HAYDON SCHOOL

GDPR Policy

2024-2025

Mission Statement

Haydon School is committed to the achievement of individual excellence, encouraging students to be creative and considerate, confident of their role in society and capable of rising to the challenges of a diverse and rapidly developing global economy.

1. Policy statement and objectives

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

1.2. The School is the Data Controller for most data processing activities.

1.3. 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 UK GDPR, the DPA 2018 and the Privacy and Electronic Communications Regulations (PECR) 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 the School's reputation and have serious consequences for the School and its stakeholders.

1.4. This Policy is backed up by written procedures.

2. Legal framework

2.1. This Policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- UK GDPR;
- DPA 2018;
- Freedom of Information Act 2000 ('FoI Act 2000');
- Electronic Commerce (EC Directive) Regulations 2002;
- The Privacy and Electronic Communications (EC Directive) Regulations 2003;
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018);
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004;
- School Standards and Framework Act 1998;
- Protection of Freedoms Act 2012;
- DfE (2023) Keeping children safe in education 2023

2.2. This Policy also has regard to the following guidance:

- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)';

- DfE (2023) 'Data protection in schools';
- ICO (2012) 'IT asset disposal for organisations';
- ICO 'Taking photographs: data protection advice for schools'.

2.3. This Policy should be viewed in conjunction with our Privacy Notices (on our website) 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.

2.4. To understand our full approach to data protection, please also refer to our E-Safety and ICT Policy, Records Management Policy, Protection of Biometric Information Policy, Freedom of Information Policy and FoI Publication Scheme, Surveillance and CCTV Policy, Child Protection and Safeguarding Policy and Code of Conduct.

3. Data Protection Officer

3.1. The Data Protection Officer ('the DPO') is responsible for ensuring School's compliance with the UK GDPR and the DPA 2018 .

3.2. The DPO acts as the central point of contact in relation to matters of data protection. The DPO is involved, in a timely manner, in all issues relating to the protection of Personal Data. To do this, the DPO is provided with the necessary support and resources including time for the DPO to fulfil their duties.

3.3. Where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member is set out.

3.4. 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.

3.6. Further, the DPO will report to the key strategic decision makers of the School, the Governing Body. This will ensure that that the governors are made aware of the pertinent data protection issues.

3.7. 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.

3.8. A DPO appointed internally by the School is permitted to undertake other tasks and duties, but these must not result in a conflict of interests with their

role as the DPO. When the School decides to appoint an internal DPO, the School will take the following action in order to avoid conflicts of interests:

- identify the positions incompatible with the function of the DPO;
- draw up internal rules to avoid conflicts of interests;
- declare that the DPO has no conflict of interests with regard to their function as the DPO, as a way of raising awareness of this requirement;
- 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.

3.9. Staff must ensure that they involve the DPO in all data protection matters closely and in a timely manner.

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 fingerprint 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 and in a cloud, 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.

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 and contractors whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following this and related 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, directly or indirectly, such as a name, an identification number, location data, or an online identifier.

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.

4.11. Privacy by Design means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR, the DPA 2018 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 is defined in the UK GDPR as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic and 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. The School processes 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. In accordance with the requirements outlined in the UK GDPR, Personal Data will be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date;
- kept for no longer than is necessary;
- processed securely, using appropriate technical or organisational measures.

5.2. The UK GDPR requires the School to take responsibility for the data processing activities and to have appropriate measures and records in place to demonstrate compliance.

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

6.1. Valid grounds for processing will be identified and documented prior to any Processing taking place.

6.2. At least one of the below lawful bases must apply whenever the School processes Personal Data: Consent; contract; legal obligation; vital interest; public task; legitimate interests (this will not apply when the School processes Personal Data for its official tasks).

6.3. 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.

6.4. The School will process Personal Data fairly and will not process Personal Data in a way that is unduly detrimental, unexpected or misleading.

6.5. 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.

6.6. For Personal Data to be processed fairly, the School informs the Data Subjects via Policies and Privacy Notices that the Personal Data is being processed; why the Personal Data is being processed; what the lawful basis is for that processing; whether the Personal Data will be shared, and if so, with whom; the existence of the Data Subject's rights in relation to the processing of that Personal Data; and the right of the Data Subject to raise a complaint with the ICO in relation to any Processing.

6.7. Where the School relies on 'legitimate interests' to process Personal Data, the School takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.

6.8. Where the School relies on Consent to process Personal Data, the School ensures that the requirements outlined in the 'Consent' section are met.

7. Sensitive Personal Data

7.1. When sensitive categories of Personal Data are processed, as well as establishing a lawful basis, a separate condition for Processing it must be met:

- the Data Subject's explicit Consent to the Processing of such Data has been obtained;
- Processing relates to Personal Data manifestly made public by the Data Subject;
- Processing is necessary for reasons of substantial public interest with a basis in law which shall be proportionate to the aim pursued and which contains appropriate safeguards;
- 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;
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
- Processing is necessary for the purposes of carrying out the obligations under employment, social security or social protection law, or a collective agreement;
- Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law;
- Processing is necessary for the reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medical products and medical devices;
- Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law.

7.2 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.

7.3 Safeguarding information is treated by the School as 'special category data' and is given extra protection. 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.

7.4 There may be circumstances where it is considered necessary to process Personal Data or special category Personal Data in order to protect the vital

interests of a Data Subject. This may include medical emergencies where it is not possible for the Data Subject to give Consent to the Processing.

8. Safeguarding

8.1 The School understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

8.2 The School will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect students. The School will ensure that staff are:

- confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category Personal Data';
- aware that information can be shared without Consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a student in a timely manner.

8.3 The School will aim to gain Consent to share information where appropriate; however, staff will not endeavour to gain Consent if to do so would place a child at risk. The School will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

8.4 Student's Personal Data will not be provided where the serious harm test is met. Where there is doubt, the School will seek independent legal advice.

9. Biometric Data

9.1. The School processes Biometric Data as part of an automated biometric recognition system for cashless catering.

9.2. Biometric Data is processed in line with the Protection of Biometric Information Policy.

10. Criminal convictions and offences

10.1. There are separate safeguards in the UK GDPR for Personal Data relating to criminal convictions and offences. The School is only able to process this if it is either under the control of official authority or authorised by domestic law. The latter point can only be used if the conditions of the reason for storing and requiring the Data fall under the processing necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Controller of the Data Subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

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

10.3. 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. 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.

10.4. Where appropriate, Data about criminal allegations, proceedings or convictions 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. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of their responsibilities as a data handler. Data Processing Agreements outlining necessary safeguards must be in place for all contactors handling DBS data.

11. Transparency

11.1. One of the key requirements of the UK GDPR relates to transparency. This means that the School must keep Data Subjects (adults and children) informed about how their Personal Data will be processed when it is collected.

11.2. The School conveys this information to individuals through Privacy Notices addressed to students, parents/carers, staff, job applicants, governors, visitors, hirers of the school premises.

11.3. In relation to Data obtained both directly from the Data Subject and indirectly, the following information will be supplied within the Privacy Notice:

- the identity and contact details of the Controller, the Controller's representative, where applicable, and the DPO;
- the purpose of, and the lawful basis for, Processing the Data;
- the legitimate interests of the Controller or third party;
- any recipient or categories of recipients of the Personal Data;
- details of transfers to third countries and the safeguards in place;
- the retention period of criteria used to determine the retention period;
- the existence of the Data Subject's rights, including the right to withdraw consent at any time and lodge a complaint with a supervisory authority;
- the existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

11.4. 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.

11.5. The School adopts a layered approach to keeping Data Subjects informed about how we process their Personal Data. This means that the Privacy Notice is just one of the tools the School uses to communicate this information. Our employees are expected to use other appropriate and proportionate methods to tell individuals how their Personal Data is being processed.

12. Consent

12.1. The School will only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR and the DPA 2018, 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.

12.2. 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.

12.3. The provision of Consent could change depending on the age and maturity of the student.

12.4. Where the School is relying on Consent as a basis for processing Personal Data about students under 13 years old or students that are not considered mature enough to understand their data protection rights, the School will obtain Consent from their Parent. In the event that we require Consent for processing Personal Data about students aged 13 or over, having considered the maturity of the student, we will require the Consent of the student although, depending on the circumstances, the School will inform Parents about this process.

12.5. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured.

12.6. Consent may need to be refreshed if the School intends to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

12.7. Consent is likely to be required if, for example, the School wishes to use a photo of a student on social media. When relying on Consent, the School will make sure that the student understands what they are consenting to, and will not exploit any imbalance in power in the relationship between us.

Coordinators of photo- or video shoots should ensure that all participants are aware of the purpose of the image.

12.8. Often the School relies on another legal basis (and does not require explicit Consent) to process most types of Sensitive Data. Otherwise, explicit Consent will be obtained.

12.9. Evidence and records of how and when Consent was given and what the Data Subject was told must be maintained.

13. 'Specified, explicit and legitimate purposes'

13.1. Personal Data will be collected for the specific purpose notified to the Data Subject. Any Data which is not necessary for that purpose should not be collected.

13.2. The School will be clear with Data Subjects about why their Personal Data is being collected and how it will be processed. The School 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.

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

14.1. 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.

14.2. 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.

14.3. 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. The School employees should ensure that any Personal Data collected is adequate and relevant for the intended purposes.

14.4. The School will implement measures to ensure that Personal Data is processed on a 'need to know' basis - 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.

14.5. When Personal Data is no longer needed for specified purposes, it must be securely deleted or anonymised.

15. ‘Accurate and, where necessary, kept up to date’

15.1. Personal Data must be accurate and kept up to date. Steps should 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 securely destroyed.

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

15.3. Where a Data Subject challenges the accuracy of their Data, the School will immediately mark their 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. Until resolved the ‘challenged’ marker will remain and all disclosures of the affected information will contain both versions of the information.

15.4. A Data Subject has the right under the UK GDPR to refer a complaint to the Information Commissioner’s Office regardless of whether the procedure has been followed.

16. ‘Data to be kept for no longer than is necessary for the purposes for which the Personal Data are processed’

16.1. Personal Data should not be kept longer than is necessary for the purpose for which it is held and in line with the Record Management Policy and Retention Schedule.

17. ‘Data to be processed in a manner that ensures appropriate security of the Personal Data’

17.1. The UK 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.

17.2. 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.

17.3. The School has developed, implemented and are maintaining 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). The Network Manager regularly evaluates and tests the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

17.4. 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.

17.5. Data Users are responsible for protecting the Personal Data we hold and 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. Staff data protection obligations are outlined in the Code of Conduct. The School holds the right to take the necessary disciplinary action against a staff member if they believe them to be in breach of the specified security measures.

17.6. Data Users must follow all procedures and technologies the School puts 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 and the relevant Acceptable Use Agreements. Data Users must not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain.

17.7. Through a notification below the School informs all Data Users 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). It is an offence to retain Personal Data 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.

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

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

17.9. 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 data security should notify the DPO.

17.10. School's E-Safety and ICT Policy describes the details for the arrangements in place to keep Personal Data secure. The School will regularly test, create and improve security features.

18. Governors

18.1. Governors 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. Governors are 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.

19. Processing in line with Data Subjects' rights

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

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

19.2. The School is required to verify the identity of an individual requesting Data under any of the rights listed above. Members of staff should not disclose Personal Data without proper authorisation. All Personal Data requests should be logged and the DPO must be informed without undue delay.

19.3. The School will comply with the data requests without undue delay and within one month of receipt of the request. Where the request is complex, or a number of requests have been received, the time frame can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request. Data requests will be handled free of charge; however, the School may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. Where no action is being taken in response to the data request, the School will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

19.4. The right to erasure:

19.4.1 Individuals, including children, hold the right to request the deletion or removal of Personal Data where there is no compelling reason for its continued Processing. Individuals, including children, have the right to erasure in the following circumstances:

- where the Personal Data is no longer necessary in relation to the purpose for which it was originally collected or processed;
- when the individual withdraws their Consent where Consent was the lawful basis on which the Processing of the Data relied;
- when the individual objects to the Processing and there is no overriding legitimate interest for continuing the Processing;
- the Personal Data was unlawfully processed;
- the Personal Data is required to be erased in order to comply with a legal obligation;
- the Personal Data is processed in relation to the offer of information society services to a child.

19.4.2 The School has the right to refuse a request for erasure where the Personal Data is being processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes;
- for the establishment, exercise or defence of legal claims.

19.4.3 The School has the right to refuse a request for erasure for special category data where Processing is necessary for:

- public health purposes in the public interest, e.g. protecting against serious cross-border threats to health;
- purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

19.4.4 As a student may not fully understand the risks involved in the Processing of Data when Consent is obtained, special attention will be given to existing situations where a student has given Consent to Processing and they later request erasure of the Data, regardless of age at the time of the request. Where Personal Data has been disclosed to third parties, they will be informed about the erasure of the Personal Data, unless it is impossible or involves disproportionate effort to do so. Where Personal Data has been made public within an online environment, the School will inform other organisations who process the Personal Data to erase links to and copies of the Personal Data in question.

19.5. The right to restrict processing:

19.5.1 Individuals, including children, have the right to block or suppress the School's Processing of Personal Data.

19.5.2 The School will restrict the Processing of Personal Data in the following circumstances:

- where an individual contests the accuracy of the Personal Data, Processing will be restricted until the School has verified the accuracy of the Data;
- where an individual has objected to the Processing and the School is considering whether their legitimate grounds override those of the individual;
- where Processing is unlawful and the individual opposes erasure and requests restriction instead;
- where the School no longer needs the Personal Data but the individual requires the data to establish, exercise or defend a legal claim.

19.5.3 In the event that processing is restricted, the School will store the Personal Data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. The School will inform individuals when a restriction on Processing has been lifted.

19.5.4 Where the School is restricting the Processing of Personal Data in response to a request, it will make that Data inaccessible to others, where possible.

19.5.5 If the Personal Data in question has been disclosed to third parties, the School will inform them about the restriction on the processing of the Personal Data, unless it is impossible or involves disproportionate effort to do so.

19.5.6 The School reserves the right to refuse requests for restricting Processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

19.6. The right to object:

19.6.1 The School informs Data Subjects of their right to object via this Policy. Data Subjects, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest;

- Processing used for direct marketing purposes;
- Processing for purposes of scientific or historical research and statistics.

19.6.2 Where Personal Data is processed for the performance of a legal task or legitimate interests:

- an individual's grounds for objecting must relate to his or her particular situation;
- the School will stop Processing the individual's Personal Data unless the Processing is for the establishment, exercise or defence of legal claims, or, where the School can demonstrate compelling legitimate grounds for the Processing, which override the interests, rights and freedoms of the individual;
- the School will respond to objections proportionally, granting more weight to an individual's objection if the Processing of their Data is causing them substantial damage or distress.

19.6.3 Where Personal Data is processed for direct marketing purposes:

- the right to object is absolute and the School will stop Processing Personal Data for direct marketing purposes as soon as an objection is received;
- the School cannot refuse an individual's objection regarding Data that is being processed for direct marketing purposes;
- the School will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

19.6.4 Where Personal Data is processed for research purposes the individual must have grounds relating to their particular situation in order to exercise their right to object.

19.6.5 Where the processing of Personal Data is necessary for the performance of a public interest task, the School is not required to comply with an objection to the processing of the Data.

19.6.6 The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings.

20. Dealing with Subject Access Requests (SARs)

20.1. The UK GDPR and DPA 2018 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 should be made in writing to the DPO, info@haydonschool.com.

20.2. On receipt of the SAR, a formal procedure will be followed.

20.3. All members of staff are trained to recognise that a verbal or a written request made by a person to gain access to their Personal Data 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 UK GDPR or the DPA 2018.

20.4. 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. The individual will be informed of the extension and the reasoning behind it within one month of the receipt of the request.

20.5. 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.

20.6. A fee may no longer be charged to the individual for provision of this information. However, where we consider the request as manifestly unfounded, repeated or excessive or if an individual requests further copies of the same information, an administrative fee based on our costs of providing information may be levied.

20.7. 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. The School will ask the requestor to specify the information the request is in relation to – the time limit for responding to the request will be paused until clarification from the requestor is received.

20.8. All files must be reviewed by the DPO before any disclosure takes place. Access will not be granted before this review has taken place.

20.9. Requests from students who are considered capable of fully understanding their rights 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 UK 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 the Data Controller, to assess whether the student is capable of understanding their rights under the UK GDPR and the DPA 2018 and the implications of their actions, and so decide whether the Parent needs to make the request on their 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.

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

20.11. Requests from parents/carers in respect of their own child will be processed as requests made on behalf of the Data Subject (the student). If a Parent makes a request for their child's Personal Data and the School evaluates that the student is capable of fully understanding their rights, the School shall ask the student for their Consent for disclosure of their Personal Data to their Parent(s). 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 student'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 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 student at risk of significant harm or jeopardise police investigation. The decision and reasons shall be documented.

20.12. 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 UK GDPR (as outlined above). This is without prejudice to the obligation on the School 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.

20.13. 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.

20.14. Following receipt of a SAR, and provided that there is sufficient information to process the request, an entry should be made in the SAR 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. 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.

20.15. Where requests are 'manifestly unfounded or excessive', in particular because they are repetitive, the School can:

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

20.16. If the request cannot be fulfilled without disclosing another individual's Personal Data, unless that individual consents or it is unreasonable to comply without Consent, the School will reject such requests. The School will explain to the individual who made the SAR why their request could not be responded to.

20.17. Confidential references are exempt from a 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.

21. Authorised disclosures

21.1. The School will only disclose Data about individuals if one of the lawful bases applies.

21.2. Only authorised and trained staff are allowed to make external disclosures of Personal Data.

21.3. 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 (further specifics can be found in our clear and transparent Privacy Notices):

- Local Authorities;
- the Department for Education and Ofsted;
- the Education & Skills Funding Agency;
- the Disclosure and Barring Service;
- the Teaching Regulation Agency;
- the Teachers' Pension Service;

- the Local Government Pension Scheme which is administered by Hillingdon Borough Council;
- HMRC;
- the Police or other law enforcement agencies;
- our legal advisors, auditors and other consultants;
- insurance providers (the Risk Protection Arrangement);
- occupational health advisors;
- exam boards including AQA, Edexcel, OCR, WJEC, and RSA;
- UCAS and Unifrog (Sixth Form students and teachers);
- the Joint Council for Qualifications;
- NHS health professionals including educational psychologists and school nurses;
- Education Welfare Officers;
- Courts, if ordered to do so;
- Prevent teams in accordance with the Prevent Duty on schools;
- 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, photography service, confidential waste collection companies, online learning platforms);
- other schools, for example, if we are negotiating a managed move;
- employment and recruitment agencies;
- Parents.

21.4. 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.

21.5. 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.

21.6. All Data Sharing Agreements must be signed off by the DPO who will keep a register of all Data Sharing Agreements.

21.7. The UK 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.

21.8. 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 UK 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.

22. Reporting a Personal Data Breach

22.1. All staff members and the governors are made aware of, and understand, what constitutes a Personal Data Breach as part of their annual data protection training.

22.2. Data Controllers must 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. 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.

22.3. A notifiable Personal Data Breach will be reported to the ICO without undue delay and where feasible within 72 hours of the School becoming aware of it.

22.4. If the breach is likely to result in high risk to affected Data Subjects, the School will inform Data Subjects without undue delay. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the ICO. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

22.5. When notifying an individual about a breach to their Personal Data, the School will provide specific and clear advice to individuals on the steps they can take to protect themselves and their Data, where possible and appropriate to do so.

22.6. The School has developed a procedure to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where is required to do so. The School will work to identify the cause of the breach and assess how a recurrence can be prevented.

22.7. 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. The School will consider any proportionate measures that can be implemented to mitigate the impact this may have on Data Subjects.

23. Accountability

23.1. The School implements appropriate technical and organisational measures to ensure compliance with the UK GDPR and DPA 2018. The School ensures compliance by :

- appointing a suitably qualified DPO;
- documenting processing activities;
- implementing Privacy by Design and completing Data Protection Impact Assessments (DPIAs) where the need is identified;
- integrating data protection into internal documents including but not limited to this Policy, E-Safety and ICT Policy, Protection of Biometric Information Policy, Records Management Policy, Retention Schedule, 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;
- regularly training School employees and governors on data protection matters including, for example, Cyber Security, Data Subject's rights, Consent, legal bases, DPIAs and Personal Data Breaches. The School maintains records of completed training.
- regularly test our systems and processes to assess compliance.

24. Record keeping

24.1. Records of activities relating to higher risk processing is maintained, such as the processing of activities that:

- are not occasional;
- could result in a risk to the rights and freedoms of individuals;
- involve the Processing of special categories of Data or criminal conviction and offence Data.

24.2. Internal records of processing activities (Data Asset Register) will include the following:

- name and details of the organisation;
- purpose(s) of the processing;
- description of the categories of individuals and Personal Data;
- retention schedule;
- categories of recipients of Personal Data;
- description of technical and organisational security measures;
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

24.3. The School will also document other aspects of compliance with the UK GDPR and DPA 2018 where this is deemed appropriate, including the following:

- information required for Privacy Notices, e.g. the lawful basis for the processing;
- records of Consent;
- Controller-Processor contracts;
- the location of Personal Data;
- DPIA reports;
- records of Personal Data Breaches.

24.4. The School will implement measures that meet the principles of data protection by design and default, such as:

- minimising the Processing of Personal Data;
- pseudonymising Personal Data as soon as possible where practical;
- ensuring transparency in respect of the functions and Processing of Personal Data;
- allowing individuals to monitor Processing;
- continuously creating and improving security features.

24.5. DPIAs are used to identify and reduce data protection risks, where appropriate.

24.6. Staff must familiarise themselves with this Policy, the Code of Conduct, the School's Record Management Policy and Retention Schedule as part of the induction process.

24.7. Data will not be kept for longer than is necessary. Unrequired data will be deleted in line with the School's Retention Schedule.

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

25.1. We strive 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.

25.2. The School assesses what Privacy by Design measures can be implemented on all programs/systems/processes that process Personal Data by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

25.3. The School implements a data protection by design and default approach by using a number of methods, including, but not limited to:

- considering data protection issues as part of the design and implementation of systems, services and practices;
- making data protection an essential component of the core functionality of processing systems and services;
- automatically protecting personal data in our ICT systems;
- implementing basic technical measures within the School network and ICT systems to ensure Data is kept secure;
- promoting the identity of the DPO as a point of contact;
- ensuring that documents are written in plain language so individuals can easily understand what is being done with Personal Data.

25.4. DPIAs are used in certain circumstances to identify the most effective method of complying with our data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the School to identify and resolve problems at an early stage.

25.5. 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):

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

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

25.7. High risk Processing includes, but is not limited to, the following:

- systematic and extensive processing activities, such as profiling;
- large scale Processing of special categories of Data or Personal Data which is in relation to criminal convictions or offences;
- the use of CCTV.

25.8. The School will ensure that all DPIAs include the following :

- a description of the Processing, its purposes and legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

25.9. 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.

26. CCTV and photography

26.1. The School recognises that recording images of identifiable individuals constitutes as Processing of personal information, so it is undertaken in line with the data protection principles.

26.2. For more information about CCTV Processing please refer to the School's Surveillance and CCTV Policy (on the school's website).

26.3. The School follows ICO's guidance "Taking photographs: data protection advice for schools" when Processing student images. Parents attending school events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by Parents or visitors to the school. The School asks that Parents not post any images or videos which include any children other than their own on any social media, or otherwise publish those images or videos.

27. Automated Decision Making and Profiling

27.1. Individuals have the right not to be subject to a decision when:

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

27.2. 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.

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

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

27.4. Automated decisions must not concern a child or be based on the Processing of sensitive Data, unless:

- the School has the explicit Consent of the individual;

- the Processing is necessary for reasons of substantial public interest.

27.5. The School will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.

27.6. The School will ensure that individuals concerned are given specific information about the Processing and an opportunity to challenge or request a review of the decision.

28. Cloud computing

28.1. For the purposes of this Policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the School staff accessing a shared pool of ICT services remotely via a private network or the internet.

28.2. All staff are made aware through this Policy, E-Safety and ICT Policy and the Code of Conduct of data protection requirements and how these are impacted by the storing of Data in the cloud, including that cloud usage does not prevent Data Subjects from exercising their data protection rights.

28.3. Robust safeguards outlined in the School's 'E-Safety and ICT Policy' and relevant procedures will be implemented when using 'cloud computing'.

28.4. The School's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the Network Manager as per relevant procedure. The Network Manager will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA 2018. A copy of the contract must be passed to the DPO for approval.

29. Policy Review

29.1. We will continue to review the effectiveness of this Policy annually to ensure it is achieving its stated objectives. The next review date is June 2025.

30. Enquiries

30.1 Further information about the Data Protection Policy is available from the DPO, dpo@haydonschool.com.

30.2 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
June 2024	3		To FBG July 2024 Approved