Haydon School

GDPR POLICY

1. Policy statement and objectives

1.1 The objectives of this data protection Policy are to ensure that Haydon School ('the School') and its trustees, members and employees are informed about, and comply with, their obligations under the General Data Protection Regulation ('the GDPR'), the Data Protection Act 2018 ('the DPA 2018') and other data protection legislation.

1.2 The School is an Academy Trust 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, students, parents/carers and other members of students' families, trustees/governors, members, volunteers, suppliers, contractors 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, the DPA 2018 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 and the DPA 2018 may expose the School to enforcement action by the Information Commissioner's Office (ICO) or 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 data protection legislation 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 governors 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.

2.2 This Policy should be viewed in conjunction with our Privacy Notices that provide details on each processing activity undertaken which involves Personal Data and provide Data Subjects with information on their data protection rights and information on how to exercise these rights.

2.3 To understand the School's full approach to data protection, please also refer to our E-Safety and ICT Policy, Record Management and Retention Policy, Protection of Biometric Information Policy, Freedom of Information Policy, Surveillance and CCTV Policy, Safeguarding Policy and Code of Conduct.

3. Data Protection Officer

3.1 The Data Protection Officer ('the DPO') is responsible for ensuring the School is compliant with the GDPR, the DPA 2018 and with this Policy. This post is held at School level by Mrs L Faraj. Any questions or concerns about the operation of this Policy should be referred in the first instance to the DPO, dpo@haydonschool.org.uk.

3.2 The DPO will play a major role in embedding essential aspects of the GDPR, the DPA 2018 and other data protection legislation 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 is involved, in a timely manner, in all issues relating to the protection of personal data. To do this, the GDPR requires that the DPO is provided with the necessary 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 the DPO 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 the DPO 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 access to external legal advice.

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 will report to the key strategic decision makers of the School, the Governing Body.

3.6 The requirement that the DPO reports directly to the Governing Body ensures that the School's trustees 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, Director of Finance and Operations, Network Manager 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 the DPO.

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 the 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;

3.9.4 declare that the DPO has no conflict of interests with regard to his or her function as the DPO, as a way of raising awareness of this requirement.

3.9.5 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 School's DPO, dpo@haydonschool.org.uk.

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 finger print or 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 and trustees whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our data protection and security policies as well as the DPO's advice 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** is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. **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 and other related legislation.

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. Sensitive categories of Personal Data are given extra protection. As the School, we process some sensitive information about our students that is not set out in the legislation as a 'special category Personal Data' such as information about children's services interactions, free school meal status, pupil premium eligibility, elements of special educational need information, and some behaviour data. We follow the Department for Education guidance and treat the above categories with the same 'high status' as the special categories set out in law.

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.

6. 'Processed lawfully, fairly and in a transparent manner'

6.1 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.

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

6.2.1 where we have the **Consent** of the Data Subject;
6.2.2 where it is necessary for compliance with a **legal obligation**;
6.2.3 the processing is necessary to fulfil a **contract** or because an individual has asked us to take specific steps before entering into a contract;
6.2.4 where processing is necessary to protect the **vital interests** of the Data Subject or another person;
6.2.5 where it is necessary to carry out a **public task** of providing education and associated functions;
6.2.6 the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests (this will not apply to processing data needed to perform our official task of providing education).

Some of the reasons listed above may overlap and there may be several grounds which justify the School's use of Personal Data.

6.3 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.

7. Sensitive Personal Data

7.1 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.

7.2 When Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 6.2 above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

7.2.1 the Data Subject's explicit consent to the processing of such data has been obtained;
7.2.2 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;
7.2.3 processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
7.2.4 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment law 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.

7.3 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, free school meal status, pupil premium eligibility, elements of special educational need information, some behaviour data, and 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.

7.4 **Safeguarding information** will be treated by the School as 'special category data' and will be given extra protection. To effectively safeguard and promote the welfare of our students, it can sometimes be essential for us to share sensitive safeguarding information with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and/or the Police. Under the GDPR and the DPA 2018, schools can share information without consent for the purpose of "safeguarding of children and individuals at risk". Information will be legally shared without consent if we are unable to, or cannot reasonably expect to, obtain consent from the individual, or if gaining consent could place a student at risk. We will also share relevant personal information if the purpose is to keep a student safe from neglect or harm, or if it protects their wellbeing. All staff members must be made aware of the procedure for reporting concerns and understand their responsibilities in relation to confidentiality and information sharing.

7.5 The School does not intend to seek or hold special categories of Personal Data except where it has been notified of the information or processing relates to Personal Data manifestly made public by the Data Subject, or it comes to the School's attention via legitimate means, or needs to be sought or held in compliance with a legal obligation or as a matter of good practice.

7.6 Biometric Data

7.6.1 The School processes Biometric Data as part of an automated biometric recognition system for cashless catering. Biometric Data is a type of Sensitive Personal Data.

7.6.2 Where Biometric Data relating to students is processed, the School must ensure that each parent of a child is notified of the School's intention to use the child's Biometric Data and obtain the written consent of at least one parent before the data is taken from the student and used as part of an automated biometric recognition system. The School must not process the Biometric Data of a student under 18 years of age where:

7.6.2.1 the student (whether verbally or non-verbally) objects or refuses to participate in the processing of their Biometric Data;
7.6.2.2 no Parent has consented in writing to the processing; or
7.6.2.3 a Parent has objected in writing to such processing, even if another Parent has given written Consent.

7.6.3 The School must provide reasonable alternative means of accessing services for those students who will not be using an automated biometric recognition system.

7.6.4 The School also must obtain the explicit Consent of staff, trustees, members or other Data Subjects before processing their Biometric Data.

7.6.5 The Protection of Biometric Information Policy is a requirement for maintained schools and academies. The Policy will be approved by the Governing Board and will be reviewed annually.

7.6.6 The School will comply with any guidance and advice issued by the Department for Education ('the DfE') on the use of Biometric Data.

7.7 Criminal convictions and offences

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

7.7.2 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, volunteers and trustees or due to information which we may acquire during the course of their employment or appointment.

7.7.3 In addition, from time to time we may acquire information about criminal convictions or offences involving students 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.

7.7.4 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 information secure.

8. Transparency

8.1 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.

8.2 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:

- Students;
- Parents/carers;
- Staff;
- Job Applicants;
- Governors;
- School's visitors;
- Lettings.

8.3 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. School 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 callers or if we ask people to complete forms requiring them to provide their Personal Data.

8.4 We will ensure that Privacy Notices are concise, transparent, intelligible, easily accessible, written in clear and plain language, particularly if addressed to a child, and free of charge.

9. Consent

9.1 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.

9.2 A Data Subject consents to processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so 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.

9.3 In the event that we are relying on Consent as a basis for processing Personal Data about students, if a student is aged under 13, we will need to obtain Consent from the parent(s). When a student is enrolled in the School, Parents will be invited to complete an online Consent form during the enrolment process.

9.4 In the event that we require Consent for processing Personal Data about students aged 13 or over, we will require the Consent of the student although, depending on the circumstances, the School will consider whether it is appropriate to inform parents about this process.

9.5 We understand that the provision of Consent could change depending on the age and maturity of the student. To that end, the School will seek generic student consent for various purposes in Year 9 and Year 12. The School will notify the Parent that generic Consent from their son/daughter is being sought so that they have the opportunity to inform the School of any reasons why the student's name or image should not be used despite the student consenting.

9.6 Consent is likely to be required if, for example, the School wishes to use a photo of a student on its website or on social media. When relying on Consent, we will make sure that the student understands what they are consenting to, and we will not exploit any imbalance in power in the relationship between us. Coordinators of photo- or videoshoots should ensure that all participants are aware of the purpose of the image.

9.7 For those who have not given the generic Consent for various purposes, there may be specific school event for which parents or students would be happy to wave their Consent. Where such events occur, the School may contact individuals to determine whether they are happy to give their permission for that particular occasion.

9.8 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.

9.9 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.

9.10 Evidence and records of Consent must be maintained so that the School can demonstrate compliance with Consent requirements. The Consent will be recorded on the School's MIS database so that all staff know what Consent applies to each student. The DPO will hold Consent records obtained for the specific school events.

10. 'Specified, explicit and legitimate purposes'

10.1 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.

10.2 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.

11. 'Adequate, relevant and limited to what is necessary'

11.1 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.

11.2 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.

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

11.4 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 trustees 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 trustees may be given access to basic information about a student 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).

11.5 When Personal Data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the School's Record Management Policy.

12. 'Accurate and, where necessary, kept up to date'

12.1 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.

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

12.3 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 DPO 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.

12.4 Notwithstanding paragraph 12.3, 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 12.3 has been followed.

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

13.1 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.

13.2 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 (Record Management Policy) for all data.

14. 'Data to be processed in a manner that ensures appropriate security of the Personal Data'

14.1 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.

14.2 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.

14.3 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.

14.4 The School takes reasonable steps to ensure that Data Users will only have access to Personal Data where it is necessary for them to do so.

14.5 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 categories of Personal Data from loss and unauthorised access, use or disclosure. All staff will be made aware of this Policy and any amendments to this Policy and their data protection obligations will be outlined in the Code of Conduct.

14.6 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 E-Safety and ICT Policy, relevant Acceptable Use Agreements for students, parents, all staff, volunteers, and governors, and Guest WiFi Acceptable Use which can be found in the E-Safety and ICT Policy - and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and the DPA 2018 and relevant standards to protect Personal Data.

14.7 Data Users must be aware that it is a criminal offence for someone to knowingly or recklessly obtain or disclose Personal Data without the School's consent (or to ask someone to do it on their behalf) and/or to retain it without our knowledge (for example, if a member of staff

accesses Personal Data about students or other members of staff without our consent and/or shares that data with people who are not permitted to see it). It is also an offence to sell or try to sell such Personal Data. These offences will also be treated as disciplinary issues in accordance with the School's HR policies.

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

14.8.1 confidentiality means that only people who are authorised to use the data can access it;
14.8.2 integrity means that Personal Data should be accurate and suitable for the purpose for which it is processed;
14.8.3 availability means that authorised users should be able to access the data if they need it for authorised purposes.

14.9 It is the responsibility of all members of staff and trustees 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 and/or the DPO.

14.10 Please see our E-Safety and ICT Policy for details for the arrangements in place to keep Personal Data secure.

15. Trustees

15.1 Trustees are likely to process Personal Data when they are performing their duties, for example, if they are dealing with employee issues, student exclusions or parent complaints. Trustees 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:

15.1.1 ensure that Personal Data which comes into their possession as a result of their trustee duties are processed in line with the data protection principles and kept secure from third party access, including family members and friends;
15.1.2 ensure they are provided with a copy of the School's E-Safety and ICT Policy, Privacy Notice for Haydon Governors and this Policy as well as the guidance on using own devices for school related business;
15.1.3 using a School email account for any School-related communications;
15.1.4 ensuring that any School-related communications or information stored or saved on an electronic device or computer is password protected/ multifactor authentication is used;
15.1.5 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;
15.1.6 taking appropriate measures to securely destroy obsolete (no longer needed) data.

12.2 Trustees will be asked to read and sign the Acceptable Use Agreement within E-Safety and ICT Policy.

16. Processing in line with Data Subjects' rights

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

16.1.1 withdraw Consent to processing at any time;

16.1.2 receive certain information about the Data Controller's processing activities;
16.1.3 request access to **their** Personal Data that we hold (Subject Access Request);
16.1.4 prevent our use of their Personal Data for direct marketing purposes;
16.1.5 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;
16.1.6 restrict processing in specific circumstances;
16.1.7 challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
16.1.8 request a copy of an agreement under which Personal Data is transferred outside of the EEA;
16.1.9 object to decisions based solely on Automated Processing, including profiling (Automated Decision Making);
16.1.10 prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
16.1.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
16.1.12 make a complaint to the supervisory authority (the ICO); and
16.1.13 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.

16.2 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. All Personal Data requests should be logged and the DPO must be informed/ consulted.

17. Dealing with Subject Access Requests (SARs)

17.1 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 to the DPO, dpo@haydonschool.org.uk. The School can invite a Data Subject to complete a form but we may not insist that they do so.

17.2 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 (SAR), even if the Data Subject does not specifically use this phrase in their request or refer to the GDPR or the DPA 2018. 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 SAR 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. Please refer to our Freedom of Information Policy for more detail.

17.3 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**. The School may extend the SAR response period by two further months where the School perceives the request as complex and/or numerous. However, the individual must be informed of the extension and the reasoning behind it within one month of the receipt of the request.

17.4 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:

- we will contact the data subject promptly (within one calendar month) and explain the situation;

- we may ask for an extension and we will provide our reasons for it;
- we may seek legal advice where this is required.

17.5 A fee may no longer be charged to the individual for provision of this information. However, where we consider the request as repeated or excessive, an administrative fee based on our costs of providing information may be levied.

17.6 The School will ask the Data Subject for reasonable identification so that we can satisfy ourselves about the person's identity before disclosing the information. We may also wish to clarify if the request is for all the Personal Data held about a Data Subject or simply that relating to particular incident or particular type of data.

17.7 In order to ensure that Data Subjects receive only information about themselves it is essential that a formal system of requests is in place. All files must be reviewed by the DPO before any disclosure takes place. Access will not be granted before this review has taken place.

17.8 Requests from students who are considered mature enough to understand their rights under the GDPR will be processed as a SAR as outlined and the data will be given directly to the student (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 students 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 DPA 2018 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.

17.9 Requests from students who do not appear to understand the nature of the request will be referred to their parents or carers.

17.10 Requests from parents/carers in respect of their own child will be processed as requests made on behalf of the Data Subject (the child) where the student is aged under 13 (subject to any exemptions that apply under the Act or other legislation). If a 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 student for their Consent for disclosure of their Personal Data to their Parent(s). Please note that there may be other lawful basis for sharing the Personal Data with the Parent(s) (subject to any enactment or guidance which permits the School to disclose the Personal Data to a parent without the child's Consent). When a student expressly withholds their agreement for their Personal Data being disclosed to their Parent(s), the School in consultation with the DSL will consider the grounds provided. The School will take into account the student's level of maturity and their ability to make decisions like this, the nature of personal data requested, any court orders relating to parental access that may apply, any duty of confidence owed to the student, whether disclosure will be in the best interests of the student or where there is a requirement to report (for example, for safeguarding) and any consequences of allowing the Parent(s) access student information (particularly when there have been allegations of ill treatment). The School shall not disclose the Personal Data if to do so would breach any of the data protection principles or where information sharing may place a child at risk of significant harm or jeopardise police investigation. The decision and reasons for disclosure/non-disclosure shall be documented.

17.11 It should be noted that the Education (Student Information) (England) Regulations 2005 do not apply to academies so the rights available to parents in those Regulations to access their child's educational records are not applicable to the School. Instead, requests from Parents for Personal Data about their child must be dealt with under the GDPR (as outlined above).

This is without prejudice to the obligation on the School in the Education (Independent School Standards) Regulations 2014 to provide an annual report of each registered student's progress and attainment in the main subject areas taught to every parent (unless they agree otherwise in writing). Please note that the School chooses to share progress, attainment and behaviour information with the Parents as per our Privacy Notices. We consider that sharing certain information with the Parents is in the best interests of our students and is essential to our task of providing education. We will use our judgement and safeguarding considerations on a case-by-case basis.

17.12 Any individual may appoint another person/organisation to request access to their records. In such circumstances, the School must have written evidence that the individual has authorised the person to make the application and the DPO must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

17.13 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). The DPO is responsible for completing the log. Should more information be required to 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. **All information relating to the individual, whether it is held in electronic or paper format, should be considered for disclosure.**

17.14 Where requests are "manifestly unfounded or excessive", in particular because they are repetitive, the School can:

17.14.1 charge a reasonable fee taking into account the administrative costs of providing the information; or
17.14.2 refuse to respond.

17.15 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 SAR and consult the DPO before refusing a request.

17.16 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. **An individual only has the automatic right to access information about themselves.** In the event that the personal data concerns more than one individual, the School must consider whether providing the information would prejudice the rights of any other individual. The School will not be able to disclose the Personal Data of third parties where it does not have their Consent, or where seeking Consent would not be reasonable and it would not be appropriate to release the information. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Where the Personal Data cannot be disclosed, a copy of the full document and a copy of the altered document should be retained with the explanation why the original document was altered. Care should be taken to ensure that documents are redacted properly.

17.17 Confidential references given, or to be given by the School, are exempt from SAR. The School will treat as exempt any confidential reference given by the School for the purpose of education, training or employment of any member of staff, volunteer or a student. Confidential references received from other parties may also be exempt from disclosure,

under the common law of confidence. However, such references can be disclosed if such disclosure will not identify the source of the reference or where the referee has given their Consent, or where disclosure is reasonable of all the circumstances.

17.18 Please seek advice from the DPO if you are unsure if exemptions may apply.

17.19 In the context of an academy a SAR is normally part of a broader complaint or concern from a parent/carer 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.

18. Providing information over the telephone

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

18.1.1 check the caller's identity to make sure that information is only given to a person who is entitled to it;
18.1.2 suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked;
18.1.3 refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

19. Authorised disclosures

19.1 The School will only disclose data about individuals if one of the lawful bases applies.

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

19.2.1 Local Authorities;
19.2.2 the Department for Education and Ofsted;
19.2.3 the Education & Skills Funding Agency;
19.2.4 the Disclosure and Barring Service;
19.2.5 the Teaching Regulation Agency;
19.2.6 the Teachers' Pension Service;
19.2.7 the Local Government Pension Scheme which is administered by Hillingdon Borough Council;
19.2.8 HMRC;
19.2.9 the Police or other law enforcement agencies;
19.2.10 our legal advisors, auditors and other consultants;
19.2.11 insurance providers (the Risk Protection Arrangement);
19.2.12 occupational health advisors;
19.2.13 exam boards including AQA, Edexcel, OCR, WJEC, and RSA;
19.2.14 UCAS and Unifrog (Sixth Form students only);
19.2.15 the Joint Council for Qualifications;
19.2.16 NHS health professionals including educational psychologists and school nurses;
19.2.17 Education Welfare Officers;
19.2.18 Courts, if ordered to do so;
19.2.19 Prevent teams in accordance with the Prevent Duty on schools;
19.2.20 our suppliers and service providers (payroll, HR providers, IT providers, MIS provider, provider of our accounting software, provider of safeguarding and child protection software, provider of performance management software, provider of

software for management of educational visits, extracurricular activities and the Accident Book, provider of our online payment system, provider of our library software, catering provider, photography service, confidential waste collection companies, online learning platforms);

19.2.21 other schools, for example, if we are negotiating a managed move;

19.2.22 schools within 4HConsortium and the 4HConsortium (Year 11 and Sixth Form students only);

19.2.23 employment and recruitment agencies;

19.2.24 parents and other students.

Further specifics can be found in our clear and transparent Privacy Notices.

19.3 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.

19.4 Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. 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.

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

19.6 The GDPR requires the School 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"). 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.

19.7 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.

20. Reporting a Personal Data Breach

20.1 The GDPR requires Data Controllers to notify a Personal Data Breach to the ICO where a breach is likely to result in a risk to the rights and freedoms of individuals and, in certain instances, to notify the Data Subject.

20.2 The term 'Personal Data Breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. The DPO will ensure that all staff members are made aware of, and understand, what constitutes a Personal Data Breach as part of school's annual data protection training.

20.3 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.

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

20.5 It is the responsibility of the DPO, or the nominated deputy, to assess the extent of the breach and the potential consequences and to decide whether to report a Personal Data Breach to the ICO.

20.6 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.

20.7 The School recognises that as we are closed or have 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 Data Breach Response Plan.

20.8 If a member of staff or trustee knows or suspects that a Personal Data Breach has occurred, our Data Breach Response Plan must be followed. In particular, the DPO or such other person identified in our Data Breach Response Plan must be notified immediately. You should preserve all evidence relating to the potential Personal Data Breach, should cooperate fully and assist the DPO with their investigation.

21. Accountability

21.1 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.

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

21.2.1 appointing a suitably qualified DPO and an executive team accountable for data privacy;
21.2.2 implementing Privacy by Design when processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where processing presents a high risk to rights and freedoms of Data Subjects;
21.2.3 integrating data protection into internal documents including but not limited to this data protection Policy, E-Safety and ICT Policy, Safeguarding and Child Protection Policy, Staff Induction Policy, NQT Policy, Code of Conduct, Surveillance and CCTV Policy, Protocol for Passing Information to the Police and Privacy Notices;
21.2.4 regularly training School employees and trustees 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
21.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

22. Record keeping

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

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

22.3 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 retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

23. Training and audit

23.1 We are required to ensure all School personnel and trustees 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.

23.2 Members of staff and school governors must attend all mandatory data privacy related training.

24. Privacy by Design and Data Protection Impact Assessments (DPIA)

24.1 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.

24.2 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:

24.2.1 the state of the art;
24.2.2 the cost of implementation;
24.2.3 the nature, scope, context and purposes of processing; and
24.2.4 the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.

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

24.4 The School should conduct a DPIA and discuss its findings with the DPO when implementing major system or business change programs involving the processing of Personal Data including (but not limited to):

24.4.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
24.4.2 automated processing including profiling and automated decision making;
24.4.3 large scale processing of Sensitive Data; and
24.4.4 large scale, systematic monitoring of a publicly accessible area.

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

24.6 A DPIA must include:

24.6.1 a description of the processing, its purposes and the School's legitimate interests if appropriate;
24.6.2 an assessment of the necessity and proportionality of the processing in relation to its purpose;
24.6.3 an assessment of the risk to individuals; and
24.6.4 the risk mitigation measures in place and demonstration of compliance.

24.7 Where a DPIA indicates high risk data processing, the School will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

25. CCTV

25.1 The School understands that recording images of identifiable individuals constitutes as processing of personal information, so it is done in line with the data protection principles.

25.2 The School uses CCTV in locations around its sites. This is to:

25.2.1 protect the school buildings and our assets;
25.2.2 manage the safety of the school site;
25.2.3 increase personal safety and reduce the fear of crime;
25.2.4 support the Police in a bid to deter and detect crime;
25.2.5 assist in identifying, apprehending and prosecuting offenders;
25.2.6 provide evidence for the School to use in its internal investigations and/or disciplinary processes in the event of behaviour by staff, students or other visitors on the site which breaches or is alleged to breach the School's policies;
25.2.7 protect members of the school community, public and private property; and
25.2.8 assist in managing the School.

25.3 Please refer to the School's Surveillance and CCTV Policy for more information.

26. Automated Decision Making and Profiling

26.1 Individuals have the right **not** to be subject to a decision when:

26.1.1 it is based on automated processing, e.g. profiling;
26.1.2 it produces a legal effect or a similarly significant effect on the individual.

26.2 The School will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

26.3 When automatically processing Personal Data for profiling purposes, the School will ensure that the appropriate safeguards are in place, including:

26.3.1 ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact;
26.3.2 using appropriate mathematical or statistical procedures;
26.3.3 implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors;
26.3.4 securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

26.4 Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

26.4.1 the School has the explicit consent of the individual;
26.4.2 the processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

27. Policy Review

27.1 It is the responsibility of the trustees to facilitate the review of this Policy. Recommendations for any amendments should be reported to the DPO.

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

27.3 This Policy will be reviewed annually or when major national, organisational, legislative or technological changes occur.

27.4 The scheduled review date for this Policy is April 2021.

28. Enquiries

Further information about the School's Data Protection Policy is available from the DPO, dpo@haydonschool.org.uk.

General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk.You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

History

Date	Issue	Status	Comments
May 2018	1	New Policy	To FGB 05.07.18
April 2020	2	Updated	To Personnel Committee 14.06.20, Approved. To Student Committee 01.07.20. Approved. To FGB for ratification 08.07.20. Approved