to at school level.

12.3 In responding to a complaint, it is important to reiterate the initial complaint, clarify how we have processed the individual's information and why and explaining how we will put things right if it transpires that something has gone wrong.

12.4 If a member of the public has engaged with the School but is still dissatisfied, they may report their concern to the ICO.

13 DATA SHARING

13.1 The School should adhere to guidelines for data sharing. This is even more important if sharing of data (e.g. pupil assessment data that contains names of pupils) takes place with any relevant educational third party.

14 EMPLOYMENT DATA

14.1 Schools and employers should be aware that personal data relating to employees includes, but is not limited to:

- personal information provided at the point of recruitment and selection
- employment records
- records relating to the monitoring of performance, including appraisal

- details used for payroll e.g. bank account and salary details
- information relating to health and wellbeing
- references for subsequent employment

14.2 It is important that all such information is handled in accord.