# Hunsdon JMI School Data Protection (GDPR) Policy

**Approved by Governing Body: June 2021**

**Review Date: June 2023**

**Designated Protection Officer (DPO)**

**Mr. Mike Newman**

**dpo@hunsdon.herts.sch.uk**

**Document Control**[1]

| Date modified | Description of modification | Modified by |
|---|---|---|
| 15/03/19 | Incorporation of various subsidiary documents as appendices.<br>Deletion of various irrelevant sections from template<br>Introduction of Document Control page and Contents section | Mike Newman |

[1]This policy should be reviewed by the School periodically and at least every 2 years. It is important to ensure that the DPO is aware of his or her obligations under this policy and that they receive the training and other support they need in order to fulfil this role.

**Contents**

## 1. Policy statement and objectives

1.1 The objectives of this Data Protection Policy are to ensure that Hunsdon JMI School (the "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.

1.2 The School is a Community school and is the Data Controller for all the Personal Data processed by the School.

1.3 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner.

1.4 The type of information that we 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, suppliers and other individuals that we communicate with. 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 we may use that information.

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 the School's employees. At the very least, a breach of the GDPR could damage our reputation and have serious consequences for the School and for our stakeholders.

## 2. Status of the Policy

2.1 This policy has been approved by the Governing Body of the School. It sets out our 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.

## 3. Data Protection Officer[2]

3.1 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 Mike Newman, Governor, dpo@hunsdon.herts.sch.uk. Any questions or concerns about the operation of this policy should be referred in the first instance to the DPO.

3.2 The DPO 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.

3.3 The DPO should be involved, in a timely manner, in all issues relating to the protection of personal data. To do this, the GDPR requires that DPOs are provided with the necessary

2 This section assumes that the DPO will be an internal appointment. It will need to be amended if the DPO is an external appointment.

support and resources to enable the DPO to effectively carry out their tasks. Factors that should be considered include the following:

3.3.1 senior management support;

3.3.2 time for DPOs to fulfil their duties;

3.3.3 adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate;

3.3.4 official communication of the designation of the DPO to make known existence and function within the organisation;

3.3.5 access to other services, such as HR, IT and security, who should provide support to the DPO;

3.3.6 continuous training so that DPOs can stay up to date with regard to data protection developments;

3.3.7 where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member;

3.3.8 whether the School should give the DPO access to external legal advice to advise the DPO on their responsibilities under this Data Protection Policy.

3.4 The DPO is responsible for ensuring that the School's processing operations adequately safeguard Personal Data, in line with legal requirements. This means that the governance structure within the School must ensure the independence of the DPO.

3.5 The School will ensure that the DPO does not receive instructions in respect of the carrying out of their tasks, which means that the DPO must not be instructed how to deal with a matter, such as how to investigate a complaint or what result should be achieved. Further, the DPO should report directly to the highest management level, i.e. the Governing Body.

3.6 The requirement that the DPO reports directly to the Governing Body ensures that the School's governors are made aware of the pertinent data protection issues. In the event that the School decides to take a certain course of action despite the DPO's advice to the contrary, the DPO should be given the opportunity to make their dissenting opinion clear to the Governing Body and to any other decision makers.

3.7 A DPO appointed internally by the School is permitted to undertake other tasks and duties for the organisation, but these must not result in a conflict of interests with his or her role as DPO. It follows that any conflict of interests between the individual's role as DPO and other roles the individual may have within the organisation impinge on the DPO's ability to remain independent.

3.8 In order to avoid conflicts the DPO cannot hold another position within the organisation that involves determining the purposes and means of processing personal data. Senior management positions such as chief executive, chief financial officer, head of marketing, head of IT or head of human resources positions are likely to cause conflicts. Some other positions may involve determining the purposes and means of processing, which will rule them out as feasible roles for DPOs.

3.9 In the light of this and in the event that the School decides to appoint an internal DPO, the School will take the following action in order to avoid conflicts of interests:

3.9.1 identify the positions incompatible with the function of DPO;

3.9.2 draw up internal rules to this effect in order to avoid conflicts of interests which may include, for example, allocating some of the DPO's other duties to other members of staff, appointing a deputy DPO and / or obtaining advice from an external advisor if appropriate;

3.9.3 include a more general explanation of conflicts of interests; and

3.9.4 include safeguards in the internal rules of the organisation and ensure that the job specification for the position of DPO or the service contract is sufficiently precise and detailed to avoid conflicts of interest.

3.10 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.

**4. Definition of terms**

4.1 **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;

4.2 **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;

4.3 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;

4.4 **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.

4.5 **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.

4.6 **Data Users** include employees, volunteers, governors 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;

4.7 **Data Processors** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

4.8 **Parent** has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child;

4.9 **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;

4.10 **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;

4.11 **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR;

4.12 **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;

4.13 **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.

## 5. Data protection principles

5.1 Anyone processing Personal Data must comply with the enforceable principles of good practice. These provide that Personal Data must be:

5.1.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

5.1.2 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;

5.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

5.1.4 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;

5.1.5 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

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 Processed lawfully, fairly and in a transparent manner

5.2.1 The GDPR is intended not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is (in this case

the School), who the Data Controller's representative is (in this case the DPO), the purpose for which the data is to be processed by us, and the identities of anyone to whom the Data may be disclosed or transferred.

5.2.2 For Personal Data to be processed lawfully, certain conditions have to be met. These may include:

5.2.2.1 where we have the Consent of the Data Subject;

5.2.2.2 where it is necessary for compliance with a legal obligation;

5.2.2.3 where processing is necessary to protect the vital interests of the Data Subject or another person;

5.2.2.4 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.

5.2.3 Personal data may only be 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.

Sensitive Personal Data

5.2.4 The School will be processing Sensitive Personal Data about our stakeholders. We recognise that the law states that this type of Data needs more protection. Therefore, Data Users must be more careful with the way in which we process Sensitive Personal Data.

5.2.5 When Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 5.1 above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

5.2.5.1 the Data Subject's explicit consent to the processing of such data has been obtained

5.2.5.2 processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, where we respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

5.2.5.3 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;

5.2.5.4 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 in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

5.2.5.5 The School recognises that in addition to Sensitive Personal Data, we are also likely to Process information about our stakeholders which is confidential in nature, for example, information about family circumstances, child protection or safeguarding issues. Appropriate safeguards must be implemented for such information, even if it does not meet the legal definition of Sensitive Personal Data.

[Biometric Data – does not apply

Criminal convictions and offences

5.2.6 There are separate safeguards in the GDPR for Personal Data relating to criminal convictions and offences.

5.2.7 It is likely that the School will Process Data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff and governors or due to information which we may acquire during the course of their employment or appointment.

5.2.8 In addition, from time to time we may acquire information about criminal convictions or offences involving pupils or Parents. This information is not routinely collected and is only likely to be processed by the School in specific circumstances, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter.

5.2.9 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.

Transparency

5.2.10 One of the key requirements of the GDPR relates to transparency. This means that the School must keep Data Subjects informed about how their Personal Data will be processed when it is collected.

5.2.11 One of the ways we provide this information to individuals is through a privacy notice which sets out important information what we do with their Personal Data. The School has developed privacy notices for the following categories of people:

5.2.11.1 Pupils – See Appendix 1

5.2.11.2 Parents – See Appendix 2

5.2.11.3 Staff – See Appendix 3

5.2.11.4 Governors – See Appendix 4

5.2.12 The School wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. This means that the privacy notice is just one of the tools we will use to communicate this information. Employees 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 Personal Data is collected about visitors to School premises or if we ask people to complete forms requiring them to provide their Personal Data.

5.2.13 We 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.

Consent

5.2.14 The School must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent. Consent is not the only lawful basis and there are likely to be many circumstances when we process Personal Data and our justification for doing so is based on a lawful basis other than Consent.

5.2.15 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 silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

5.2.16 In the event that we are relying on Consent as a basis for Processing Personal Data about pupils, if a pupil is aged under 13, we will need to 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, depending on the circumstances, the School should consider whether it is appropriate to inform Parents about this process. Consent is likely to be required if, for example, the School wishes to use a photo of a pupil on its website or on social media. Consent is also required is also required before any pupils are signed up to online learning platforms. Such Consent must be from the Parent is the pupil is aged under 13. When relying on Consent, we will make sure that the child understands what they are consenting to, and we will not exploit any imbalance in power in the relationship between us.[3]]

5.2.17 Data Subjects must be easily able to withdraw Consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.2.18 Unless we can rely on another legal basis of processing, Explicit Consent is usually required for processing Sensitive Personal Data. Often we will be relying on another legal basis (and not require Explicit Consent) to process most types of Sensitive Data.

5.2.19 Evidence and records of Consent must be maintained so that the School can demonstrate compliance with Consent requirements.

5.3 Specified, explicit and legitimate purposes

5.3.1 Personal data should 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. Any data which is not necessary for that purpose should not be collected in the first place.

3 Amend this section depending on whether you are a primary or secondary school.

5.3.2 The School will be clear with Data Subjects about why their Personal Data is being collected and how it will be processed. We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

5.4 Adequate, relevant and limited to what is necessary

5.4.1 The School will ensure that the Personal Data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary.

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

5.4.3 Employees must also give due consideration to any forms stakeholders are asked to complete and consider whether the all the information is required. We may only collect Personal Data that is needed to operate as a school functions and we should not collect excessive data. We should ensure that any Personal Data collected is adequate and relevant for the intended purposes.

5.4.4 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. In practice, this means that the School may adopt a layered approach in some circumstances, for example, members of staff or governors may be given access to basic information about a pupil or employee if they need to know it for a particular purpose but other information about a Data Subject may be restricted to certain members of staff who need to know it, for example, where the information is Sensitive Personal Data, relates to criminal convictions or offences or is confidential in nature (for example, child protection or safeguarding records).

5.4.5 When Personal Data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the School's data retention guidelines.

5.5 Accurate and, where necessary, kept up to date

5.5.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken 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.

5.5.2 If a Data Subject informs the School of a change of circumstances their records will be updated as soon as is practicable.

5.5.3 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, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Data Protection 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.

5.5.4 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.

5.6 Data to be kept for no longer than is necessary for the purposes for which the Personal Data are processed

5.6.1 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 our systems when it is no longer required.

5.6.2 Hunsdon JMI's Data Retention Policy is incorporated at Appendix 5

5.6.3 It is the duty of the DPO, after taking appropriate guidance for legal considerations, to ensure that obsolete data are properly erased. The School has a retention schedule for all data.

5.7 Data to be processed in a manner that ensures appropriate security of the Personal Data

5.7.1 The School has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

5.7.2 Hunsdon JMI's Data Security Policy is incorporated at Appendix 6.1

5.7.3 The GDPR requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

5.7.4 We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data.

5.7.5 Data Users are responsible for protecting the Personal Data we hold. Data Users must implement reasonable and appropriate security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Data Users must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

5.7.6 Data Users must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Data Users must comply with all applicable aspects of our Online Safety Policy, eSafety Policy and Confidentiality Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

5.7.7 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:

5.7.7.1 **Confidentiality** means that only people who are authorised to use the data can access it.

5.7.7.2 **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed.

5.7.7.3 **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

5.7.8 It is the responsibility of all members of staff and governors to work together to ensure that the Personal Data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Headteacher or the DPO.

5.7.9 Please see our eSafety Policy for details for the arrangements in place to keep Personal Data secure

Governors

5.7.10 Governors are likely to process Personal Data when they are performing their duties, for example, if they are dealing with employee issues, pupil exclusions or parent complaints. Governors should be trained on the School's data protection processes as part of their induction and should be informed about their responsibilities to keep Personal Data secure. This includes:

5.7.10.1 Ensure that Personal Data which comes into their possession as a result of their School duties is kept secure from third parties, including family members and friends

5.7.10.2 Ensure they are provided with a copy of the School's Data Security Policy

5.7.10.3 Ensuring that any School-related Personal Data stored or saved on an electronic device or computer is password

5.7.10.4 Taking appropriate measures to keep Personal Data secure, which includes ensuring that hard copy documents are securely locked away so that they cannot be access by third parties

5.7.11 Governors will be asked to read and sign an Acceptable Use Agreement.

5.8 Processing in line with Data Subjects' rights

5.8.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

5.8.1.1 withdraw Consent to processing at any time;

5.8.1.2 receive certain information about the Data Controller's processing activities;

5.8.1.3 request access to their Personal Data that we hold;

5.8.1.4 prevent our use of their Personal Data for direct marketing purposes;

5.8.1.5 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;

5.8.1.6 restrict processing in specific circumstances;

5.8.1.7 challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

5.8.1.8 request a copy of an agreement under which Personal Data is transferred outside of the EEA;

5.8.1.9 object to decisions based solely on Automated processing, including profiling (Automated Decision Making);

5.8.1.10 prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;

5.8.1.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

5.8.1.12 make a complaint to the supervisory authority (the ICO); and

5.8.1.13 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.

5.8.2 We are required to verify the identity of an individual requesting data under any of the rights listed above. Members of staff should not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

## 6. Subject Access Requests

6.1 The GDPR extends to all Data Subjects a right of access to their own Personal Data. A formal request from a Data Subject for information that we hold about them must be made in writing. The School can invite a Data Subject to complete a form but we may not insist that they do so.

6.2 It is important that all members of staff are able to recognise that a written request made by a person for their own information is likely to be a valid Subject Access Request, even if the Data Subject does not specifically use this phrase in their request or refer to the GDPR. In some cases, a Data Subject may mistakenly refer to the "Freedom of Information Act" but this should not prevent the School from responding to the request as being made under the GDPR, if appropriate. Some requests may contain a combination of a Subject Access Request for Personal Data under the GDPR and a request for information under the Freedom of Information Act 2000 ("FOIA"). Requests for information under the FOIA must be dealt with promptly and in any event within 20 school days.

6.3 Any member of staff who receives a written request of this nature must immediately forward it to the DPO as the statutory time limit for responding is one calendar month. Under the Data Protection Act 1998 (DPA 1998), Data Controllers previously had 40 calendar days to respond to a request.

6.4 As the time for responding to a request does not stop during the periods when the School is closed for the holidays, we will attempt to mitigate any impact this may have on the

rights of Data Subjects to request access to their data by implementing the following measures: Head and DPO will regularly review their email accounts.

6.5 A fee may no longer be charged to the individual for provision of this information (previously a fee of £10 could be charged under the DPA 1998).

6.6 The School may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

6.7 In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

6.8 Requests from pupils who are considered mature enough to understand their rights under the GDPR will be processed as a subject access request as outlined below and the data will be given directly to the pupil (subject to any exemptions that apply under the GDPR or other legislation). [As the age when a young person is deemed to be able to give Consent for online services is 13, we will use this age as a guide for when pupils may be considered mature enough to exercise their own subject access rights]. In every case it will be for the School, as Data Controller, to assess whether the child is capable of understanding their rights under the GDPR and the implications of their actions, and so decide whether the Parent needs to make the request on the child's behalf. A Parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age.

6.9 Requests from pupils who do not appear to understand the nature of the request will be referred to their Parents or carers.

6.10 Requests from Parents in respect of their own child will be processed as requests made on behalf of the Data Subject (the child) where the pupil is aged under 13 (subject to any exemptions that apply under the Act or other legislation). If the Parent makes a request for their child's Personal Data and the child is aged 13 or older and / or the School considers the child to be mature enough to understand their rights under the GDPR, the School shall ask the pupil for their Consent to disclosure of the Personal Data if there is no other lawful basis for sharing the Personal Data with the Parent (subject to any enactment or guidance which permits the School to disclose the Personal Data to a Parent without the child's Consent). If Consent is not given to disclosure, the School shall not disclose the Personal Data if to do so would breach any of the data protection principles.[4]

6.11 It should be noted that the Education (Pupil Information) (England) Regulations 2005 (the "Regulations") applies to maintained schools so the rights available to parents in those Regulations to access their child's educational records apply to the School. This means that following receipt of a request from a parent for a copy of their child's educational records, the School must provide a copy within 15 school days, subject to any exemptions or court orders which may apply. The School may charge a fee for providing a copy of the educational record, depending on the number of pages as set out in the Regulations. This is a separate statutory right that parents of children who attend maintained schools have so such requests should not be treated as a subject access request.

6.12 Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry should be made in the School's Subject Access log book, showing the date of receipt, the Data Subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information (not more than one calendar month from the request date). Should more information be required to

4 Amend paragraphs 12.8 – 12.10 according to whether you are a primary or secondary school.

establish either the identity of the Data Subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

6.13 Where requests are “manifestly unfounded or excessive”, in particular because they are repetitive, the School can:

6.13.1 charge a reasonable fee taking into account the administrative costs of providing the information; or

6.13.2 refuse to respond.

6.14 Where we refuse to respond to a request, the response must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Members of staff should refer to any guidance issued by the ICO on Subject Access Requests and consult the DPO before refusing a request.

6.15 Certain information may be exempt from disclosure so members of staff will need to consider what exemptions (if any) apply and decide whether you can rely on them. For example, information about third parties may be exempt from disclosure. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support from the DPO if you are unsure which exemptions apply.

6.16 [Further information about exemptions to be added once the Data Protection Bill becomes law.]

6.17 In the context of a School a subject access request is normally part of a broader complaint or concern from a Parent or may be connected to a disciplinary or grievance for an employee. Members of staff should therefore ensure that the broader context is taken into account when responding to a request and seek advice if required on managing the broader issue and the response to the request.

Providing information over the telephone

6.18 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:

6.19 Check the caller’s identity to make sure that information is only given to a person who is entitled to it.

6.20 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.

6.21 Refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

Authorised disclosures

6.22 The School will only disclose data about individuals if one of the lawful bases apply.

6.23 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:

6.23.1 Local Authorities

6.23.2 the Department for Education

6.23.3 the Disclosure and Barring Service

6.23.4 the Teaching Regulation Agency

6.23.5 the Teachers' Pension Service

6.23.6 the Local Government Pension Scheme which is administered by HCC

6.23.7 our external HR provider: (HCC)

6.23.8 our external payroll provider: (HCC)

6.23.9 Our external IT Provider: INTERM

6.23.10 HMRC

6.23.11 the Police or other law enforcement agencies

6.23.12 [our legal advisors and other consultants]

6.23.13 [insurance providers]

6.23.14 occupational health advisors

6.23.15 exam boards including QCA;

6.23.16 the Joint Council for Qualifications;

6.23.17 NHS health professionals including educational psychologists and school nurses;

6.23.18 Education Welfare Officers;

6.23.19 Courts, if ordered to do so;

6.23.20 Prevent teams in accordance with the Prevent Duty on schools;

6.23.21 other schools, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances;

6.23.22 confidential waste collection companies;

6.24 Some of the organisations we share Personal Data with may also be Data Controllers in their own right in which case we will be jointly controllers of Personal Data and may be jointly liable in the event of any data breaches.

6.25 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. However, they are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.

6.26 All Data Sharing Agreements must be signed off by the Data Protection Officer who will keep a register of all Data Sharing Agreements.

6.27 The GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the data is processed ("GDPR clauses"). A summary of the GDPR requirements for contracts with Data Processors is set out in Appendix 7. It will be the responsibility of the School to ensure that the GDPR clauses have been added to the contract with the Data Processor. 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.

6.28 In some cases Data Processors may attempt to include additional wording when negotiating contracts which attempts to allocate some of the risk relating to compliance with the GDPR, including responsibility for any Personal Data Breaches, onto the School. In these circumstances, the member of staff dealing with the contract should contact the DPO for further advice before agreeing to include such wording in the contract.

## 7. Data Breach

7.1 The GDPR requires Data Controllers to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject.

7.2 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.

7.3 If the breach is likely to result in high risk to affected Data Subjects, the GDPR, requires organisations to inform them without undue delay.

7.4 It is the responsibility of the DPO, or the nominated deputy, to decide whether to report a Personal Data Breach to the ICO.

7.5 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

7.6 Our Data Breach Response Plan is incorporated at Appendix 7

7.7 As the School is closed or has limited staff available during school holidays, there will be times when our ability to respond to a Personal Data Breach promptly and within the relevant timescales will be affected. We will consider any proportionate measures that we can implement to mitigate the impact this may have on Data Subjects when we develop our [SECURITY INCIDENT RESPONSE PLAN].

7.8 If a member of staff or governor knows or suspects that a Personal Data Breach has occurred, our [SECURITY INCIDENT RESPONSE PLAN] must be followed. In particular, the DPO or such other person identified in our Security Incident Response Plan must be notified immediately. You should preserve all evidence relating to the potential Personal Data Breach.

## 8. Accountability

8.1 The School must 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.

8.2 The School must have adequate resources and controls in place to ensure and to document GDPR compliance including:

8.3 appointing a suitably qualified DPO (where necessary) and an executive team accountable for data privacy;

8.4 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;

8.5 integrating data protection into internal documents including this Data Protection Policy, related policies and Privacy Notices;

8.6 regularly training employees and governors on the 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 must maintain a record of training attendance by School personnel; and

8.7 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.

## 9. Record keeping

9.1 The GDPR requires us to keep full and accurate records of all our Data Processing activities.

9.2 We must keep and maintain accurate records reflecting our processing including records of Data Subjects' Consents and procedures for obtaining Consents.

9.3 These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, processing activities, processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, Hunsdon JMI will undertake and routinely review a Data Asset Audit sheet

## 10. Training and audit

10.1 We are required to ensure all School personnel have undergone adequate training to enable us to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

10.2 Members of staff must attend all mandatory data privacy related training.

## 11. Privacy By Design and Data Protection Impact Assessment (DPIA)

11.1 We are required to 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.

11.2 This means that we must assess what Privacy by Design measures can be implemented on all programs/systems/processes that process Personal Data by taking into account the following:

11.2.1 the state of the art;

11.2.2 the cost of implementation;

11.2.3 the nature, scope, context and purposes of processing; and

11.2.4 the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.

11.3 We are also required to conduct DPIAs in respect to high risk processing.

11.4 The School should conduct a DPIA and discuss the findings with the DPO when implementing major system or business change programs involving the processing of Personal Data including:

11.4.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

11.4.2 Automated processing including profiling and ADM;

11.4.3 large scale processing of Sensitive Data; and

11.4.4 large scale, systematic monitoring of a publicly accessible area.

11.5 We will also undertake a DPIA as a matter of good practice to help us to assess and mitigate the risks to pupils. If our processing is likely to result in a high risk to the rights and freedom of children then a DPIA should be undertaken.

11.6 A DPIA must include:

11.6.1 a description of the processing, its purposes and the School's legitimate interests if appropriate;

11.6.2 an assessment of the necessity and proportionality of the processing in relation to its purpose;

11.6.3 an assessment of the risk to individuals; and

11.6.4 the risk mitigation measures in place and demonstration of compliance.

## 12. CCTV

12.1 The School uses CCTV in locations around the School site. This is to:

12.1.1 protect the School buildings and their assets;

12.1.2 increase personal safety and reduce the fear of crime;

12.1.3 support the Police in a bid to deter and detect crime;

12.1.4 assist in identifying, apprehending and prosecuting offenders;

12.1.5 provide evidence for the School to use in its internal investigations and / or disciplinary processes in the event of behaviour by staff, pupils or other visitors on the site which breaches or is alleged to breach the School's policies;

12.1.6 protect members of the school community, public and private property

## 13. Policy Review

13.1 It is the responsibility of the Governing Body to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be reported to the DPO.

13.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

## 14. Enquiries

14.1 Further information about the School's Data Protection Policy is available from the DPO.

14.2 General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk

**Appendix 1**

# Hunsdon JMI Privacy Notice – Pupil Data

| |
|---|
| **What is this Privacy Notice for?** |
| Hunsdon JMI School<br>Hunsdon JMI is committed to protecting the privacy and security of personal information. We collect a lot of data and information about our pupils so that we can run effectively as a school. This privacy notice explains how and why we collect pupils' data, what we do with it, who we share it with and what rights parents and pupils have. |
| **Why do we collect and use pupil information?** |
| We have a legal obligation to submit pupil data to the Department for Education (DfE) and the Local Authority as well as other regulatory bodies.<br>We also use pupil data to support our function of running a school and for safeguarding purposes.<br>Where we collect data not covered by these reasons, e.g. for publishing photos on our website, we will ask for your consent. This consent can be withdrawn at any time.<br>To find out more about the data collection requirements placed on us by the DfE (for example; via the school census) go to: https://www.gov.uk/education/data-collection-and-censuses-for-schools |
| **What pupil information do we collect, hold and share?** |
| This is a wide range of information from name, date of birth, ethnicity etc. to attendance, assessment, medical and safeguarding information. |
| **How long do we keep the information?** |
| We hold pupil data securely for specific periods, as recommended by both national and local guidelines. Certain types of data may be held for longer, e.g. safeguarding. For more information on the recommended timescales please see our Data Retention Policy |
| **Who do we share pupil information with?** |
| We may share pupil information with the DfE, the Local Authority, and other bodies and organisations. We do not share information about pupils with anyone without consent unless the law or our policies allow us to do so. When we share personal data, we will provide the minimum amount necessary to fulfil the purpose for which it is required. For more details, please see our Data Protection (GDPR) Policy |

| |
|---|
| **How can you request access to the pupil information we hold?** |
| Parents and/or pupils have the right to request access to pupil information that we hold via a Subject Access Request (SAR). To make a request for your or your child's personal data, contact the school's designated Data Protection Officer (DPO). The legal timescales for the school to respond to a Subject Access Request is one calendar month. As the school has limited staff resources outside of term time, we encourage parents to submit Subject Access Requests during term time and to avoid sending a request during periods when the school is closed or is about to close for the holidays, if possible. This will assist us in responding to your request as promptly and fully as possible. [For further information about how we handle Subject Access Requests, please see our Data Protection (GDPR) Policy |
| **For more information about Data Protection Regulations and your rights see:** |
| https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ |
| If you have a concern about the way we are collecting or using your personal data, please raise with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/ |
| **If you would like to discuss anything in this privacy notice, please contact:** |
| Mr Mike Newman dpo@hunsdon.herts.sch.uk |

**Appendix 2**

# Hunsdon JMI Privacy Notice – Parents / Carers Data

| **What is this Privacy Notice for?** |
|---|
| Hunsdon JMI School<br>Hunsdon JMI is committed to protecting the privacy and security of personal information. We collect data and information about parents / carers of our pupils so that we can operate effectively as a school. This privacy notice explains how and why we collect parent / carer data, what we do with it, who we share it with and what rights parents have. |
| **Why do we collect and use parent / carer information?** |
| We process information about parents / carers as part of our legal obligation to provide an education to our pupils, to support our function of running a school and for safeguarding purposes.<br>Where we process data not covered by these reasons, we will ask for your consent. This consent can be withdrawn at any time. |
| **What parent / carer information do we collect, hold and share?** |
| This will include personal information such as name, name, address, telephone number and email address. It could also include information relating to your identity, marital status, employment status, religion, ethnicity, language, medical conditions and free school meal / pupil premium eligibility / entitlement to certain benefits, information about court orders in place affecting parenting arrangements for pupils. |
| **How long do we keep the information?** |
| We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, insurance or reporting requirements, as recommended by both national and local guidelines. Certain types of data may be held for longer, e.g. safeguarding. For more information on the recommended timescales please see our Data Protection (GDPR) Policy[or e.g. links to IRMS toolkit etc.] |

| |
|---|
| **Who do we share your information with?** |
| We routinely share parent / carer information with schools that pupils attend after leaving us. We may share pupil information with the DfE, the Local Authority, and other bodies and organisations. We do not share information with anyone without consent unless the law or our policies allow us to do so. When we share personal data, we will provide the minimum amount necessary to fulfil the purpose for which it is required. For more details, please see our Data Retention Policy |
| **How can you request access to your personal data?** |
| Parents / carers have the right to request access to information about them that we hold via a Subject Access Request (SAR). To make a request for your or your child's personal data, contact the school's designated Data Protection Officer (DPO). The legal timescales for the school to respond to a Subject Access Request is one calendar month. As the school has limited staff resources outside of term time, we encourage you to submit Subject Access Requests during term time and to avoid sending a request during periods when the school is closed or is about to close for the holidays, if possible. This will assist us in responding to your request as promptly and fully as possible. For further information about how we handle Subject Access Requests, please see our Data Protection (GDPR) Policy |
| **For more information about Data Protection Regulations and your rights see:** |
| https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/<br><br>If you have a concern about the way we are collecting or using your personal data, please raise with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/ |
| **If you would like to discuss anything in this privacy notice, please contact:** |
| Mr Mike Newman dpo@hunsdon.herts.sch.uk |

**Appendix 3**

# Hunsdon JMI Privacy Notice – Staff Data

| **What is this Privacy Notice for?** |
|---|
| Hunsdon JMI is committed to protecting the privacy and security of your personal information.<br>This privacy notice describes how we collect and use personal information about you and who we share it with, before, during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).<br>It applies to all employees, workers and contractors. |
| **Why do we collect and use staff information?** |
| We need data from you primarily to allow us to perform our contract with you, but also because we have a legal obligation to submit staff data to the Department for Education (DfE) and the Local Authority as well as other regulatory bodies.<br>We also use your data to support our function of running a school and for safeguarding purposes.<br>Where we collect data not covered by these reasons we will ask for your consent. This consent can be withdrawn at any time.<br>To find out more about the data collection requirements placed on us by the DfE (for example; via the School Workforce census) go to: https://www.gov.uk/education/data-collection-and-censuses-for-schools |
| **What staff information do we collect, hold and share?** |
| This is a wide range of information from name, date of birth, ethnicity etc. to NI number, bank account details, employment records etc.<br>For a more complete list see our Data Retention Policy |
| **How long do we keep the information?** |
| We hold data securely for specific periods, as recommended by both national and local guidelines. Certain types of data may be held for longer, e.g. safeguarding. For more information on the recommended timescales please see our Data Retention Policy |

| |
|---|
| **Who do we share your information with?** |
| We may share information with the DfE, the Local Authority, and other bodies and organisations. We do not share information with anyone without consent unless the law or our policies allow us to do so. When we share personal data, we will provide the minimum amount necessary to fulfil the purpose for which it is required. For more details, please see our Data Retention Policy |
| **How can you request access to the information we hold?** |
| Staff have the right to request access to information about them that we hold via a Subject Access Request (SAR). To make a request for your personal data, contact the school's designated Data Protection Officer (DPO). The legal timescales for the school to respond to a Subject Access Request is one calendar month. As the school has limited staff resources outside of term time, we encourage you to submit Subject Access Requests during term time and to avoid sending a request during periods when the school is closed or is about to close for the holidays, if possible. This will assist us in responding to your request as promptly and fully as possible. [For further information about how we handle Subject Access Requests, please see our Data Protection (GDPR) Policy |
| **For more information about Data Protection Regulations and your rights see:** |
| https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ |
| If you have a concern about the way we are collecting or using your personal data, please raise with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/ |
| **If you would like to discuss anything in this privacy notice, please contact:** |
| Mr Mike Newman dpo@hunsdon.herts.sch.uk |

**Appendix 4**

# Hunsdon JMI Privacy Notice – Governors' Data

| |
|---|
| **What is this Privacy Notice for?** |
| Hunsdon JMI is committed to protecting the privacy and security of your personal information.<br>This privacy notice describes how we collect and use personal information about you, and who we share it with, before, during and after your relationship with us as a [governor/trustee] in accordance with the General Data Protection Regulation (GDPR). |
| **Why do we collect and use your information?** |
| We collect personal information about governors / trustees through the application and recruitment process. We process this data for legal obligations, to support our function of running a school and for safeguarding purposes.<br>Where we collect data not covered by these reasons we will ask for your consent. This consent can be withdrawn at any time. |
| **What information do we collect, hold and share?** |
| This is a wide range of information from name, date of birth, contact details etc. to information acquired as part of your application to become a [governor/trustee].<br>For a more complete list see our Data Retention Policy |
| **How long do we keep the information?** |
| We hold data securely for specific periods, as recommended by both national and local guidelines. Certain types of data may be held for longer, e.g. safeguarding. For more information on the recommended timescales please see our Data Retention Policy |
| **Who do we share your information with?** |
| We may share information with the DfE, the Local Authority, and other bodies and organisations. We do not share information with anyone without consent unless the law or our policies allow us to do so. When we share personal data, we will provide the minimum amount necessary to fulfil the purpose for which it is required. For more details, please see our Data Retention Policy |

| |
|---|
| **How can you request access to the information we hold?** |
| You have the right to request access to information about you that we hold via a Subject Access Request (SAR). To make a request for your personal data, contact the school's designated Data Protection Officer (DPO). The legal timescales for the school to respond to a Subject Access Request is one calendar month. As the school has limited staff resources outside of term time, we encourage you to submit Subject Access Requests during term time and to avoid sending a request during periods when the school is closed or is about to close for the holidays, if possible. This will assist us in responding to your request as promptly and fully as possible. [For further information about how we handle Subject Access Requests, please see our Data Protection (GDPR) Policy |
| **For more information about Data Protection Regulations and your rights see:** |
| https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ |
| If you have a concern about the way we are collecting or using your personal data, please raise with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/ |
| **If you would like to discuss anything in this privacy notice, please contact:** |
| Mr Mike Newman dpo@hunsdon.herts.sch.uk |

**Appendix 5**

# Hunsdon JMI School – Data Retention Policy

**November 2018**

The School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited. It covers:

• Scope

• Responsibilities

• Relationships with existing policies

## 1. Scope of the policy

1.1 This policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.

1.2 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

1.3 A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the County Archives Service.

## 2. Responsibilities

2.1 The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Head of the school.

2.2 The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

2.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

## 3. Relationship with existing policies

This policy has been drawn up within the context of:

• Freedom of Information policy

• Data Protection policy

and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school.

**The purpose of the retention guidelines**

Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule listing the record series which the school creates in the course of its business. The retention schedule lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use. The retention schedule lays down the basis for normal processing under both the Data Protection Act 1998 and the Freedom of Information Act 2000.

Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

The retention schedule refers to record series regardless of the media in which they are stored.

**Using the Retention Schedule**

The Retention Schedule is divided into thirteen sections:

6.1 Governors

6.2 Management

6.3 Pupils

6.4 Curriculum

6.5 Personnel

6.6 Health and Safety

6.7 Administrative

6.8 Finance

6.9 Property

6.10 LEA

6.11 DfES

6.12 Connexions

6.13 School Meals

| Governors | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Minutes | | | | | |
| *Principal set (signed)* | No | | Permanent | Retain in school for 6 years from date of meeting | Transfer to Archives |
| *Inspection copies* | No | | Date of meeting + 3 years | DESTROY [If these minutes contain any sensitive personal information they should be shredded] | |
| Agendas | No | | Date of meeting | DESTROY | |
| Reports | No | | Date of report + 6 years | Retain in school for 6 years from date of meeting | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| Annual Parents' meeting papers | No | | Date of meeting + 6 years | Retain in school for 6 years from date of meeting | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| Instruments of Government | No | | Permanent | Retain in school whilst school is open | Transfer to Archives when the school has closed |

| Governors | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Trusts and Endowments | No | | Permanent | Retain in school whilst operationally required | Transfer to Archives |
| Action Plans | No | | Date of action plan + 3 years | DESTROY | It may be appropriate to offer to the Archives for a sample to be taken if the school has been through a difficult period |
| Policy documents | No | | Expiry of policy | Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process) | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| Complaints files | Yes | | Date of resolution of complaint + 6 years | Retain in school for the first six years Review for further retention in the case of contentious disputes Destroy routine complaints | |

| 1 Governors | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Annual Reports required by the Department for Education and Skills | No | Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171 | Date of report + 10 years | | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| Proposals for schools to become, or be established as Specialist Status schools | No | | Current year + 3 years | | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |

| 2 Management | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Log Books | Yes5 | | Date of last entry in the book + 6 years | Retain in the school for 6 years from the date of the last entry. | Transfer to the Archives |

5 From January 1st 2005 subject access is permitted into unstructured filing systems and log books and other records created within the school containing details about the activities of individual pupils and members of staff will become subject to the Data Protection Act 1998.

| 2 | Management | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Minutes of the Senior Management Team and other internal administrative bodies | Yes[1] | | Date of meeting + 5 years | Retain in the school for 5 years from meeting | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| Reports made by the head teacher or the management team | Yes[1] | | Date of report + 3 years | Retain in the school for 3 years from meeting | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities | Yes[1] | | Closure of file + 6 years | DESTROY If these records contain sensitive information they should be shredded | |
| Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities | No | | Date of correspondence + 3 years | DESTROY If these records contain sensitive information they should be shredded | |
| Professional development plans | Yes | | Closure + 6 years | SHRED | |
| School development plans | No | | Closure + 6 years | Review | Offer to the Archives |

| 3 Pupils | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Admission Registers | Yes | | Date of last entry in the book (or file) + 6 years | Retain in the school for 6 years from the date of the last entry. | Transfer to the Archives |
| Attendance registers | Yes | | Date of register + 3 years | DESTROY<br>[If these records are retained electronically any back up copies should be destroyed at the same time] | |
| Pupil record cards | Yes | | | | |
| *Primary* | | | Retain for the time which the pupil remains at the primary school | Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service | |
| Pupil files | Yes | | | | |
| *Primary* | | | Retain for the time which the pupil remains at the primary school | Transfer to the secondary school (or other primary school) when the child leaves the school.<br>In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service | |

| 3 Pupils | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Special Educational Needs files, reviews and Individual Education Plans | Yes | | DOB of the pupil + 25 year6 | SHRED | |
| Letters authorising absence | No | | Date of absence + 2 years | SHRED | |
| Absence books | | | Current year + 6 years | SHRED | |
| Examination results | Yes | | | | |
| *Public* | No | | Year of examinations + 6 years | DESTROY | Any certificates left unclaimed should be returned to the appropriate Examination Board |
| *Internal examination results* | Yes | | Current year + 5 years7 | DESTROY | |
| Any other records created in the course of contact with pupils | Yes/No | | Current year + 3 years | Review at the end of 3 years and either allocate a further retention period or DESTROY | |
| EHCP maintained under The Education Act 1996 - Section 324 | Yes | Special Educational Needs and Disability Act 2001 Section 1 | DOB + 30 years | DESTROY unless legal action is pending | |

6 As above

7 If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary.

**3 Pupils**

| Basic file description | Data Prot Issues | Statutory Provisions | Retention Period [operational] | Action at the end of the administrative life of the record | |
|---|---|---|---|---|---|
| Proposed EHCP or amended EHCP | Yes | Special Educational Needs and Disability Act 2001 Section 1 | DOB + 30 years | DESTROY unless legal action is pending | |
| Advice and information to parents regarding educational needs | Yes | Special Educational Needs and Disability Act 2001 Section 2 | Closure + 12 years | DESTROY unless legal action is pending | |
| Accessibility Strategy | Yes | Special Educational Needs and Disability Act 2001 Section 14 | Closure + 12 years | DESTROY unless legal action is pending | |
| Children SEN Files | Yes | | Closure + 35 years | DESTROY unless legal action is pending | |

**4 Curriculum**

| Basic file description | Data Prot Issues | Statutory Provisions | Retention Period [operational] | Action at the end of the administrative life of the record | |
|---|---|---|---|---|---|
| Curriculum development | No | | Current year + 6 years | DESTROY | |
| Curriculum returns | No | | Current year + 3 years | DESTROY | |
| School syllabus | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY | |

| 4 Curriculum | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Schemes of work | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY | |
| Timetable | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY | |
| Class record books | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY | |
| Mark Books | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY | |
| Record of homework set | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY | |
| Pupils' work | No | | Current year + 1 year | It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY | |
| Examination results | Yes | | Current year + 6 years | DESTROY<br>[These records should be shredded] | |
| SATS records | Yes | | Current year + 6 years | DESTROY<br>[These records should be shredded] | |
| ASP reports | Yes | | Current year + 6 years | DESTROY<br>[These records should be shredded] | |

| 4 Curriculum | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Value added records | Yes | | Current year + 6 years | DESTROY [These records should be shredded] | |

**6.5 Personnel**

| Basic file description | Data Prot Issues | Statutory Provisions | Retention Period [operational] | Action at the end of t |
|---|---|---|---|---|
| Timesheets, sick pay | Yes | Financial Regulations | Current year + 6 years | SHRED |
| Staff Personal files | Yes8 | | Termination + 7 years | SHRED |
| Interview notes and recruitment records | Yes | | Date of interview + 6 months | SHRED |
| Pre-employment vetting information (including CRB checks) | No | CRB guidelines | Date of check + 6 months | SHRED<br>[by the designates mer |
| Disciplinary proceedings: | Yes | | **Please note that all these retention periods w**<br>**may change in light of any recommendation** | |
| *Oral warning* | | | Date of warning + 6 months | SHRED<br>If this is placed on a pe<br>must be weeded from t |
| *written warning – level one* | | | Date of warning + 6 months | SHRED<br>If this is placed on a pe<br>must be weeded from t |
| *written warning – level two* | | | Date of warning + 12 months | SHRED<br>If this is placed on a pe<br>must be weeded from t |
| *final warning* | | | Date of warning + 18 months | SHRED<br>If this is placed on a pe<br>must be weeded from t |
| *case not found* | | | DESTROY immediately at the conclusion of the case | |
| Records relating to accident/injury at work | Yes | | Date of incident + 12 years | Review at the end of th<br>the case of serious acc<br>further retention period<br>be applied |
| Annual appraisal/assessment records | No | | Current year + 5 years | SHRED |
| Salary cards | Yes | | Last date of employment + 85 years | SHRED |

8 These files should be subject to KCC's open file policy where the employees are employed by RECORDS MANAGEMENT SOCIETY OF GREAT BRITAIN as the Local Education Authority.

**6.5 Personnel**

| Basic file description | Data Prot Issues | Statutory Provisions | Retention Period [operational] | Action at the end of t |
|---|---|---|---|---|
| Maternity pay records | Yes | Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567) | Current year, +3yrs | SHRED |
| Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995 | Yes | | Current year + 6 years | SHRED |

| 6.6 Health and Safety | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Accessibility Plans | | Disability Discrimination Act | Current year + 6 years | DESTROY | |
| Accident Reporting | | Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980 | | | |
| *Adults* | Yes | | Current year + 3 years | SHRED | |
| *Children* | Yes | | DOB + 25 years9 | SHRED | |
| COSHH | | | Current year + 10 years | Review [where appropriate an additional retention period may be allocated] | |
| Incident reports | Yes | | Current year + 20 years | SHRED | |
| Policy Statements | | | Date of expiry + 1 year | DESTROY | |
| Risk Assessments | | | Current year + 3 years | DESTROY | |

9 A child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the pupil reaches the age of 25 this retention period has been applied.

| 6.6 Health and Safety | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Process of monitoring of areas where employees and persons are likely to have come in contact with **asbestos** | | | Last action + 40 years | DESTROY | |
| Process of monitoring of areas where employees and persons are likely to have come in contact with **radiation** | | | Last action + 50 years | DESTROY | |
| Fire Precautions log books | | | Current year + 6 years | DESTROY | |

| 6.7 Administrative | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Employer's Liability certificate | | | Permanent whilst the school is open | DESTROY once the school has closed | |
| Inventories of equipment and furniture | | | Current year + 6 years | DESTROY | |
| General file series | | | Current year + 5 years | Review to see whether a further retention period is required | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| School brochure/prospectus | | | Current year + 3 years | | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| Circulars (staff/parents/pupils) | | | Current year + 1 year | DESTROY | |
| Newsletters, ephemera | | | Current year + 1 year | Review to see whether a further retention period is required | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |

| 6.7 Administrative | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Visitors' book | | | Current year + 2 years | Review to see whether a further retention period is required | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| PTA/Old Pupils' Associations | | | Current year + 6 years | Review to see whether a further retention period is required | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |

| 6.8 Finance | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Annual Accounts | | Financial Regulations | Current year + 6 years | | Offer to the Archives |
| Loans and grants | | Financial Regulations | Date of last payment on loan + 12 years | Review to see whether a further retention period is required | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| Contracts | | | | | |
| under seal | | | Contract completion date + 12 years | SHRED | |

| 6.8 Finance | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| under signature | | | Contract completion date + 6 years | SHRED | |
| monitoring records | | | Current year + 2 years | SHRED | |
| Copy orders | | | Current year + 2 years | SHRED | |
| Budget reports, budget monitoring etc | | | Current year + 3 years | SHRED | |
| Invoice, receipts and other records covered by the Financial Regulations | | Financial Regulations | Current year + 6 years | SHRED | |
| Annual Budget and background papers | | | Current year + 6 years | SHRED | |
| Order books and requisitions | | | Current year + 6 years | SHRED | |
| Delivery Documentation | | | Current year + 6 years | SHRED | |
| Debtors' Records | | Limitation Act 1980 | Current year + 6 years | SHRED | |
| School Fund – Cheque books | | | Current year + 3 years | SHRED | |
| School Fund – Paying in books | | | Current year + 6 years | SHRED | |
| School Fund – Ledger | | | Current year + 6 years | SHRED | |
| School Fund – Invoices | | | Current year + 6 years | SHRED | |
| School Fund – Receipts | | | Current year + 6 years | SHRED | |
| School Fund – Bank statements | | | Current year + 6 years | SHRED | |
| School Fund – School Journey books | | | Current year + 6 years | SHRED | |

| 6.8 Finance | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Applications for free school meals, travel, uniforms etc | | | Whilst child at school | SHRED | |
| Student grant applications | | | Current year + 3 years | SHRED | |
| Free school meals registers | Yes | Financial Regulations | Current year + 6 years | SHRED | |
| Petty cash books | | Financial Regulations | Current year + 6 years | SHRED | |

| 6.9 Property | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Title Deeds | | | Permanent | These should follow the property | Offer to Archives |
| Plans | | | Permanent | Retain in school whilst operational then | Offer to Archives |
| Maintenance and contractors | | Financial Regulations | Current year + 6 years | DESTROY | |
| Leases | | | Expiry of lease + 6 years | DESTROY | |
| Lettings | | | Current year + 3 years | DESTROY | |
| Burglary, theft and vandalism report forms | | | Current year + 6 years | SHRED | |
| Maintenance log books | | | Last entry + 10 years | DESTROY | |
| Contractors' Reports | | | Current year + 6 years | DESTROY | |

**6.10 LEA**

| Basic file description | Data Prot Issues | Statutory Provisions | Retention Period [operational] | Action at the end of the administrative life of the record | |
|---|---|---|---|---|---|
| Secondary transfer sheets (Primary) | Yes | | Current year + 2 years | SHRED | |
| Attendance returns | Yes | | Current year + 1 year | DESTROY | |
| Circulars from LEA | | | Whilst operationally required | Review to see whether a further retention period is required | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |

**6.11 DfES**

| Basic file description | Data Prot Issues | Statutory Provisions | Retention Period [operational] | Action at the end of the administrative life of the record | |
|---|---|---|---|---|---|
| HMI reports | | | These do not need to be kept any longer | | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| OFSTED reports and papers | | | Replace former report with any new inspection report | Review to see whether a further retention period is required | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |
| Returns | | | Current year + 6 years | DESTROY | |

| 6.11 DfES | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Circulars from DfES | | | Whilst operationally required | Review to see whether a further retention period is required | Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation] |

| 6.12 Connexions | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Service level agreements | | | Until superseded | SHRED | |
| Work Experience agreement | | | DOB of child + 18 years | SHRED | |

| **6.13School Meals** | | | | | |
|---|---|---|---|---|---|
| **Basic file description** | **Data Prot Issues** | **Statutory Provisions** | **Retention Period [operational]** | **Action at the end of the administrative life of the record** | |
| Dinner Register | | | Current year + 3 years | SHRED | |
| School Meals Summary Sheets | | | Current year + 3 years | SHRED | |

**Appendix 6**

# Hunsdon JMI Data Security Policy

Policy statement and objectives

1.1 The objectives of this Data Security Policy are to ensure that Hunsdon JMI 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.

1.2 The School is a Community school and is the Data Controller for all the Personal Data controlled/processed by the School.

1.3 The purpose of this policy is to inform staff about their specific responsibilities in maintaining and improving security standards and data management, through their working practices and day-to-day interaction with the Hunsdon JMI's ICT systems.

1.4 We hold personal data on pupils, staff and others to allow the Hunsdon JMI to conduct its day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can also result in media coverage and potentially damage the reputation of the Hunsdon JMI, its staff and pupils. Therefore everybody has a shared responsibility to be mindful about data security when they are going about their daily activities and consider how data security risks and threats can be minimised.

1.5 The policy applies to all staff of the Hunsdon JMI whether temporarily or permanently employed. It also applies to contractors engaged by/working with the Hunsdon JMI or who have access to information held by the Hunsdon JMI.

1.6 The Hunsdon JMI should ensure all staff are aware of and understand the content of this policy. If any staff member is found to have breached this policy, they could be subject to the Disciplinary and Dismissal Policy & Procedure.

1.7 The policy applies to all locations from which the Hunsdon JMI systems are accessed by staff including remote use and the use of portable devices.

## 2 Status of the policy

2.1 This policy has been approved by the Governing Body of the School. It sets out our rules on data security and the legal conditions that must be satisfied in relation to the secure handling, processing, storage, transportation and destruction of personal information.

## 3 Network/Server Security

3.1 Servers should be physically located in an access-controlled environment. Unrestricted access to the computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment. Restricted access may be given to other staff or third party support where there is a specific job function need for such access.

3.2 The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

3.3 Servers should have security software (Anti-Virus and Anti-Spyware) installed appropriate to the machine's specification.

3.4 Servers should always be password protected, and locked when not in use.

3.5 Security-related events should be reported to the IT team and to the DPO. Corrective measures will be prescribed as needed. Security-related events could include, but are not limited to, port-scan attacks, evidence of unauthorised access to privileged accounts.

3.6 IT infrastructure such as routers, switches, wireless access points etc. should be kept securely and only be handled by authorised personnel.

3.7 Backup Procedures:

3.7.1 Backup software must be scheduled to run routinely, as required, to capture all data as required.

3.7.2 Backups should be monitored to make sure they are successful.

3.7.3 A test restoration process will be run regularly.

3.7.4 Backup media must be securely stored in a fireproof container.

3.7.5 Any backup media stored off-site must be transported and stored securely.

## 4 Workstation Security

4.1 Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information is restricted to authorised users, including:

4.1.1 Restricting physical access to workstations to only authorised personnel.

4.1.2 Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorised access.

4.1.3 Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.

4.1.4 Complying with all applicable password policies and procedures.

4.1.5 Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.

4.1.6 Ensuring workstations are used for authorised purposes only.

4.1.7 Never installing unauthorised software on workstations.

4.1.8 Storing all confidential information on network servers.

4.1.9 Keeping food and drink away from workstations in order to avoid accidental spills.

4.1.10 Complying with the Anti-Virus policy.

## 5 Password Security

5.1 Requirements:

5.1.1 All system-level passwords (Administrator, etc.) must be changed on a quarterly basis, as a minimum.

5.1.2 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.

5.1.3 All user-level and system-level passwords must conform to the standards described below.

5.2 Standards - All users should be aware of how to select strong passwords. Strong passwords have the following characteristics:

5.2.1 Contain at least three of the five following character classes: Lower case characters; Upper case characters; Numbers; Punctuation; “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/).

5.2.2 Contain at least eight to fifteen alphanumeric characters.

5.2.3 The password is NOT a word found in a dictionary (English or foreign).

5.2.4 The password is NOT a name or common pattern (e.g. 12345678).

5.2.5 Passwords should be easily remembered. One way to do this is create a password based on a song title or other phrase.

5.3 Protective Measures

5.3.1 Do not share passwords with anyone. All passwords are to be treated as sensitive, confidential information.

5.3.2 Passwords should never be written down, unless securely stored, or stored electronically without encryption.

5.3.3 Do not reveal a password in email, chat, or other electronic communication.

5.3.4 Do not speak about a password in front of others.

5.3.5 Always decline the use of the “Remember Password” feature of applications.

## 6 Access Control

6.1 Staff should only access systems for which they are authorised. Under the Computer Misuse Act 1990 it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation.

6.2 All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

6.3 Formal procedures will be used to control access to systems. An authorised manager must request each application for access and access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Staff with management responsibilities must ensure they advise IT of any changes requiring such modification/removal.

6.4 Staff should pay particular attention to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals and documentation.

6.5 Line managers should ensure that all PC files of continuing interest to the business of the Hunsdon JMI are transferred to another user before a staff member leaves their employment. It is also good practice for a meeting to be held during which the manager notes all the systems to which the member of staff had access and informs the relevant system administrators of the leaving date. Particular attention needs to be taken when access to personal, commercially sensitive or financial data is involved.

6.6 Any contractors (working on site or working remotely via a communications link) to maintain or support computing equipment and software for the Hunsdon JMI must comply with the terms of this policy and any access control measures with which they are requested to comply with by Hunsdon JMI staff.

6.7 Physical security to all office areas should be maintained. Staff should feel confident about challenging strangers in the office areas without an ID badge.

6.8 Clear Desk Policy:

6.8.1 Staff are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into desk drawers and cupboards as appropriate.

6.8.2 Although security measures are in place to ensure only authorised access to office areas, staff members should ensure that documents, particularly of a confidential nature are not left lying around.

## 7 Security of Portable Equipment and Mobile Devices

7.1 Staff using portable computers/laptops must have appropriate access protection, for example passwords and encryption.

7.2 Devices must not be left unattended in public places or left in unattended vehicles at any time. Staff are also responsible for the security of the hardware and the information it holds at all times on or off Hunsdon JMI property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly

7.3 Staff should always secure laptops, handheld equipment and any removable media when leaving an office unattended and lock equipment away when leaving the office.

7.4 Staff working from home must ensure appropriate security is in place to protect equipment or information not be used by non-Hunsdon JMI staff. This will include ensuring equipment and information is kept out of sight.

7.5 Staff should ensure that any machine not routinely connected to the school network, is brought in regularly to receive updates by the IT team.

7.6 Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop and should synchronise all locally stored data with the Hunsdon JMI network server on a frequent basis.

7.7 Mobile Computing and Storage Devices include, but are not limited to: laptop computers, plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, smartphones, tablets, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or

Hunsdon JMI owned, that may connect to or access the information systems at the Hunsdon JMI. These devices are easily lost or stolen, presenting a high risk for unauthorised access and introduction of malicious software to the IT network. These risks must be mitigated to acceptable levels:

7.7.1 Encryption - portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive information must use encryption or equally strong measures to protect the data while it is being stored.

7.7.2 Database or portions thereof, which reside on the network shall not be downloaded to mobile computing or storage devices.

7.7.3 Report lost or stolen mobile computing and storage devices immediately to the IT department and/or the DPO.

7.7.4 Non-departmental owned device that may connect to the Hunsdon JMI network must first be approved by the IT department.

## 8 Acceptable Use

8.1 While the Hunsdon JMI's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the systems remains the property of the Hunsdon JMI.

8.2 Staff must pay particular attention to the protection of personal data and commercially sensitive data. All sensitive files must be password protected or encrypted where possible.

8.3 For security and network maintenance purposes, authorised individuals within the Hunsdon JMI may monitor equipment, systems and network traffic at any time.

8.4 Authorised staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If staff are in doubt as to whether the individual requesting such access is authorised to do so, they should ask for their identification badge and contact their department. Any authorised staff member will be happy to comply with this request.

8.5 Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Hunsdon JMI business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of the ICT systems; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

8.6 Authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

8.7 All monitoring, surveillance or investigative activities are conducted by authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2018 (RIPA) and the Lawful Business Practice Regulations 2000.

8.8 Please note that personal communications using Hunsdon JMI ICT systems may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

8.9 Staff must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

8.10 If it is suspected that there may be a virus on any Hunsdon JMI ICT equipment, staff should stop using the equipment and contact the IT team immediately. They will advise what actions to take and be responsible for advising others that need to know.

8.11 It is imperative that staff do not access, load, store, post or send from Hunsdon JMI ICT system any material that is, or may be considered to be: illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the Hunsdon JMI or may bring the Hunsdon JMI into disrepute. This includes, but is not limited to: jokes, chain letters, files, emails, clips or images that are not part of the Hunsdon JMI's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

8.12 Any information held on Hunsdon JMI systems, hardware or used in relation to Hunsdon JMI business may be subject to The Freedom of Information Act or a Subject Access Request.

8.13 Where necessary, permission should be obtained from the owner or owning authority and any relevant fees paid before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

## 9 Printing, Copying and Transmission of Data

9.1 It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents emailed, faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used.

9.2 Anyone sending a confidential or sensitive fax should notify the recipient before it is sent.

9.3 Staff should ensure that the entire document has copied or printed and check that the copier has not run out of paper. This is particularly important when copying or printing large documents.

9.4 Staff should not leave the printer unattended when using it, as another person may pick up the printing by mistake.

9.5 When sending data, the most secure method of transmission must be selected, especially where information is particularly sensitive or confidential. All staff should consider the risk of harm or distress that could be caused to the relevant Data Subject if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.

9.6 Send only the minimum amount of personal or sensitive information, by whichever method is chosen.

9.7 Sending information by email:

9.7.1 Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes.

9.7.2 If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list.

9.7.3 Take care when replying 'to all' – do they really all need to receive the information being sent.

9.7.4 If emailing sensitive information, password protect any attachments. Use a separate email or different method to communicate the password e.g. telephone call.

9.7.5 When sending sensitive files, consider the use of secure file transfer systems where available, such as Schoolsfx or HertsFX (Hertfordshire schools).

9.8 Sending information by post:

9.8.1 Check that the address is correct.

9.8.2 Ensure only the relevant information is in the envelope and that someone else's letter has not been included in error.

9.8.3 Consider using tracking, e.g. recorded delivery or a courier if appropriate.

**10 Use of Email**

10.1 The Hunsdon JMI gives all staff and governors their own email account to use for all Hunsdon JMI business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and to avoid the risk of personal profile information being revealed.

10.2 Staff and governors should use their school email for all professional communication.

10.3 Monitoring – Hunsdon JMI employees shall have no expectation of privacy in anything they store, send or receive on the Hunsdon JMI email system. The Hunsdon JMI may monitor messages without prior notice.

10.4 It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced.

10.5 Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

10.6 All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

10.7 Staff should avoid sending or forwarding attachments unnecessarily. Whenever possible, the location path to the file on a shared drive should be sent instead.

10.8 Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated line manager.

10.9 When emailing confidential/personal data, obtain express consent from a manager to provide the information by email and exercise caution when sending by performing the following checks:

10.9.1 Encrypt and/or password protect attachments. Provide the encryption key or password by a separate contact with the recipient(s).

10.9.2 Verify the details, including accurate email address, of any intended recipient of the information. Do not copy or forward the email to any more recipients than is absolutely necessary.

10.9.3 Verify the details of a requestor before responding to email requests for information.

10.9.4 Consider using other secure file transfer methods, such as HertsFX or Schoolsfx (Hertfordshire schools).

10.9.5 Request confirmation of safe receipt.

10.10 The Hunsdon JMI email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Hunsdon JMI employee should report the matter immediately. The following activities are strictly prohibited, with no exceptions:

10.10.1 Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).

10.10.2 Any form of harassment via email, telephone or messaging, whether through language, frequency, or size of messages.

10.10.3 Creating or forwarding “chain letters”, “joke” emails, or “pyramid” schemes of any type.

10.11 Users should actively manage their email account by:

10.11.1 Checking emails regularly.

10.11.2 Deleting all emails of short-term value.

10.11.3 Organising email into folders and carrying out frequent house-keeping on all folders and archives.

10.11.4 Activating an out-of-office notification when away for extended periods.

10.12 Personal Use - using a reasonable amount of Hunsdon JMI resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email.

10.13 The Hunsdon JMI email account should not be used for personal advertising.

10.14 All the above apply whether accessing the Hunsdon JMI email account onsite, or through webmail or on non-Hunsdon JMI devices.

## 11 Data Breaches

11.1 The Information Commissioner's Office (ICO) has the power to serve notices requiring organisations to pay up to €20 million or 4% of annual global turnover, whichever is higher, for serious breaches of the GDPR and Data Protection Act 2018.

11.2 Staff are responsible for:

11.2.1 Ensuring that no breaches of information security result from their actions.

11.2.2 Reporting any breach, or suspected breach of security without delay.

11.2.3 Ensuring information they have access to remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from its loss.

11.2.4 Ensuring they are aware of and comply with any restrictions specific to their role or service area. All staff should be aware of the confidentiality clauses in their contract of employment.

11.3 Advice and guidance on information security can be provided by the Hunsdon JMI DPO and/or Data Protection Lead.

11.4 A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of Hunsdon JMI ICT hardware, software or services from the offending individual.

11.5 For staff any policy breach is grounds for disciplinary action in accordance with the Hunsdon JMI Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated. Policy breaches may also lead to criminal or civil proceedings.

11.6 If a member of staff or governor knows or suspects that a Personal Data Breach has occurred, then the actions in the Data Breach Response Plan (Appendix 7) must be followed. In particular, the DPO or such other person identified in the Data Breach Response Plan must be notified immediately.

11.7 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person.

## 12 Disposal of Redundant ICT Equipment Policy

12.1 All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

12.2 All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. The Hunsdon JMI will only use authorised companies who will supply a written guarantee that this will happen.

12.3 Disposal of any ICT equipment will conform to: the Waste Electrical and Electronic Equipment Regulations 2018, the Data Protection Act 2018, the Electricity at Work Regulations 1989.

12.4 The Hunsdon JMI will maintain a comprehensive inventory of all its ICT equipment including a record of disposal. This will include:

12.4.1 Date item disposed of.

12.4.2 Authorisation for disposal, including: verification of software licensing, any personal data likely to be held on the storage media.

12.4.3 How it was disposed of e.g. waste, gift, sale.

12.4.4 Name of person and/or organisation who received the disposed item.

12.5 Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

## 13 Policy Review

13.1 It is the responsibility of the Governing Body to facilitate the review of this policy on a regular basis, and at least every 2 years or if any new technologies are introduced. Recommendations for any amendments should be reported to the DPO.

13.2 The Hunsdon JMI will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

## 14 Enquiries

14.1 Further information can be found in the Online Safety policy and the Data Protection Policy

**Appendix 7**

# Hunsdon JMI Data Breach Response Plan

**Data Breach Response Plan for Hunsdon JMI School**

## 1 Introduction

1.1 Hunsdon JMI School has implemented appropriate technical and organisations measures to avoid data security breaches. However, in the event that a data security breach happens, we recognise that is important that the [School / Trust] is able to detect it and react swiftly and robustly in order to mitigate any risks to Data Subjects and to comply with our obligations under the General Data Protection Regulation ('GDPR').

1.2 This Data Breach Response Plan sets out how we will respond to any suspected or actual data breaches and should be read alongside our [Data Protection Policy] [Information Security Policy] [LIST ANY OTHER RELEVANT POLICIES].

1.3 The procedures set out in this document are particularly important as, prior to the GDPR, there was no obligation on the [School / Trust] to notify the Information Commissioner's Office ('ICO') of data security breaches, although it was good practice to report serious breaches.

1.4 The GDPR requires the school to report 'notifiable breaches' without undue delay and, where feasible, not later than 72 hours after having become aware of it. Notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals. In the event that a report is not made within 72 hours, the [School / Trust] is required to provide the reasons for the delay in reporting it to the ICO.

1.5 If there is deemed to be a "high risk" to the rights and freedoms of individuals following a data breach, the school is also required to notify the individuals affected by the breach. However, in the interests of transparency, the school recognise that on some occasions it will be appropriate to notify affected individuals, even if we are not legally obliged to do so.

1.6 If the school fails to report a notifiable personal data breach, we are at risk of receiving a sanction from the ICO, which may include a fine. Aside from our desire to avoid receiving any sanctions, the purpose of this Data Breach Response Plan is to ensure that we protect the Personal Data of our stakeholders and minimise any risks to them following a breach.

1.7 The school will ensure that staff are aware of and are trained on this Data Breach Response Plan to ensure it is effective should a data security incident occur. In particular, the [Data Response Team] identified below, must receive training on their roles and responsibilities should a breach occur. For example, our external IT support must be trained on how to identify if the security of our IT systems have been compromised and the steps that need to be taken to respond to a breach, for example, if data on a remote device needs to be wiped. Further details of our security procedures are set out in our Data Security Policy.

1.8 We rely on our staff to be alert to the risk of data security breaches and to follow the procedures set out in this Data Breach Response Plan to ensure that we can react promptly in the event that a breach or suspected breach occurs. Any member of staff who becomes aware of a suspected or actual personal data breach must follow the escalation procedures set out below. Failure to comply with these procedures may be a disciplinary issue.

1.9 The school's DPO is Mr Mike Newman dpo@hunsdon.herts.sch.uk.

## 2 What is a personal data breach?

2.1 The legal definition of a personal data breach is, “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.”

2.1.1 A data security breach covers more than the simple misappropriation of data and may occur through incidents, such as:

2.1.2 Loss or theft of data or equipment;

2.1.3 People gaining inappropriate access to personal data;

2.1.4 A deliberate attack on systems;

2.1.5 Equipment failure;

2.1.6 Human error;

2.1.7 Acts of God (for example, fire or flood);

2.1.8 Malicious acts such as hacking, viruses or deception.

2.2 Breaches can be categorised according to the following three well-known information security principles:

2.2.1 “Confidentiality breach” - where there is an unauthorised or accidental disclosure of, or access to, personal data;

2.2.2 “Integrity breach” - where there is an unauthorised or accidental alteration of personal data;

2.2.3 “Availability breach” - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

2.3 Depending on the circumstances, a breach can relate to the confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

2.4 A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

2.5 A security incident resulting in personal data being made unavailable for temporary period is also a type of breach, as the lack of access to the data could have a significant impact on the rights and freedoms of Data Subjects, for example, if our IT system goes down. This type of breach should be recorded in the school’s Data Breach Log set out in Appendix 1 so that we keep records of all such incidents. However, depending on the circumstances of the breach, it may or may not require notification to the ICO and communication to affected individuals.

2.6 Where personal data is unavailable due to planned system maintenance being carried out, this should not be regarded as a ‘breach of security’.

## 3 Understanding the risk to the rights and freedoms of individuals

3.1 A breach can potentially have a number of consequences for individuals, which can result in physical, material, or non-material damage. This can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals.

3.2 When assessing the risk to individuals, the DPO must consider the following factors:

3.2.1 the type of breach;

3.2.2 the nature, sensitivity, and volume of personal data;

3.2.3 ease of identification of individuals;

3.2.4 severity of consequences for individuals;

3.2.5 special characteristics of the individual;

3.2.6 special characteristics of the data controller; and

3.2.7 the number of affected individuals.

## 4 Timescales for reporting a breach

4.1 The school is required to report a notifiable breach without undue delay and, where feasible, not later than 72 hours after having become aware of it.

4.2 It is likely that the school will be deemed as having become “aware” of a breach when we have a reasonable degree of certainty that a security incident has occurred which has led to personal data being compromised. The GDPR expects us to ascertain whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place. This puts an obligation on us to ensure that we will be “aware” of any breaches in a timely manner so that we can take appropriate action.

4.3 While some breaches may be obvious, in other cases we may need to establish whether personal data has been compromised. In such circumstances, we will investigate promptly in accordance with the procedures below to determine whether a breach has happened which, in turn, will enable us to decide if remedial action is needed and if the breach needs to be notified to the ICO and the affected Data Subjects.

4.4 It is possible that we may not have established all of the relevant facts following a data security breach or completed our investigation within 72 hours. However, in the event that the school determines that a breach has taken place and that it needs to be notified to the ICO, a report should be made within 72 hours with the information held at that point in time. In these circumstances, the report to the ICO should explain that further information will be provided as and when it is available.

4.5 It is possible that some breaches may come to the attention of a member of staff or may be flagged up by our IT systems. However, it is also possible that we may be notified about breaches by third parties, such as the people who are affected by the breach, a data processor or by the media.

4.6 In the event that we investigate a suspected breach and we are able to establish that no actual breach has occurred, the Data Breach Log in Appendix 1 must still be completed

so that we can keep records of 'near misses' or other weaknesses in our systems and procedures in order to continuously review and improve our processes.

## 5 Response Plan

5.1 A member of staff within the school who becomes aware of a suspected or actual data security breach must inform the DPO by email without delay. The email address for contacting the DPO is dpo@hunsdon.herts.sch.uk and the email account should be regularly reviewed by the DPO. The Headteacher of the school should be copied in to the email to the DPO

5.2 If a member of staff is unsure if a breach has happened, the above procedures must still be followed without delay so that the suspected breach can be investigated in order to establish whether a breach has happened and, if so, whether it needs to be notified to the ICO or the Data Subjects.

5.3 Once a breach or suspected breach has been reported to the DPO, the DPO must commence an investigation and assess whether he / she has sufficient information to identify next steps. The purpose of the investigation is to:

5.3.1 establish if a breach has happened;

5.3.2 establish the nature and cause of the breach;

5.3.3 establish the extent of the damage or harm that results or could result from the breach;

5.3.4 identify the action required to stop the data security breach from continuing or recurring; and

5.4 mitigate any risk of harm that may continue to result from the breach.

5.5 The DPO should contact the Headteacher if further information is required. The DPO may also need to speak to the member of staff who first reported the breach or suspected breach.

5.6 If the DPO is unavailable for any reason, for example, the DPO is on annual leave, on sickness absence or is otherwise not available to respond to the data breach, then the Headteacher must fulfil the responsibilities of the DPO set out in this Data Breach Response Plan. The Headteacher must have access to the email account identified above to which data breaches are reported.

5.7 The DPO should consider whether input is required from the school's IT and/or HR support in order to further investigate the incident, including the extent of the incident and whether any steps need to be taken to contain any breach.

5.8 Depending on the circumstances, the DPO should also consider legal advice is required and if the incident needs to be reported to the Police and the Local Authority. The DPO should also consider if specialist IT support is required in order to contain and manage a breach.

5.9 If the breach or suspected breach has occurred at one of our Data Processors, the DPO must liaise with the Data Processor to obtain as much information as possible about the extent of the breach or suspected breach and any steps being taken to mitigate any risk to Data Subjects. It remains the school's responsibility to decide whether to report any such breach to the ICO within 72 hours.

5.10 Depending on the timescales as to when a member of staff originally became aware of a breach, the DPO must be mindful of the requirement to notify the ICO without delay and within 72 hours unless it is unlikely to result in a risk to the rights and freedoms of individuals. As stated above, it is therefore possible that a data security breach may need to be reported to the ICO before the school has fully investigated or contained the breach. A report to the ICO must contain the following information:

5.10.1 the nature of the personal data breach including where possible, the categories and approximate number of Data Subjects concerned;

5.10.2 the name and contact details of the DPO or other contact point where more information can be obtained;

5.10.3 the likely consequences of the personal data breach;

5.10.4 the measures taken or proposed to be taken by the school to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

5.11 The DPO is not required to provide precise details in the report to the ICO if this information is not available and an updated report can be made as and when further details come to light. Such further information may be provided in phases without undue further delay. The DPO should inform the ICO if the school does not yet have all the required information and if further details will be provided later on.

5.12 If a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred, this information could then be added to the information already given to the ICO and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

5.13 In the event that a notifiable breach is not reported to the ICO within 72 hours, a report should be made without delay with the reasons for the delay.

5.14 If the DPO concludes that a referral to the ICO is required and also concludes that there is likely to be a high risk to the rights and freedoms of individuals resulting from the data security breach then the Data Subjects affected by the breach must also be notified without undue delay. The DPO must liaise with the Headteacher in relation to how the issue should be communicated to the relevant stakeholders. The DPO will need to consider which is the most appropriate way to notify affected Data Subjects, bearing in mind the security of the medium as well as the urgency of the situation. The notice to the affected individuals should contain the following information:

5.15 description of the nature of the breach;

5.16 the name and contact details of the DPO or other contact point;

5.17 a description of the likely consequences of the breach; and

5.18 a description of the measures taken or proposed to be taken by the school to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.19 Given that a large number of our stakeholders are children, if a data breach affects our pupils, it is likely that the above information will need to be given to parents.

5.20 If the DPO decides to notify Data Subjects about a breach, the notification should at the very least include a description of how and when the breach occurred and what data was involved. Details of what the organisation has already done to respond to the risks posed

by the breach should also be included. The school should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised.

5.21 The DPO must complete the Data Breach Log in Annex 1 before making the referral to the ICO and keep it under review as and when further information comes to light.

5.22 In certain circumstances, where justified, and on the advice of law-enforcement authorities, the school may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, Data Subjects would still need to be promptly informed after this time.

5.23 Even if the DPO initially decides not to communicate the breach to the affected Data Subjects, the ICO can require us to do so, if it considers the breach is likely to result in a high risk to individuals.

5.24 In the event that the DPO concludes that it is not necessary to refer the breach to the ICO, the DPO must still complete the Data Breach Log and clearly set out the reasons why the DPO is satisfied that a referral is not required. The DPO must keep the decision under review and be prepared to make a referral to the ICO if any circumstances change or if any information comes to light which means that a referral should be made.

5.25 Once the breach has been contained and action taken to stop or mitigate the breach, the DPO must then review the incident and identify any steps which need to be taken in order to prevent a similar breach occurring in future. This may also include whether any disciplinary action is required against any members of staff or pupils.

5.26 As part of the review process, the DPO should undertake an audit which should include a review of whether appropriate security policies and procedures were in place and if so, whether they were followed. The audit should include an assessment of any ongoing risks associated with the breach and evaluate the school's response to it and identify any improvements that can be made. The review should also consider the effectiveness of this Data Breach Response Plan and whether any amendments need to be made to it.

5.27 Where security is found not to be appropriate, the DPO should consider what action needs to be taken to raise data protection and security compliance standards and whether any staff training is required.

5.28 Where a data processor caused the breach, the DPO should consider whether adequate contractual obligations were in place to comply with the GDPR and if so, whether the data processor is in breach of contract.

## 6 School holidays

6.1 The school recognises that there are times throughout the year when our ability to identify and respond to a breach swiftly and robustly may be impeded because the school is closed during school holidays. A breach may still occur during these periods and we will implement the following steps to mitigate any risk caused if a breach happens during the school holidays:

6.2 The DPO's email address will be made available to staff and will be available on our website and in our privacy notices so that a member of staff can be contacted should an incident occur. This email address will be monitored regularly by the assigned member of staff.

6.3 The DPO will have the contact details for the Headteacher so that action can be taken without delay should a breach occur.

6.4 The DPO should follow the steps set out above as best as he / she can in the circumstances. In particular, this should include reporting notifiable breaches to the ICO within 72 hours and, if required, the affected individuals. The report to the ICO should state that the school is closed due to the school holidays and, depending on the circumstances, advice should be sought from the ICO on the steps the school should take to mitigate any risks.

## 7 Review

7.1 This Data Breach Response Plan will be kept under review by the DPO and may be revised to reflect good practice or changes to our organisational structure.

**Annex 1 – Data Breach Log for Hunsdon JMI School**

This Data Breach Log must be completed by a suitably trained person following any reports of a security breach or suspected breach involving personal data. Staff must follow theschool's Data Breach Response Plan following notification of a breach or suspected breach. In the event you are unsure whether to notify the ICO and the Data Subjects, you should obtain legal advice without delay as the ICO must be informed about notifiable breaches within 72 hours.

| Information | Response |
|---|---|
| **Date and time this record was completed** | |
| **Name of person completing this record** | |
| **General description of the breach** | |
| **Name and job title of person who originally reported the breach / suspected breach** | |
| **Date and time the breach / suspected breach was reported** | |
| **Who was the breach / suspected breach reported to?** | |
| **Has the Data Protection Officer been informed?** | |
| **Has the Data Breach Response Team been notified?** | |
| **What are the details of the breach / suspected breach (include as much detail as possible)**<br>**NB: An investigation must be undertaken where appropriate** | |

| Information | Response |
|---|---|
| **Who is responsible for the breach i.e. the school as data controller, a joint data controller or a data processor?** | |
| **Is the breach ongoing or has it been contained?** | |
| **Is any other information required in order to assess the extent of the breach / the risk to Data Subjects? If so, specify that information here.** | |
| **Whose data has / may have been compromised as a result of the breach / suspected breach?** | |
| **Type of data involved in the breach / suspected breach** | |
| **Does the breach / potential breach involve sensitive personal data[10] or information about criminal offences?** | |
| **What is the likely risk to individuals?** | |
| **Is there likely to be a high risk to individuals?** | |
| **Does the breach need to be reported to the ICO?**<br>**If yes, and if the breach happened more than 72 hours ago, what is the reason for the delay if notifying the ICO?** | |
| **If the breach has already been reported to the ICO, confirm the date and time the report was made, who made the report and whether the report was made within 72 hours** | |

10 Information about an individual's: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, sexual orientation.

| Information | Response |
|---|---|
| **If a report has been made to the ICO, what advice or recommended actions have been given?**<br><br>**Specify any sanctions that are issued by the ICO following a breach.** | |
| **If a report to the ICO is not being made, confirm the reasons why and whether the decision needs to be kept under review** | |
| **Do the Data Subjects affected need to be notified about the breach? If so, confirm who will notify them and how and when they will be notified.**<br><br>**If Data Subjects are not going to be informed, explain the reasons why.** | |
| **Does the breach need to be reported to the Police?** | |
| **Do any other steps need to be taken e.g. comms to stakeholders, provision of complaints policy, consult legal advisors, notify insurers, external IT support.** | |
| **Is there likely to be press / media interest as a result of the breach? If so, have the appropriate protocols for handling media enquires been followed?** | |

| Information | Response |
| --- | --- |
| **Outline the actions that need to be taken in response to the breach / suspected breach to reduce the risk of a re-occurrence and who is responsible for implementing them and the relevant timescales. This should include whether an investigation under the school's disciplinary policy is recommended.**<br><br>**NB: The information provided in response to this question is likely to be a summary as a more detailed report / audit is likely to be required following a data breach which is notified to the ICO.** | |

**Appendix 7**

# GDPR Contract Clauses

**Explanation for Schools / Academy Trusts**

Schools and Academy Trusts are Data Controllers for the purposes of the General Data Protection Regulation ("GDPR"). It is likely that Schools and Academy Trusts will enter into relationships with suppliers and service providers who are Data Processors. A Data Processor is "…*a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller*."

In summary, a Data Controller determines the purposes and means of processing personal data and a Data Processor is responsible for processing personal data on behalf of a controller.

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*."

This means that, for a School or Academy Trust, a Data Processor is likely to include (but is not limited to) the following:

- online third party software providers;
- outsourced HR;
- outsourced payroll;
- external clerks;
- external IT Contractors;
- confidential waste collection companies; and
- outsourced governance support.

The GDPR states that where a Data Processor processes Personal Data on behalf of a Data Controller, a written contract must be in place and the contract must contain certain clauses (which, for the purposes of this note will be described as the "GDPR clauses"). Article 28(1) of the GDPR requires the Controller to "use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements" of the GDPR". A contract is also needed when a processor, with the School or Academy Trust's written authority, employs another processor.

Under the GDPR, Data Controllers are required to have contracts in place with Data Processors to ensure there is appropriate security in place. In addition, a Data Processor can be legally liable and could be fined if they are responsible for a breach. The Data Controller also remains directly liable for compliance with all aspects of the GDPR, and for demonstrating that compliance. If this is not achieved then the School / Trust can be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures. The Information Commissioner's Office ("ICO") guidance states the following in relation to Data Controllers, "Unless you can prove that you were "not in any way responsible for the event giving rise to the damage", you will be fully liable for any damage caused by non-compliant processing, regardless of your use of a processor."

The purpose of the GDPR clauses is to ensure that Data Processors have taken appropriate steps to keep Personal Data secure and that swift action can be taken if a Data Processor becomes aware of a data security breach.

In the future, standard contract clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However at the time of drafting no standard clauses have been drafted.

**Joint Data Controllers**

From time to time, a School or Academy Trust is likely to share data with joint Data Controllers, for example, statutory information that is shared with the Department for Education, Local Authority, legal advisors and, in the case of a Church school, the Diocese. An organisation is likely to be a Data Controller (i.e. not a Data Processor) if they can:

1. determine the purpose(s) for which and the manner in which the Data will be processed or used;
2. decide the legal basis for collecting data;
3. decide what Data to collect;
4. determine which individuals to collect Data about;
5. decide whether to disclose the Data, and if so, who to;
6. decide whether subject access and other individuals' rights apply including the application of any exemptions
7. decide how long to retain the Personal Data;
8. determine whether to make non-routine amendments to the Personal Data.

The 'GDPR clauses' do not need to be put in place if a School or Academy Trust shares information with joint Data Controllers but, depending on the circumstances, it may be good practice to enter into a Data Sharing Agreement to set out the respective roles and responsibilities of the Joint Controllers regarding the Data Subjects. If you are unsure if another organisation is a Data Processor or a joint Data Controller, you should seek legal advice.

**The practicalities of agreeing the GDPR clauses**

If a School or Academy Trust's contracts with a Data Processor do not already contain the GDPR clauses, the contract will need to be updated by 25 May 2018 to comply with the GDPR. Future contracts with Data Processors will also need to contain the GDPR clauses. Failure to do so may result in enforcement action being taken by the ICO. Further, if a data breach involving a Data Processor occurs and the GDPR clauses have not been put in place, this may increase the severity of any sanction applied to the School or Academy Trust and / or the Data Processor.

It is the School or Academy Trust's responsibility to ensure that the contract contains the GDPR clauses. In practice, some of the larger suppliers to schools may initiate the conversation with the School or Academy Trust and put forward their draft clauses. In other cases, the School or Academy Trust will need to take the initiative with their Data Processors to agree the contract wording by writing to suppliers notifying them of changes they intend to make to relevant contracts to bring them into line with the new data protection regulations.

It should not be necessary to re-negotiate the entire contract with the Data Processors as the GDPR clauses can be added as a contract addendum or a side letter which is signed by both parties but it will depend on the nature of the contract and what is appropriate in the circumstances.

It is possible that during the course of negotiations, a Data Processor may try to include wording in the clauses which attempts to push some or all of the financial risk for a breach back onto the School or Academy Trust, for example, by including an indemnity in favour of the Processor. The School or Academy Trust should resist such wording as Data Processors should consider taking out insurance to cover any such risk. The law has been extended directly to Processors to ensure better performance and enhanced protection for personal data, therefore a clause which attempts to remove the Data Processor's exposure to GDPR fines or court claims undermines these principles. A School or Trust should refer to their DPO and / or take legal advice before agreeing to any wording which they are unsure about.

Suppliers should also be expected to manage their own costs in relation to GDPR compliance and Schools and Academy Trusts should not routinely accept contract price increases from suppliers as a result of work associated with compliance with the GDPR.

Aside from agreeing the GDPR clauses, a School or Academy Trust should consider whether it has undertaken sufficient due diligence on its Data Processors. If not, Schools and Academy Trusts should conduct due diligence on existing contracts to ensure suppliers can implement the appropriate technical and organisational measures to comply with GDPR. It would also be good practice to implement a due diligence process as and when new contracts with Data Processors are entered into and to keep records to demonstrate that this has happened.

**Caution**

**The wording set out in Annex 1 is an example of wording that could be agreed as a contract addendum between a School or Academy Trust and a Data Processor and assumes that the Data Processor is based in the UK. Given the wide variety of contracts that Schools and Academy Trusts enter into, the wording must be tailored and amended according to the specific contract, the relevant circumstances, the type of personal data that is being processed and any specific processes in the contract for agreeing variations.**

**The clauses in Appendix 1 should not be relied on as legal advice to be applied to any particular set of circumstances and Schools and Academy Trusts should seek specific legal advice on the application of the clauses and on any specific issues which arise during the negotiation with the Data Processor if you are unsure about any aspect of their application.**

**Further, this explanatory note and the draft clauses are subject to the Data Protection Bill which was going through Parliament at the time of drafting, and further ICO guidance may be issued to reflect good practice between Data Controllers and Data Processors so Schools and Academy Trusts must keep the clauses under review.**

**March 2018**

**Annex 1 - EXAMPLE OF GDPR CLAUSES WITH DOCUMENT NOTES (DELETE FOOTNOTES FROM THE CLAUSES BEFORE USE)**

This addendum is entered into on [DATE11].

These Data Protection Clauses form part of the Agreement between Hunsdon JMI School (the ["School"] ["Trust"]) and [Name of Contractor] (the "Contractor")

The terms used in this contract addendum shall have the meanings set out below. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement. Except where the context requires otherwise, references in this addendum to the Agreement are to the Agreement as amended by, and including, this addendum.

**DEFINITIONS**

**Agreement:** means the contract for [ ] between [ ] and [ ] dated [ ]

**Contractor Personnel:** means all directors, officers, employees, temporary and agency workers, agents, consultants and contractors of the Contractor and/or of any Sub-Contractor engaged in the performance of its obligations under this Agreement

**Data Protection Clauses:** means the clauses set out below numbered [1.1] – [1.X]12 including the Schedule.

**Data Protection Legislation:** (i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation (*(EU) 2016/679*) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 2018.

**Data Protection Impact Assessment**: an assessment by the school of the impact of the envisaged processing on the protection of Personal Data.

**Data Protection Officer:** means theschool's Data Protection Officer whose contact details are [INSERT NAME AND EMAIL ADDRESS]

**Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Data Subject Access Request** take the meaning given in the Data Protection Legislation

**1. DATA PROTECTION CLAUSES**

1.1 Both parties will comply with all applicable requirements of the Data Protection Legislation. This clause [NUMBER] is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

1.2 The parties acknowledge that for the purposes of the Data Protection Legislation, the school is the data controller and the Contractor is the data processor (where **Data Controller** and **Data Processor** have the meanings as defined in the Data Protection Legislation). The Schedule13 sets out the scope, nature and purpose of processing by the Contractor, the duration of the processing and the types of personal data (as defined

11 Insert the date when the clauses have been agreed and you are ready to enter into a binding agreement with the data processor.
12 Amend as appropriate.
13 The Schedule must be completed with the relevant information relating to the contract

in the Data Protection Legislation, **Personal Data**) and categories of Data Subject. The only processing that the Contractor is authorised to do is listed in the Schedule by the school and may not be determined by the Contractor.

1.3 Without prejudice to the generality of clause 1.1, the school will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Contractor for the duration and purposes of this agreement.

1.4 Without prejudice to the generality of clause 1.1, the Contractor shall, in relation to any Personal Data processed in connection with the performance by the Contractor of its obligations under the Agreement:

1.4.1 process that Personal Data only on the written instructions of the school14 as set out in the Schedule unless the Contractor is required by law to process Personal Data (**Applicable Laws**). Where the Contractor is relying on an Applicable Law as the basis for processing Personal Data, the Contractor shall promptly notify the school of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Contractor from so notifying the school;

1.4.2 ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the school, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it15);

1.4.3 ensure that it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that:

1.4.3.1 appropriate pre-recruitment checks on any Contractor Personnel have been undertaken [including, where appropriate, Disclosure and Barring Service checks];

1.4.3.2 they are aware of and comply with the Contractor's duties under this clause;

1.4.3.3 they are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor, including a duty of confidence;

1.4.3.4 they are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the school or as otherwise permitted by these Data Protection Clauses; and

1.4.3.5 they have undergone adequate training in the use, care, protection and handling of Personal Data;

14 The instructions could be contained in the contract itself

15 Include any specific requirements the School / Trust may have.

1.4.4 not transfer any Personal Data outside of the European Economic Area unless the prior written consent of the school has been obtained and the following conditions are fulfilled:

1.4.4.1 the school or the Contractor has provided appropriate safeguards in relation to the transfer;

1.4.4.2 the Data Subject has enforceable rights and effective legal remedies;

1.4.4.3 the Contractor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

1.4.4.4 the Contractor complies with reasonable instructions notified to it in advance by the school with respect to the processing of the Personal Data;

1.4.5 at the written direction of the school, delete or return Personal Data and copies thereof to the school on termination of the agreement unless required by Applicable Law to store the Personal Data; and

1.4.6 maintain complete and accurate records and information to demonstrate its compliance with these Data Protection Clauses and the Data Protection Legislation and allow for audits by the school or the school's designated auditor provide the school with all the information that is needed to show that that the school and the Contractor have met the obligations set out in the Data Protection Legislation.

1.5 [The school does not consent to the Contractor appointing any third party processor of Personal Data under this agreement.] **OR16**

[The school consents to the Contractor appointing [NAME OF THIRD-PARTY PROCESSOR] as a third-party processor of Personal Data under this agreement. The Contractor confirms that it has entered or (as the case may be) will enter with the third-party processor into a written agreement [substantially on that third party's standard terms of business **OR** incorporating terms which are substantially similar to those set out in this clause [NUMBER]] provided that the Contractor shall inform the school of any changes it makes to the written agreement that it puts in place with the third party processor and give the school a chance to object to any such changes. As between the school and the Contractor, the Contractor shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this clause [NUMBER]]17.

1.6 The Contractor shall notify the school immediately if it considers that any of the school's instructions infringe the Data Protection Legislation.

1.7 The Contractor shall provide all reasonable assistance to the school in the preparation of any Data Protection Impact Assessment prior to commencing any processing, taking into account the nature of processing and the information available to the Contractor. Such assistance may, at the discretion of the school, include:

1.7.1 a systematic description of the envisaged processing operations and the purpose of the processing;

16 Amend this clause as appropriate.

17 Amend this clause as appropriate before sending it to the Data Processor.

1.7.2 an assessment of the necessity and proportionality of the processing operations in relation to the services;

1.7.3 an assessment of the risks to the rights and freedoms of Data Subjects;

1.7.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data; and / or

1.7.5 assisting the school to consult the Information Commissioner's Officer if the Data Protection Impact Assessment indicates there is an unmitigated high risk to the processing.

1.8 The Contractor shall notify the school, in particular the Data Protection Officer, [immediately] **OR** [without undue delay] if it:

1.8.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

1.8.2 receives a request to rectify, block or erase any Personal Data;

1.8.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

1.8.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

1.8.5 receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

1.8.6 becomes aware of any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach ("Data Loss Event").

1.9 The Contractor's obligation to notify under clause 1.8 shall include the provision of further information to the school in phases, as details become available.

1.10 Taking into account the nature of the processing, the Contractor shall provide the school with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.8 (and insofar as possible within the timescales reasonably required by the school) including by promptly providing:

1.10.1 the school with full details and copies of the complaint, communication or request;

1.10.2 such assistance as is reasonably requested by the school to enable the school to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

1.10.3 the school, at its request, with any Personal Data it holds in relation to a Data Subject;

1.10.4 assistance as requested by the school following any Data Loss Event;

1.10.5 assistance as requested by the school with respect to any request from the Information Commissioner's Office, or any consultation by the school with the Information Commissioner's Office.

1.11 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The school may on not less than 30 Working Days' notice to the Contractor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.12 Either party may, at any time on not less than 30 days' notice, revise this clause [NUMBER x] by replacing it with any applicable controller to processor standard clauses or similar terms forming party of an applicable certification scheme (which shall apply when replaced by attachment to this agreement).

1.13 The parties acknowledge that nothing within these Data Protection Clauses relieves the Contractor of its own direct responsibilities and liabilities under the Data Protection Legislation.

1.14 Any provisions in the Agreement which limit or purport to limit the Contractor's liability and / or in which the school indemnifies the Contractor for losses shall not apply to any breach by the Contractor of these Data Protection Clauses and / or the Data Protection Legislation.

This addendum is entered into and becomes a binding part of the Agreement with effect from the date first set out above.

**Signed by [ ] on behalf of Hunsdon JMI School**

Signature _____

Name _____

Title _____

Date Signed _____

**Signed by [ ] on behalf of [Name of Contractor]**

Signature _____

Name _____

Title _____

Date Signed _____

**SCHEDULE18**

**PROCESSING, PERSONAL DATA AND DATA SUBJECTS**

The Contractor shall comply with any further written instructions with respect to processing by the school. Any such further instructions shall be incorporated into this Schedule.

**1. PROCESSING BY THE CONTRACTOR**

**SCOPE**

[***This should be a high level, short description of what the processing is about i.e. its subject matter***]

**NATURE AND PURPOSES**

***[Be as specific as possible, but make sure that you cover all intended purposes.***

***The nature of the processing means any operation 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 of data (whether or not by automated means) etc.***

***The purpose might include: employment processing, statutory obligation, provision of support services for the benefit of pupils, IT and infrastructure support etc.]***

**DURATION OF THE PROCESSING**

***[Clearly set out the duration of the processing including dates]***

**TYPES OF PERSONAL DATA**

***[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data, religion, ethnicity, information about trade union membership, information about Data Subjects' health, information about criminal offences, etc.]***

**CATEGORIES OF DATA SUBJECT**

***[Examples include: Staff (including volunteers, agents, and temporary workers), students / pupils, members of the public, parents/ carers, governors / trustees etc.]***

**PLAN FOR RETURN AND DESTRUCTION OF THE DATA**

[***Describe how long the data will be retained for, how it will be returned or destroyed unless the Data Processor is legally required to keep the data]***

18 The information required by this schedule must be completed.