



# Hemingford Grey

## SCHOOL

<p><b>Data Protection Policy, Subject Access Requests and Personal Data Breach Procedure</b></p>
----------------------------------------------------------------------------------------------------------

Policy was reviewed	April 2020
---------------------	------------

This Policy has been adapted from a Judicium model template from September 2018 and a model template from the School's DPO at The ICT Service from December 2018.

## **DATA PROTECTION POLICY**

### **Introduction**

The General Data Protection Regulation (GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

### **SECTION 1 - DEFINITIONS**

#### **Personal Data**

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data, but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

#### **Special Category Data (Please see Appendix 1)**

Previously termed "Sensitive Personal Data", Special Category Data identified under article 9 of the GDPR is similar by definition and refers to data concerning an individual Data

Subject's racial or ethnic origin, political or religious or philosophical beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

### **Data Subject**

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

### **Data Controller**

The organisation storing and controlling such information (i.e. the School) is referred to as the Data Controller.

### **Data Processor**

An individual or other body who processes personal data on behalf of the data controller

### **Processing**

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

### **Automated Processing**

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

### **Data Protection Impact Assessment (DPIA)**

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

### **Criminal Records Information**

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures and could include DBS checks.

## **SECTION 2 - WHEN CAN THE SCHOOL PROCESS PERSONAL DATA**

### **Data Protection Principles**

The School is responsible for and adhere to the principles relating to the processing of personal data as set out in the GDPR.

The principles the School must adhere to are: -

- (1) Personal data must be processed lawfully, fairly and in a transparent manner;
- (2) Personal data must be collected only for specified, explicit and legitimate purposes;
- (3) Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- (4) Personal data must be accurate and, where necessary, kept up to date;
- (5) Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed; and
- (6) Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Further details on each of the above principles is set out below.

**Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner**

The School only collect, process and share personal data fairly and lawfully and for specified purposes. The School must have a specified purpose for processing personal data and special category of data as set out in the GDPR.

Before the processing starts for the first time we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data

The School may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law; or
- For the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

### Special Category Data

The School may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with a disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health; or
- The processing is necessary for archiving, statistical or research purposes.

The School identifies and documents the legal grounds being relied upon for each processing activity.

### Consent

Where the School relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the School will normally seek another legal basis to process that data. However if explicit consent is required the data subject will be provided with full information in order to provide explicit consent.

The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

**Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes**

Personal data will not be processed in any manner that is incompatible with the legitimate purposes.

The School will not use personal data for new, different or incompatible purposes from that disclosed when the data was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

**Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed**

The School will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the School shall delete or anonymise the data. Please refer to the School's Data Retention Policy for further guidance.

**Principle 4: Personal data must be accurate and, where necessary, kept up to date**

The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the School.

**Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed**

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The School will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the School's Data Retention Policy for further details about how the School retains and removes data.

**Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage**

In order to assure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the School replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles; and
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The School follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

**Sharing Personal Data**

The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

- Has a need to know the information for the purposes of providing the contracted services;
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the Local Authority, Ofsted or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our School shall be clearly defined within written notifications and details and basis for sharing that data given.

### **Transfer of Data Outside the European Economic Area (EEA)**

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

The School will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the GDPR. All staff must comply with the School's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

### **SECTION 3 - DATA SUBJECT'S RIGHTS AND REQUESTS**

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the School handle their personal data are set out below: -

- (a) (Where consent is relied upon as a condition of processing) to withdraw consent to processing at any time;
- (b) Receive certain information about the School's processing activities;
- (c) Request access to their personal data that we hold;
- (d) Prevent our use of their personal data for marketing purposes;
- (e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- (f) Restrict processing in specific circumstances;
- (g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- (h) Request a copy of an agreement under which personal data is transferred outside of the EEA;
- (i) Object to decisions based solely on automated processing;



- (j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- (k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- (l) Make a complaint to the supervisory authority; and
- (m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the School to verify the identity of the individual making the request.

### **Subject Access Requests (SAR)**

A Data Subject has the right to be informed by the School of the following: -

- (a) Confirmation that their data is being processed;
- (b) Access to their personal data;
- (c) A description of the information that is being processed;
- (d) The purpose for which the information is being processed;
- (e) The recipients/class of recipients to whom that information is or may be disclosed;
- (f) Details of the School's sources of information obtained; and
- (g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct.
- (h) Other supplementary information

Any Data Subject who wishes to obtain the above information must notify the School in writing of his or her request. This is known as a Data Subject Access Request.

The request should in the first instance be sent to the Headteacher.

### **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 13 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.

### **Direct Marketing**

The School are subject to certain rules and privacy laws when marketing. For example a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The School will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

### **Employee Obligations**

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the School in the course of their employment or engagement. If so, the School expects those employees to help meet the School's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction. Please refer to the Electronic Communication and Acceptable Use Policy for further details about our security processes).
- Not to remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information; and
- Not to store personal information on local drives.

## **SECTION 4 - ACCOUNTABILITY**

The School will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the GDPR principles.

The School have taken the following steps to ensure and document GDPR compliance: -

### **Data Protection Officer (DPO)**

Please find below details of the School's Data Protection Officer: -

Donna Flynn at The ICT Service.

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

-

- (a) If you are unsure of the lawful basis being relied on by the School to process personal data;
- (b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);
- (c) If you need to draft privacy notices or fair processing notices;
- (d) If you are unsure about the retention periods for the personal data being processed but would refer you to the School's data retention policy in the first instance;
- (e) If you are unsure about what security measures need to be put in place to protect personal data;
- (f) If there has been a personal data breach and would refer you to the procedure set out in the School's breach notification policy;
- (g) If you are unsure on what basis to transfer personal data outside the EEA;
- (h) If you need any assistance dealing with any rights invoked by a data subject;
- (i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
- (j) If you plan to undertake any activities involving automated processing or automated decision making;
- (k) If you need help complying with applicable law when carrying out direct marketing activities; or
- (l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

## Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will alert the Headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system.

- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

### **Actions to minimise the impact of data breaches**

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

### **Sensitive information being disclosed via email (including safeguarding records)**

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

## **Transparency and Privacy Notices**

The School will provide detailed, specific information to data subjects. This information will be provided through the School's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how the School use their data and the School's privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the GDPR including the identity of the data protection officer, the School's contact details, how and why we will use, process, disclose, protect and retain personal data. This will be provided in our privacy notice.

When personal data is collected indirectly (for example from a third party or publically available source), we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the GDPR

## **Privacy by Design**

The School adopt a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the School takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

## **Data Protection Impact Assessments (DPIAs)**

In order to achieve a privacy by design approach, the School conduct DPIAs for any new technologies or programmes being used by the School which could affect the processing of personal data. In any event the School carries out DPIAs when required by the GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data; or
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).



Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

## **Record Keeping**

The School is required to keep full and accurate records of our data processing activities. These records include: -

- The name and contact details of the School;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the School's processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

## **Training**

The School will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

## **Audit**

The School will test our data systems and processes in order to assess compliance. These are done through data audits which take place regularly in order to review use of personal data.

## **Related Policies**

Staff should refer to the following policies that are related to this data protection policy: -

Privacy Notices

Data Retention Schedule

## **Appendix 1**

### **Special Categories of Data Policy**

Special Categories of data is defined under article 9 of the GDPR as;

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life.

To process such data, a legal reason for processing must be identified.

The type data which we process at Hemingford Grey Primary School that falls in to this category and the legal reasons for processing it is identified below:

Type of Data	Legal reason for processing	Used for
Racial	Article 9(2)(d) Substantial Public Interest	School Census
Ethnic	Article 9(2)(d) Substantial Public Interest	School Census
Religious	Article 9(2)(d) Substantial Public Interest	School Census
Trade Union?	(Article 9(2)(b) Obligations and exercising rights of employer for fundamental rights of data subject	Equality Legislation
Biometric (Fingerprint)	Explicit Consent	Library identification
Health	Article 9(2)(d) Substantial Public Interest	Safeguarding of children

When processing this data, we will ensure that we will adhere to the following principles:

Lawful, fair and transparent. We have identified or legal reasons for processing above and have shared them with you in the privacy notice.

We will only use this data for the purposes identified above.

We will only collect the minimum amount of data that is required for this purpose.

We will ensure by regularly asking you to check this data is correct that it kept up to date and ask you to inform us of any data that needs to be rectified or erased as no longer relevant.

We will only keep this data for as long as is necessary. Please see our data retention schedule linked to the privacy notice for how long we retain this data.

We will process this data using all appropriate means to ensure the security of this data.

## **Pupils**

### **Article 6**

#### **Public Interest**

The vast majority of the data we process is because we need it to be able to perform the function of being a school. As a school it is necessary that we hold this information to perform our public task.

e.g. We need to know your son/ daughters name and parental contact details as well as any medical conditions to be able to provide the appropriate care for them whilst at school.

#### **Consent**

Where we rely upon consent we will ask you to be able to process that data.

e.g. We ask for your permission to use photographs of your child in the school, on the school website, in press articles etc.

When you have given consent, you are able to withdraw it any time. Please contact us in writing to inform us.

#### **Vital Interest**

If there was a medical emergency where we couldn't get in contact with you and it was in the Vital Interest that we shared the medical information for the child with a Doctor/ Ambulance Crew etc.

#### **Legal Obligation**

If we are required to process this information because we have a legal obligation to do so.

e.g. We have to submit a School Census to the DfE 3 times a year.

### **Article 9**

#### **Special Categories of Data**

We also collect racial, ethnicity, religion and medical condition(s) data. This data is determined to be a special category of data.

#### **Public Interest**

The Special Categories of Data processed by is also undertaken in the public interest; we have to collect it by law. For certain categories of data such as ethnicity/ religion you have the right to refuse to give it to us but we are required to record that it has been refused.

#### **Vital Interest**

If there was a medical emergency where we couldn't get in contact with you and it was in the Vital Interest that we shared the medical information for the child with a Doctor/ Ambulance Crew etc.

## **Staff**

### **Article 6**

#### **Performance of a Contract**

We collect your information so that we can enter in to a contract. We need to know you bank details, National Insurance number etc. to be able to pay you.

#### **Legal Obligation**

The data we collect on you may also be processed because we have a legal obligation to.

e.g. we need to share your information with Government because we must undertake a School Workforce Census

#### **Vital Interest**

If there was a medical emergency was in the Vital Interest that we shared the medical information for the child with a Doctor/ Ambulance Crew etc.

### **Article 9**

#### **Special Categories of Data**

We also collect sexual orientation racial, ethnicity, religion and medical condition(s) data. This data is determined to be a special category of data.

#### **Obligations in the field of Employment Law**

We need to process this to ensure we comply with Equalities Legislation.

#### **Purposes of Preventive or Occupational Medicine**

We may process data if required to assess the working capacity of the employee.

#### **Vital Interest**

If there was a medical emergency and it was in the Vital Interest that we shared the medical information for the child with a Doctor/ Ambulance Crew etc.