Houghton Primary School

Working hard to achieve our best

Data Protection Policy and Privacy Notice

Date reviewed and adopted:	March 2023
Reviewed and adopted by:	Governors: Full Governing Body
Chair of governors	Sally Michaels
Headteacher	Andrew Spencer
Date of next review:	Spring 2025

Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

This policy complies with our funding agreement and articles of association.

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.
Sensitive 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 (such as fingerprints, retina and 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.

The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Data protection principles

The GDPR is based on data protection principles that 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.

Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

The data protection officer (DP)) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Mark Denny and he is contactable via mark.denny@majorseventh.co.uk

The headteacher acts as the representative of the data controller on a day-to-day basis.

Staff are responsible for:

- Collecting, storing and processing any 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, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not 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

Collecting personal data

Lawfulness, fairness and transparency

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 that 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**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Limitation, minimisation and accuracy

We 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 record retention schedule.

Sharing personal data

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 our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which 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.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their 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 the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

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

- Name of individual
- Correspondence address
- 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. mark.denny@majorseventh.co.uk

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. 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.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

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 another 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 tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

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.

Parental requests to see the educational record

Parents, or those with parental responsibility, do not have a legal right to access to their child's educational record (which includes most information about a pupil). If you wish to have access please put your request and reasons in writing to the Headteacher.

CCTV

We currently do not use CCTV at Houghton Primary School. If this changes at any point before this policy is reviewed, we will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we would make it clear where individuals are being recorded. Security cameras will be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about a CCTV system which is installed should be directed to the headteacher.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- 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 set out in relevant data protection law (see section 6)
- 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 members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, 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

15. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else 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.
- All staff who use a school computer/laptop work use the local authority's secure cloud based hosting system for SIMS, FMS, email and office documents (Central Hosting). This can only be accessed off-site using a key fob which is PIN and password protected. All documents which are created by staff must be saved within Central Hosting and not to the desk top or folders outside of the secure hosting system.

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment. 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.

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow these procedures;

Any individual that discovers a security data breach will report this immediately to the headteacher and data controller.

When an incident is raised, the headteacher will record the following information:

- Name of the individual who has raised the incident
- Description of the incident
- Description of any perceived impact
- Description and identification codes of any devices involved, e.g. school-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident

The school's data controller will take the lead in investigating the breach, and will be allocated the appropriate time and resources to conduct this.

The data controller, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or compromised.

The data controller will oversee a full investigation and produce a comprehensive report.

The cause of the breach, and whether or not it has been contained, will be identified – ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.

If the data controller determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

- In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access.
- The headteacher will issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in the E-safety Policy.
- In the event of any external or internal breach, the data controller will record this using an incident log and respond

appropriately, e.g. by updating the firewall, changing usernames and passwords, updating filtered websites or creating further back-ups of information.

- The data controller will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes.

Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups.

Where the security risk is high, the school will establish what steps need to be taken to prevent further data loss which will require support from various school departments and staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process.
- Taking systems offline.
- Retrieving any lost, stolen or otherwise unaccounted for data.
- Restricting access to systems entirely or to a small group.
- Backing up all existing data and storing it in a safe location.
- Reviewing basic security, including:
- Changing passwords and login details on electronic equipment.
- Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the data controller will inform the police of the security breach.

The data controller will test all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the school's systems are safe to use.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring arrangements

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed by the Finance, Personnel, Premises and Safety Committee of governors **every 2 years** and shared with the full governing body.

Next scheduled review: Spring term 2024

Privacy/fair processing notices

Privacy notice for pupils, parents/carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.

Houghton Primary School is the 'data controller' for the purposes of data protection law.

Our data protection officer is Ian Hoare (see 'Contact us' below).

Why we collect and use pupil information

We collect and use pupil information as defined by the General Data Protection Regulations May 2018 to complete and meet our responsibilities in the Public Interest for a PUBLIC TASK (Education). Where the data category is in **bold (Special Category Data)** we process data as it is of substantial public interest. The main pieces of legislation are:

- The Education Act (various years)
- The Education (Pupil Registration) (England) Regulations
- The School Standards and Framework Act 1998
- The School Admissions Regulations 2012
- Children and Families Act 2014
- The Special Educational Needs and Disability Regulations 2014
- General Data Protection Regulations 2018
- Data Protection Bill 2018

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Personal information (such as; name, unique pupil number, address, contact details, contact preferences, date of birth, identification documents)
- Personal information about a child's parents and/or other relatives (such as; name, contact details, relationship to child)
- Characteristics (such as; **ethnicity**, language, **religion**, nationality, country of birth, eligibility for free school meals, or special educational needs)
- Attendance information (such as; sessions attended, number of absences, reasons for absence)
- Assessment information (such as; results of internal assessments, teacher assessments and externally set tests)
- Pupil and curricular records
- Exclusion/behavioural information
- Relevant **medical information**, including physical and mental health and any injuries received
- Safeguarding information
- **Special Education Need** information (such as; Pupil Individual Plans, Education Health Care Plans)
- Details of any support received, including care packages, plans and support providers
- Images; these could be individual, group or on film (OPTIONAL by consent)

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care/support

- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Comply with the law regarding data sharing
- Comply with the law regarding health and safety
- Share data for statutory inspections and audit purposes

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a specified way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

In order to comply with the General Data Protection Regulation May 2018, and in line with the school's Data Protection Policy, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Data Protection Act 2018 (DPA 2018)

We hold (on your behalf) additional contacts 3 & 4 that we may use in an emergency, should we be unable to contact either parent/carer.

From you about other people:

If you provide information on behalf of anyone else, then in doing so you are confirming that you have explained how their information may be used by us and they have given you permission to do so**.** We will delete this information when you or they inform us and/or the child leaves the school.

How we store this data

We hold pupil data for varying lengths of time depending on what the information is and what other laws and safeguarding practices govern the duration we retain this information.

Typically pupil data is held for 7 years after the child reached Year 6. However, if you wish to know more, please contact the school to access the Information Audit Register detailing specific retention information and associated reasoning.

Data sharing

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 (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- *Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions*
- *The Department for Education - to meet our legal obligations to share certain information with it, such as safeguarding concerns, exclusions and pupil progress data*
- *The pupil's family and representatives – so they are aware of the progress that pupils are making, pastoral care they may receive, any additional support to meet a child's Special Educational Needs*
- *Educators and examining bodies*
- *Health authorities – to ensure the health, safety and wellbeing of a pupil*
- *Police forces, courts, tribunals – where this affects the safety and wellbeing of pupils*
- *Ofsted – Progress and attainment data about groups of children*
- *Agencies, professional services and other organisations we commission to deliver services on our behalf. We will write to you as and when new additional projects such as these arise. Privacy Notices and GDPR Compliance Statements from these agencies and organisations are obtained as part of the commissioning process. Agencies, professional services and other organisations may include;*
    - *Survey and research organisations – to ensure the attainment, progress, health and wellbeing of groups of pupils*
    - *Professional advisers and consultants – to ensure the attainment and progress of all children and different groups of children.*
    - *Charities and voluntary organisations - to ensure the attainment, progress, health and wellbeing of groups of pupils*
    - *Professional bodies - to ensure the attainment, progress, health and wellbeing of groups of pupils*
    - *Educational Resources Providers – Tapestry, Purple Mash, Mathletics, Accelerated reading, Cool Milk*

National Pupil Database

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to 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 our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases 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 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 the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: http://houghton.cambs.sch.uk/index.php/about-us/policies

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Parents and pupils' rights regarding personal data

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

To make a request for your personal information, or be given access to your child's educational record, contact the School Business Manager at office@houghton.cambs.sch.uk in the first instance. The school's Data Protection Officer is Mr Mark Denny and he can be contacted via the school by emailing mark.denny@majorseventh.co.uk

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer, Mark Denny via mark.denny@majorseventh.co.uk

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact;

- The headteacher via office@houghton.cambs.sch.uk
- our data protection officer, Mark Denny via mark.denny@majorseventh.co.uk

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.

Privacy notice for staff

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

Houghton Primary School is the 'data controller' for the purposes of data protection law.

Our data protection officer is Mark Denny (see 'Contact us' below).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Copy of passport
- Photographs
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning

- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our record retention schedule.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- *Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns*
- *The Department for Education – to track staff recruitment and retention*
- *Your family or representatives – in the event of an illness or injury*
- *Ofsted – to ensure the safeguarding of pupils*
- *Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll*
- *Our auditors – to ensure the compliance of our internal policies*
- *Trade unions and associations – to ensure the compliance of our internal policies*
- *Health authorities – to ensure the health and wellbeing of staff*
- *Security organisations – to ensure the health, safety and wellbeing of staff*

- *Professional bodies, advisers and consultants – to track progress and attainment for groups of pupils linked to performance management targets*
- *Police forces, courts, tribunals – to ensure the safeguarding of pupils and staff*

Transferring data internationally

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.

Your rights

How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

Mark Denny mark.denny@majorseventh.co.uk

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in this school.

Links with other policies

This policy may also be read in conjunction with:

Acceptable Use Code of Conduct

E-Safety