POLICY FOR DATA PROTECTION INCLUDING PRIVACY NOTICE

Document history

Date	**Description** [i.e. draft, consultation with staff, approval by Governors, review due]
June 2019	Approved by Governors
May 2021	Reviewed and Approved by Governors

Contents

1. Aims

Ivybridge Primary School is committed to protecting the rights and freedoms of data subjects (natural persons), the safe and secure processing of their data, in accordance with Data Protection Legislation.

Data Protection Lgislation means the Data Protection Act 2018 which incorporates the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the General Data Protection Regulation which is the governing legislation that regulates data protection across the EEA. This includes any replacement legislation coming into effect from time to time.

We hold personal data about our employees, governors, volunteers, pupils, pupil parents, suppliers and other individuals for a variety of business purposes. Our school aims to ensure that all data is collected, stored and processed in accordance with the Data Protection Legislation.

This policy sets out how we seek to protect personal data and ensure that our employees understand the rules governing their use of the Personal Data to which they have access in the course of their work.

In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that the relevant compliance steps are addressed.

Our school's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all employees share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

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

2. Legislation and guidance

This policy is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

It also takes into account the provisions of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR),.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll, medical, attendance, educational, safeguarding, and assessment purposes. Business purposes include the following: - Compliance with our legal, regulatory and corporate governance obligations and good practice - Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests - Ensuring school policies are adhered to (such as policies covering email and internet use) - Operational reasons, such as recording transactions, training and assessment, ensuring the confidentiality of sensitive information. - Investigating complaints - Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments - Monitoring staff conduct, disciplinary matters - Marketing our school - Improving services
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data we gather may include: individuals' name, date of birth, phone number, email address, first language, educational background, financial and pay details, National Insurance Number, details of certificates and diplomas, education and skills, marital status, nationality, job title,

	and CV.
Special categories of personal data	Data such as: • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Genetic or biometric information • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	'Processing' means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data subject	The person whose personal data is held or processed
Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

Data processor	'Processor' means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organization is the Information Commissioners Office.

4. Scope

This policy applies to all processing of personal data whether;

- Wholly or partly by automated means (i.e. by computer) or
- by other means (i.e. paper records) that form part of filing system or are intended to form part of a filing system.

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to Internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

Our school is responsible for determining how and why personal information relating to pupils, staff and visitors is processed, and, therefore, is a data controller.

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

As our Data Protection officer (DPO), The DPO Centre has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary. The school has appointed The DPO Centre Ltd to act as data protection officer. Contact details 50 Liverpool Street, London, EC2M 7PY, 020 3797 1289, hello@dpocentre.com.

5. Data protection principles

The purpose of this policy is to provide guidance on the data protection principles that all those acting on behalf of the school must adhere to when any personal data belonging to or provided by data subjects is collected, stored or transmitted.

It is therefore imperative that all those who access this policy comply with the Data Protection Principles, summarised below.

The GDPR is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly, lawfully and transparently
- Personal data shall be obtained only for one or more specified, explicit and lawful purposes
- Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which it is processed

- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data
- Accountability and transparency
- We must ensure accountability and transparency in all our use of personal data.
- Data protection legislation obliges all employees to take a proactive approach to data protection.
- In order to encourage best practice – and to avoid penalties from the Information Commissioner's Office.
- All employees are required to read this policy, to treat others' personal information with due care and consideration and to ensure that the school is able to demonstrate compliance.

6. Roles and responsibilities

The governing board has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Regulations.

Day-to-day responsibilities rest with the headteacher, or the deputy headteacher in the headteacher's absence. The headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

The data protection officer will conduct audits of the school's data processing activities to ensure compliance and act as a point of contact for the school, data subjects, parents and GDPR supervisory authorities such as the Information Commissioner's Office.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

7. Our Procedures

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased

Controlling vs. Processing data

Ivybridge Primary School is classified as a data controller. We must maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling data.

As a Data Controller, we must ensure any contracts and data sharing agreements with data processors comply with the current data protection regulations.

As a Data Controller, we must:

▪ Not use a sub-processor without a written data sharing agreement with the data processor

▪ Co-operate fully with the ICO or other supervisory authority

▪ Ensure the security of the data in our possession

▪ Keep accurate records of processing activities

▪ Notify our DPO of any incidents regarding personal data that could lead to a breach. If a breach is identified, we must inform the affected data subjects and the ICO.

If you are in any doubt about how we handle data, contact the DPO for clarification.

Lawful basis for processing data

We must establish a lawful basis for processing data.

Employees must ensure that any data they are responsible for managing or working with has a written lawful basis approved by the DPO.

At least one of the following conditions must apply whenever we process personal data:

1. Consent

   We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. Contract

   Processing is necessary to fulfil or prepare a contract for the individual.

3. Legal obligation

   Processing is necessary to meet a legal obligation (excluding a contract).

4. Vital interests

   Processing is necessary to protect a person's life or in a medical situation.

5. Public function

   Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. Legitimate interest

   Processing is necessary for the business/organisation's legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

As a school the personal data collected is due to legal obligation and due to the public function of education carried out by the school. The legal obligation to collect sensitive pupil data is set out in section 83 of The Children Act 1989 and section 537A of The Education Act 1996. The legal obligation to collect sensitive employee information is set out in section 114 of The Education Act 2005.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.

8. Special categories of personal data

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

▪ race

▪ ethnic origin

▪ politics

▪ religion

▪ trade union membership

▪ genetics

▪ biometrics (where used for ID purposes)

▪ health including SEND

▪ sexual orientation

In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

At school this information is legally required for census returns but data subjects are provided with the option to state they do not wish their information to be recorded.

Criminal record checks (DBS)

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such.

9. Responsibilities

School responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised
- Fully understand our data protection obligations
- Check that any data processing activities comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through our actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay to our DPO
- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly

- Researching third-party services, such as cloud services the company is considering using to store or process data
- Ensure privacy notices are supplied to data subjects at the time data is obtained

Responsibilities of the Data Protection Officer

- Keeping the school updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, governing body members and other stakeholders
- Responding to individuals such as pupils, parents and employees who wish to know which data is being held on them by us
- Support the school to ensure that third parties that handle the company's data have appropriate contracts or agreements regarding data processing
- Monitoring compliance with data protection legislation across the organisation

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Data security

We will ensure that personal data is kept secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

▪ In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it

▪ Printed data should be shredded when it is no longer needed

▪ Data stored on a computer should be protected by strong passwords that are changed regularly.

▪ Data stored on memory sticks and school staff laptops must be encrypted and password protected and locked away securely when they are not being used

▪ The DPO must approve any cloud used to store data

▪ Servers containing personal data must be kept in a secure location, away from general office space

▪ Data should be regularly backed up in line with the company's backup procedures

▪ Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

▪ All servers containing sensitive data must be approved and protected by security software

▪ All possible technical measures must be put in place to keep data secure

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was

obtained, but should be determined in a manner consistent with our data retention guidelines. A copy of our Retention schedule can be obtained on request from the DPO.

Transferring data internationally

There are restrictions on international transfers of personal data. The transfer of personal data abroad, or anywhere else outside of normal rules and procedures will not take place without express permission from the DPO.

10. Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

    ▪ Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.

    ▪ Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

    ▪ Enabling individuals to access their personal data and supplementary information

    ▪ Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

    ▪ We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.

    ▪ This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

4. Right to erasure

    ▪ We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

    ▪ We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.

    ▪ We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

    ▪ We must provide individuals with their data so that they can reuse it for their own purposes or across different services.

    ▪ We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

    ▪ We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.

    ▪ We must respect the right of an individual to object to direct marketing, including profiling.

    ▪ We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

    ▪ We must respect the rights of individuals in relation to automated decision making and profiling.

    ▪ Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

11. Privacy notice

When to supply a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which mean within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

Full Pupil, Staff, Governor and Visitor privacy notices can be viewed in the appendix to this policy.

11.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests

- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions
- CCTV footage

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

In addition, the School also uses CCTV cameras around the school site for security purposes and for the protection of staff and pupils. CCTV footage may be referred to during the course of disciplinary procedures (for staff or pupils) or investigate other issues. Please see our CCTV policy for more details.

11.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures
- Records of DBS checks
- CCTV footage

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the headteacher.

In addition, the School also uses CCTV cameras around the school site for security purposes and for the protection of staff and pupils. CCTV footage may be referred to during the course of disciplinary procedures (for staff or pupils) or investigate other issues. Please see our CCTV policy for more details.

11.3 Governors

We process data relating to those who are appointed governors at the school. The purpose of processing this data is to assist in the running of the school, including to:

- Facilitate safe appointment
- Support effective governance at the school

Governor personal data includes, but is not limited to, information such as:

- Contact details
- Records of DBS checks
- Statement of interests
- Contributions to meetings
- CCTV footage

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to publish certain information about governors on our school website and on the Get Information about Schools website.

Any governor wishing to see a copy of information about them that the school holds should contact the headteacher.

In addition, the School also uses CCTV cameras around the school site for security purposes and for the protection of staff and pupils. CCTV footage involving governors will only be processed to the extent that it is lawful to do so. Please see our CCTV policy for more details.

12. Subject access requests

Under the GDPR, pupils have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- The pupil's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests

- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child
- Information that could identify another individual who has not consented to their data being disclosed

Subject access requests will be provided within one month. In the case of the request being manifestly unfounded or excessive the school may charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

13. Parental requests to see the educational record

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil.

If parents ask for copies of information, they will be required to pay the cost of making the copies.

14. Storage and disposal of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Printed data should be shredded when it is no longer needed
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Personal information is not to be taken off site whether in paper or electronic formats, except on school residential activities where contact details are required. Secure, password protected, remote access is available to the school network for individual staff members working at home.
- 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.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up.
- Mobile devices such as school staff laptops and tablets are encrypted to prevent unauthorised access.
- Electronic data that is no longer required will be overwritten.
- Old hard drives will be securely and safely disposed of by an approved contractor.

- Information is retained for the periods recommended by the IRMS Information Management Toolkit for Schools (2016).

15. Right to erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

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

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.

- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

The checking of Free School Meal eligibility does do automated decision-making with the equivalent of legal effect, i.e. eligibility to claim free school meals and other additional funding for the school that the pupil attends. This is based upon DWP and DfE policy, therefore if a parent or guardian disagrees they should approach the school for an appeal or understanding of how the decision was based.

16. Training

Our staff and governors are provided with data protection training as part of their induction process, relevant to their role.

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

17. Monitoring arrangements

Monitoring

Everyone must observe this policy. Staff must notify the DPO of any breaches of this policy. Staff must comply with this policy fully and at all times.

The headteacher is responsible for monitoring and reviewing this policy with advice from the DPO.

The school business manager checks that the school complies with this policy by, among other things, reviewing school records and requesting that parents check their stored data is accurate annually.

This document will be reviewed when the General Data Protection Regulation comes into force, and then **every 2 years**.

At every review, the policy will be shared with the governing body.

Data audits

Annual data audits to manage and mitigate risks will be carried out. This includes information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. The school will conduct an annual data audit as defined by the DPO and normal procedures.

18. Third parties

Using third party controllers and processors

As a data controller, we must have written contracts in place with any third party data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR that the rights of data subjects will be respected and protected.

Contracts

Our contracts must comply with the GDPR contractual clauses and where applicable, the requirements set out by the ICO. Our contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.
At a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

19. Reporting Breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible to the DPO. This means as soon as staff have become aware of a breach. If in the opinion of the DPO the breach has caused a risk to the rights and freedoms of data subjects, the school has a legal obligation to report the data breach to the Information Commissioner's Office within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to our data security breach management policy for our complete reporting procedure.

20. Compliance

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

Questions about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Officer.

Any individual who considers that the Policy has not been followed in respect of Personal Data about themselves should also raise the matter with the Data Protection Officer.

Further information about the DPA and the GDPR can be found on the Information Commissioner's Office website **https://ico.org.uk/**

APPENDIX

IVYBRIDGE PRIMARY SCHOOL

Summerwood Road, Isleworth, Middlesex TW7 7QB
Telephone 020 8891 2727 Fax 020 8607 9112
Headteacher : Ms Caroline McKay

PRIVACY NOTICE FOR PUPILS/PARENTS - Data Protection Act 2018

We **IVYBRIDGE PRIMARY SCHOOL** are the Data Controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service.

The appointed Data Protection Officer is The DPO Centre Ltd, 50 Liverpool Street, London, EC2M 7PY, 020 3797 1289, hello@dpocentre.com.

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

- Personal information (such as name, date of birth, gender, unique pupil number, National Insurance number, contact numbers, email address, home address)
- Characteristics (such as ethnicity, language, nationality, country of birth, religion and free school meal eligibility)
- Special educational needs information
- Relevant medical information and dietary requirements
- Assessment information
- Attendance information (such as sessions attended, number of absences, previous school history and absence reasons)
- Child Protection records
- Closed circuit television footage
- Photographs (only with parent's consent and only ever accompanied by pupil's first name if any name used at all)

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 provide educational and administrative services through third parties
to assess the quality of our services
to comply with the law regarding data sharing
to apply for school funding
CCTV for site security
photographs used for in-school displays and website news

The lawful basis on which we use this information

We collect and use pupil information under article 6 (1) (c) – legal obligation, (e) – public interest, and article 9 (2) (j) – public interest and statistical purposes, of the General Data Protection Regulations as specified in article 537A of the Education Act 1996 and section 83 of The Children Act 1989.

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 Data Protection Regulations, 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 only as long as is recommended by the IRMS Information Management Toolkit for Schools (2016). All personal data is disposed of securely.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- NHS
- Third party online payments administrator
- Data backup provider
- Educational resource providers (maths packages, reading)
- Administrative service providers (text to parents, school milk providers, free meal eligibility checkers)
- Assessment trackers
- Pupil survey providers
- Pupil welfare services

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 (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.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)

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: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

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

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the headteacher in writing.

You also have the right to:

- object to processing of personal data that is likely to cause, or is 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 are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can 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 the headteacher.

IVYBRIDGE PRIMARY SCHOOL

Summerwood Road, Isleworth, Middlesex TW7 7QB
Telephone 020 8891 2727 Fax 020 8607 9112
Headteacher : Ms Caroline McKay

PRIVACY NOTICE
School Workforce: those employed or otherwise engaged to work at a school or the Local Authority

Privacy Notice - Data Protection Act 2018

We **IVYBRIDGE PRIMARY SCHOOL** are the Data Controller for the purposes of the Data Protection Act.

The appointed Data Protection Officer is The DPO Centre Ltd, 50 Liverpool Street, London, EC2M 7PY, 020 3797 1289, hello@dpocentre.com.

Personal data is held by the school about those employed or otherwise engaged to work at the school or Local Authority. This is to assist in the smooth running of the school and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector;
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- Informing the development of recruitment and retention policies;
- Demonstrating safer recruitment practices
- Ensuring the health and safety of employees
- Support the effective performance management of staff
- Allowing better financial modelling and planning;
- Enabling ethnicity and disability monitoring; and
- Supporting the work of the School Teacher Review Body and the School Support Staff Negotiating Body.

This personal data includes some or all of the following - identifiers such as name, National Insurance Number, date of birth, address, telephone number, next of kin details, relevant medical information, records of DBS checks, CCTV footage, characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information.

We will not give information about you to anyone outside the school or Local Authority (LA) without your consent unless the law and our rules allow us to.

We share staff information with:

- Our staff absence insurance provider
- Our human resources consultant
- Our occupational health provider
- Our internet services provider
- Third party online payments administrator
- Data backup provider
- Educational resource providers (maths packages, reading)

We are required by law to pass on some of this data to:

- the LA
- the Department for Education (DfE)
- the Disclosure and Barring Service

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the headteacher.

In addition the school also uses CCTV cameras around the school site for security purposes and for the protection of staff and pupils. CCTV footage may be referred to during the course of disciplinary procedures (for staff or pupils) or to investigate other issues. CCTV footage involving governors will only be processed to the extent that it is lawful to do so. Please see our CCTV policy for more details.

If you require more information about how the LA and/or DfE store and use this data please go to the following websites:

- https://www.hounslow.gov.uk/info/20110/open_data_and_information_requests/1368/privacy_notice/1

If you are unable to access these websites, please contact the LA or DfE as follows:

Data Protection Officer Children's Services and Lifelong Learning London Borough of Hounslow Hounslow House 7 Bath Road Hounslow MIDDX TW3 3EB Email: csll-communications@hounslow.gov.uk Tel: 0208 583 2641	Public Communications Unit Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT Website: www.education.gov.uk Email: info@education.gsi.gov.uk Telephone: 0870 000 2288

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

.

IVYBRIDGE PRIMARY SCHOOL

Summerwood Road, Isleworth, Middlesex TW7 7QB
Telephone 020 8891 2727 Fax 020 8607 9112
Headteacher : Ms Caroline McKay

PRIVACY NOTICE
School Governors - Data Protection Act 2018

We **IVYBRIDGE PRIMARY SCHOOL** are the Data Controller for the purposes of the Data Protection Act.

The appointed Data Protection Officer is The DPO Centre Ltd, 50 Liverpool Street, London, EC2M 7PY, 020 3797 1289, hello@dpocentre.com.

Personal data is held by the school about those appointed to be governors at the school. This information is collected for the following reasons:

- Facilitate safe appointment
- Providing information on our website about our governors and on the Get Information about Schools website
- Support effective governance at the school

Governor personal data includes, but is not limited to, information such as:

- Contact details – name, address, telephone numbers, email address
- Records of DBS checks
- Statement of interests
- Contributions to meetings
- Identification photograph
- CCTV footage

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about governors with third parties without consent unless the law allows us to.

We are required, by law, to publish certain information about governors on our school website and on the Get Information about Schools website.

Any governor wishing to see a copy of information about them that the school holds should contact the headteacher.

In addition, the school also uses CCTV cameras around the school site for security purposes and for the protection of staff and pupils. CCTV footage involving governors will only be processed to the extent that it is lawful to do so. Please see our CCTV policy for more details.

We will not give information about you to anyone outside the school or Local Authority (LA) without your consent unless the law and our rules allow us to.

We share governor information with:

- Data backup provider
- The Local Authority
- The Department for Education
- The Disclosure and Barring Service
- Our human resources consultant

We are required by law to pass on some of this data to:

- the LA
- the Department for Education (DfE)
- the Disclosure and Barring Service

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

IVYBRIDGE PRIMARY SCHOOL

Summerwood Road, Isleworth, Middlesex TW7 7QB
Telephone 020 8891 2727 Fax 020 8607 9112
Headteacher : Ms Caroline McKay

PRIVACY NOTICE
School volunteers, placement students, coaches, other visitors - Data Protection Act 2018

We **IVYBRIDGE PRIMARY SCHOOL** are the Data Controller for the purposes of the Data Protection Act.

The appointed Data Protection Officer is The DPO Centre Ltd, 50 Liverpool Street, London, EC2M 7PY, 020 3797 1289, hello@dpocentre.com.

Personal data is held by the school about those who visit the school. This information is collected for the following reasons:

- Record of the time visitors enter and leave school for fire safety purposes
- Safeguarding of pupils
- Communication and identification purposes

The amount of personal data collected will depend on the type of visitor. This could include information such as:

- Contact details – name, date of birth, organization, address, telephone numbers, email address
- Emergency contact details
- Records of DBS checks
- Identification photograph
- CCTV footage

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

In addition, the school also uses CCTV cameras around the school site for security purposes and for the protection of staff and pupils. CCTV footage involving visitors will only be processed to the extent that it is lawful to do so. Please see our CCTV policy for more details.

We will not give information about you to anyone outside the school or Local Authority (LA) without your consent unless the law and our rules allow us to.

We do not share visitor information with third parties, unless compelled under the law.

Any visitor wishing to see a copy of information about them that the school holds should contact the headteacher.

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