Be all you can be
Hayes School

No. 28. DATA PROTECTION POLICY

Adopted on: 4th June 2018 **Review Date: June 2020**

Contents:

1. Purpose

1.1 In order to operate effectively, Hayes School has to collect, process and retain information about people who may include current, past and prospective pupils, parents/carers, members of the public, staff, suppliers, volunteers and Governors. Our aim is to ensure that this information is kept secure and in accordance with data protection regulations.

1.2 The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 are effective from 25th May 2018, and replace the Data Protection Act (DPA) 1998. The legislation exists to safeguard every individual's data.

1.3 The GDPR exists to protect individual rights in an increasingly digital world. This policy applies to all information, regardless of the way it is used and whether the information is held electronically or in hard copy.

2. Scope

2.1 Data refers to any information relating to a living person that identifies them. For example; name, address or phone number. It also relates to details about that person which can include their opinions.

2.2 Some data is considered more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life, sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

2.3 Schools have to collect sensitive data to meet Department for Education (DfE) and Local Authority requirements amongst others, and pupil data may contain information about safeguarding, Special Educational Needs or health needs. Information about other family members may also be held within school records.

2.4 We send a Privacy Notice to all parents and staff and publish the parent notice on our website at: www.hayes.torbay.sch.uk/privacy .

3. Key principles of the General Data Protection Regulation

3.1 The GDPR is based on data protection principles which our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for
- which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

3.2 Lawfulness, transparency and fairness

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**

- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

3.3 Additionally, special categories of personal data are processed on the grounds of:

- explicit consent from the data subject or about their child;
- it is necessary to comply with employment rights or obligations;
- the protection of the vital interests of the data subject or associated person;
- being necessary to comply with the legitimate activities of the school;
- where existing personal data has been made public by the data subject and is no longer confidential;
- when bringing or defending legal claims;
- for safeguarding reasons;
- to comply with legislation regarding processing genetic, biometric or health data.

Processed data is held within the operating systems of the School.

3.4 Collecting and using data for a specific purpose

The School will not use data for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

3.5 Limitation, minimisation, accuracy and retention

The School will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Records Retention Schedule.

The School will take steps to ensure that the data collected is accurate and remains up to date. For pupils and staff, data checks are performed when they join the school and this is checked on an annual basis by sending out data collection sheets.

If a Data Subject believes that the information held is inaccurate, should no longer be held by the Controller, or should not be held by the controller in any event, a complaints policy is in place. Wherever possible we aim to resolve issues as soon as possible, and as such if you have concerns please contact the school.

The School has a records retention schedule which explains how long records are retained. This is available on request from the School office and is on the website under Policies.

4. Data Subjects

4.1 Data Subjects are those people whose details are kept on file by the School. We recognise that some information is more sensitive than others. The GDPR legislation explains that some data such as health conditions and ethnicity are more sensitive, for example, than names and phone numbers.

4.2 Data Subjects have a right:

- to be informed of their rights regarding data protection

- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

4.3 Data subjects' rights are also subject to child protection and safeguarding concerns and sharing of information for the prevention and detection of crime.

4.4 The School has a legal and contractual obligation to share information with organisations such as the Department for Education, Social Care, Local Authority and HMRC amongst others and in some cases these obligations override individual rights.

5. Data Controller

5.1 The Governing Body is the Data Controller and has ultimate responsibility for how the school manages its data and compliance.

5.2 Responsibility within the school is delegated to the Data Protection Officer (DPO) to act on the School's behalf. The Headteacher is responsible for the day to day activities of the DPO.

6. Data Processors

6.1 A Data Processor is the person or organisation that collects, uses, accesses or amends the data that the Data Controller has either collected or authorised to be collected.

6.2 A Data Processor can be a member of staff, a third-party company, a Governor, contractor or temporary employee. It can also be another organisation such as the Police or Local Authority.

6.3 Data Controllers require Data Processors to be as careful about the collection, access and use of data, as the Data Controller themselves.

7. Data Protection Officer (DPO)

7.1 The School has nominated a Data Protection Officer whose role is to:

- Inform and advise the controller or the processor and the employees who carry out processing of their obligations under the GDPR
- monitor compliance with the GDPR and DPA
- provide advice about and monitor data protection impact assessments
- be the point of contact for Data Subjects if there are concerns about data protection
- cooperate with the supervisory authority and manage the breach procedure
- advise about training and CPD for the GDPR

7.2 The School has appointed Mrs A Grant as Data Protection Officer. Telephone: 01803 557336.

8. Staff Responsibilities

8.1 Staff are responsible for:

- Collecting, storing and processing personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law and keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether they have a lawful basis to use personal data in a particular way

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties.

9. Our Data Protection Measures:

We will show that we have integrated data protection into all data processing activities by:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles in relevant legislation
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and
- when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training staff on data protection law, policy and data protection matters
- Regularly conducting reviews and audits to test privacy measures and compliance with legislation
- Maintaining records of our processing activities, including:
  - For data subjects, making available the contact details of the school and DPO and all information we must share about how we process personal data (via privacy notices)
  - For all personal data held, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

10. Data Sharing

10.1 We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of staff at risk
- We need to liaise with other agencies – we will seek consent where necessary in advance
- Our suppliers or contractors need data to enable us to provide services to staff and pupils – for example; IT companies.

When doing this, we will:

- Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and Government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Where we transfer

personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

11. Breaches and Non Compliance

11.1 The school will endeavour to ensure there are no personal data breaches. An incidence of non-compliance with this policy, associated processes, or if there is a breach as described within the GDPR and DPA 2018, we will follow the procedure set out in Appendix 2.

12. Consent

12.1 The School will seek consent from staff, Governors, volunteers, young people, parents and carers to collect and process their data. We will be clear about the reasons for requesting the data and how it will be used. There may be contractual, statutory and regulatory occasions when consent is not required, however, in most cases data will only be processed if explicit consent has been obtained.

12.2 Consent is defined by the GDPR as "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".

12.3 We may on occasion seek consent from young people also. This will be dependent on the child and the reason for processing.

12.4 Pupils and Parents/Carers Consent

All parents/carers will be asked to complete a form giving next of kin details, emergency contact and other essential information about their child when they apply for a place at the school. The school will also ask you to give consent to use the information for other educational purposes as set out on the data collection/consent form. This will be sent out for review annually.

We review your contact details and consent form on an annual basis. It is important to inform us if your details change, or your decision about consent changes.

12.5 Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints.
Where more than one person has the ability to provide or withdraw consent we will consider each situation on its merits and within the principles of GDPR, child welfare, protection and safeguarding principles.

13. Subject Access Requests

13.1 You have the right to ask for copies of information held about yourself (to make a 'subject access request'. This includes:

- Confirmation that your personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long data will be stored for, or if this is not possible, the criteria used to determine this period
- The source of the data, if not yourself

- Whether any automated decision-making is being applied to the data, and what the significance and consequences of this might be.

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name and correspondence address of individual
- Contact number and email address
- Details of the information requested.

If staff receive a subject access request they must immediately forward it to the DPO.

For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. A pupil's ability to understand their rights will always be judged on a case-by-case basis. In certain situations subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil.

13.2 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will explain why, and tell the requester that they have the right to complain to the ICO.

14. Other data protection rights of the individual

14.1 In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO

- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

15. Parental requests to see the educational record

15.1 Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

16. CCTV and Media Policy

16.1 CCTV is used to obtain and store images for a period and may be used for:

- Detection and prevention of crime
- Disciplinary procedures
- Pupil behaviour and exclusion management processes
- To assist the school in complying with legal and regulatory obligations

16.2 We will adhere to the ICO's code of practice for the use of CCTV. We do not need to seek permission to use CCTV but security cameras are clearly visible and signposted.

16.3 The schools seeks explicit parental consent for media exposure for all pupils when they start at the school.

17. Data Security

17.1 We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives containing personal data are kept under lock and key when not in use
- Papers containing confidential personal data are not left on office/classroom desks, in the staff room, on notice/display boards, or left anywhere where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices
- Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff or governors who store personal information on personal devices are expected to follow the same security procedures as for school equipment (see our E-Safety policy and ICT acceptable use policy).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

18. Physical Security

18.1 Every secure area within the School has designated people who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked.

18.2 Offices/cupboards which contain personal data will be secured if the Data Processor is not present.

18.3 All staff, contractors and third parties who have control over lockable areas are required to take due care to prevent data breaches.

19. Secure Disposal

19.1 When disposal of items is necessary a suitable process is used. This is to secure the data and ensure it is not shared in error or by malicious or criminal intent. Personal data which is no longer needed will be disposed of securely. We will shred paper-based records and delete electronic files.

19.2 These processes, when undertaken by a third party, are subject to contractual conditions to ensure GDPR and DPA compliance.

20. Complaints and the Information Commissioner Office (ICO)

20.1 The Complaints Policy deals with complaints about Data Protection. This is available on the School website.

20.2 You have a right to complain if you feel that data has been shared without consent or lawful authority.

20.3 You can complain if you have asked the School to erase, rectify or not process data and we have not agreed to your request.

20.4 We will always try to resolve issues on an informal basis. If this is not successful we will invoke our formal complaints procedure.

20.5 In the UK, the Information Commissioner's Office (ICO) has the responsibility for safeguarding and enforcing the GDPR and DPA. Their contact details are:
Email: casework@ico.org.uk
Helpline: 0303 123 1113
Web: www.ico.org.uk
Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, DK9 5AF

21. Review

21.1 A review of the effectiveness of GDPR compliance, policies and processes will be conducted by the Data Protection Officer every 2 years from the date of this policy.

22. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- E safety Policy
- ICT Acceptable Use Policy for Staff
- Safeguarding and Child Protection Policy

Appendix 1: Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (eg fingerprints, retina/iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Data Protection Officer (DPO)	The person responsible for ensuring the school is compliant with data protection legislation, reporting to the Headteacher and Governing Body.

Appendix 2: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, all staff must immediately notify the DPO.
- The DPO will investigate and decide whether it is a breach. They will consider whether personal data has been accidentally or unlawfully lost, stolen, destroyed, altered, disclosed when it should not have been or made available to unauthorised people.
- The DPO will alert the headteacher and the chair of Governors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff/data processors. (Actions relevant to specific data types are below.)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This will be judged on a case-by-case basis. The DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision and save a record of this on the IT system.
- If the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals and personal data records concerned
        - The name and contact details of the DPO
        - A description of the likely consequences of the breach
        - A description of the measures that have been, or will be taken, to deal with the breach and mitigate effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach (whether or not it is reported to the ICO) including the facts and cause, effects, action taken to contain it and ensure it does not happen again (such as agreeing more robust processes or providing training for staff). The details will be stored on the School's computer system.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different data breaches, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Actions that will be taken in the event of sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has:
    - not been made public; if it has, we will contact the publisher/website owner or
    - administrator to request that the information is removed from their website and deleted.

Appendix 3: Privacy Notice for Parents

Privacy Notice – (How we use pupil information)

We, **Hayes School,** are a data controller for the purposes of the Data Protection Act. We collect personal information from you and may receive information about you from your previous school and the Learning Records Service.

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address).
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility, special educational needs, medical information, exclusions and behavioural information).
- Attendance information[1] (such as sessions attended, number of absences and absence reasons).
- National curriculum assessment results.

The lawful basis on which we use this information

We collect and use pupil information under Article 6 of the General Data Protection Regulations (GDPR), where processing is necessary for compliance with a legal obligation to which the school is subject; where processing is necessary to protect the vital interests of the data subject or of another natural person; and where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school.

We process personal data under Article 9 of the GDPR where:

- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the school;
- 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; and
- Processing is carried out in the course of the school's legitimate activities with appropriate safeguards.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data for the length of time your child attends our school.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupils attend after leaving us

- our local authority (LA)
- the Department for Education (DfE)
- the school nursing service
- the National Health Service

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. We share pupils' data with the Department for Education on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We will not give information about you to anyone without your consent unless the law and our policies allow us to.

We are required to provide data to external agencies under the following Acts:

- section 114 of the Education Act 2005
- section 537A of the Education Act 1996
- section 83 of the Children Act 1989
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and holds information about pupils in schools in England. It provides evidence on educational performance for independent research and DfE studies. It is held in electronic format for statistical purposes. The information is securely collected from sources including schools, local authorities and awarding bodies.

We are required by law, to provide pupil information to the DfE through statutory data collections such as the school census and early years' census. Some of this information is stored in the NPD. To find out more about the NPD,see https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of data is maintained and there are strict controls regarding access and use of data. Decisions on whether DfE releases data to third parties are subject to an approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of data. For information about DfE's data sharing processes, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
https://www.gov.uk/government/publications/national-pupil-database-requests-received

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to access information held about them. To make a request for your personal information, or be given access to your child's educational record, contact the data protection officer at the school (contact details below).

You also have the right to:

- object to processing of personal data that is likely to cause/causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we collect or use your personal data, please raise your concern with us in the first instance. Alternatively, contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact Mrs Allison Grant, Data Protection Officer, by email at: agrant@hayes.torbay.sch.uk or telephone: 01803 557336.

For more information about how the LA and DfE use your information, please see:
http://www.education.gov.uk/researchandstatistics/datatdatam/privacynotices/b00212337/datause
http://www.torbay.gov.uk/council/policies/cs/privacy-notices/

If you cannot access these websites, please contact the LA or DfE as follows:
School Improvement
Torbay Council
Tor Hill House, 1st Floor South
Torquay, TQ1 3DR
Tel: 01803 208916

Public Communications Unit,
Department for Education
Sanctuary Buildings, Great Smith Street
London, SW1P 3BT. www.education.gov.uk
Email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

Appendix 4: Privacy Notice for Staff (How we use school workforce information)

We, **Hayes School,** are a data controller for the purposes of the Data Protection Act. We collect personal information from you and may receive information about you from your previous employer, HM Revenue and Customs and your pensions provider.

Why we collect and use this information

We use school workforce data to:

- enable development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- provide statutory information to agencies such as the Department for Education (DfE) and Local Authority (LA)
- to comply with the law regarding data sharing

The categories of school workforce information we collect, process, hold and share include:

- Personal information (such as name, employee or teacher number, national insurance number and address).
- Special Characteristics (such as ethnicity, language, nationality, gender, country of birth, age and medical information).
- contract information (start dates, hours worked, post, roles, salary information).
- work absence information (such as number of absences and reasons).
- qualifications (and, where relevant, subjects taught)

The lawful basis on which we use this information

We collect and use school workforce information under Article 6 of the General data Protection Regulations (GDPR), where:

- Processing is necessary for compliance with a legal obligation to which the school is subject
- Processing is necessary to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school

We process personal data under Article 9 of the GDPR where:

- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the school;
- Processing is necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent; and
- Processing is carried out in the course of the school's legitimate activities with appropriate safeguards

An example of data processed

An example for data collection purposes (Departmental Censuses) is the Education Act 1996 – see guidance documents at: https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold school workforce data for the length of time you are employed by the school plus 6 years (in line with the school's records retention policy).

Who we share this information with

We routinely share this information with:

- our local authority (LA)
- the Department for Education (DfE)
- the National Health Service

Why we share school workforce information

We do not share information about our workforce with anyone without consent unless the law and our policies allow us to do so. We share information with the Department for Education on a statutory basis. This data sharing underpins school funding and educational policy and monitoring.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools who work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

To find out more about the data collection requirements placed on us by DfE including the data that we share with them, see: https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure the confidentiality of personal data is maintained and there are stringent controls in place regarding its access and use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data. For more information about the data sharing process, visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to access information about you that we hold. To make a request for your personal information, contact the data protection officer at the school (contact details below).

You also have the right to:

- object to processing of personal data that is likely to cause/causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we collect or use your personal data, please raise your concern with us in the first instance. Alternatively, contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact: Mrs Allison Grant, Data Protection Officer, by email at: agrant@hayes.torbay.sch.uk or telephone: 01803 557336.

For more information about how the LA and DfE use your information, please see:
http://www.education.gov.uk/researchandstatistics/datatdatam/privacynotices/b00212337/datause
http://www.torbay.gov.uk/council/policies/cs/privacy-notices/

If you cannot access these websites, please contact the LA or DfE as follows:

School Improvement
Torbay Council
Tor Hill House, 1st Floor South
Torquay, TQ1 3DR
Tel: 01803 208916

Public Communications Unit,
Department for Education
Sanctuary Buildings, Great Smith Street
London, SW1P 3BT. www.education.gov.uk
Email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

Appendix 5: Model publication scheme – Information Commissioner's Office

Freedom of Information Act

This model publication scheme has been prepared and approved by the Information Commissioner. It may be adopted without modification by any public authority without further approval and will be valid until further notice. This publication scheme commits an authority to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the authority. Additional assistance is provided to the definition of these classes in sector specific guidance manuals issued by the Information Commissioner.

The scheme commits an authority:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications below.
- To specify the information which is held by the authority and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the authority makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.
- To publish any dataset held by the authority that has been requested, and any updated versions it holds, unless the authority is satisfied that it is not appropriate to do so; to publish the dataset, where reasonably practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and the public authority is the only owner, to make the information available for re-use under the terms of the Re-use of Public Sector Information Regulations 2015, if they apply, and otherwise under the terms of the Freedom of Information Act section 19.

The term 'dataset' is defined in section 11(5) of the Freedom of Information Act. The term 'relevant copyright work' is defined in section 19(8) of that Act.

Classes of information

Who we are and what we do.
Organisational information, locations and contacts, constitutional and legal governance.

What we spend and how we spend it.
Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

What our priorities are and how we are doing.
Strategy and performance information, plans, assessments, inspections and reviews.

How we make decisions.
Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

Our policies and procedures.
Current written protocols for delivering our functions and responsibilities.

Lists and registers.

Information held in registers required by law and other lists and registers relating to the functions of the authority.

The services we offer.
Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered. The classes of information will not generally include:
- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

The method by which information published under this scheme will be made available

The authority will indicate clearly to the public what information is covered by this scheme and how it can be obtained. Where it is within the capability of a public authority, information will be provided on a website. Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, a public authority will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.
Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so. Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

Charges which may be made for information published under this scheme

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the authority for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on a website will be provided free of charge.
Charges may be made for information subject to a charging regime specified by Parliament.
Charges may be made for actual disbursements incurred such as:
- photocopying
- postage and packaging
- the costs directly incurred as a result of viewing information

Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.

Charges may also be made for making datasets (or parts of datasets) that are relevant copyright works available for re-use. These charges will be in accordance with the terms of the Re-use of Public Sector Information Regulations 2015, where they apply, or with regulations made under section 11B of the Freedom of Information Act, or with other statutory powers of the public authority.

If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

Written requests

Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.