



# DATA PROTECTION POLICY

**Statutory Policy**  
Adopted: Autumn 2020  
Adopted by the Governing Body: Autumn 2020  
To be reviewed: Autumn 2023

## Vision Phrase

'Aim high and smile'

If you would like to discuss anything in this privacy notice, please contact:

Data Protection Officer: **James England**

Telephone: 0800 0862018

Email: [dpo@dataprotection.education](mailto:dpo@dataprotection.education)

We are committed to safeguarding and ensuring the health, safety and well-being of all pupils in accordance with safeguarding procedures and guidance for staff outlined in the school's Health and Safety, Child Protection, Security and Safeguarding policies.



# Document version Control

Version	Author	Date	Approved by	Effective from
1.1	DPE - JE	1/5/2018	WHIS: WH	25/05/18
1.2	DPE - TK	2/5/2018	WHIS: WH	25/05/18
1.3	DPE - TK	7/9/2020	WHIS: WH	07/10/20

# Contents

Scope .....	4
Definitions .....	4
<b>COMMITMENT TO GDPR AND DATA PROTECTION BY DESIGN.....</b>	<b>7</b>
Data Principles.....	7
Data Subject’s Rights .....	8
Lawful processing .....	8
Information Commissioner’s Office .....	9
Data Sharing .....	9
<b>FAIR AND TRANSPARENT PROCESSING OF DATA</b>	
<b>LAWFUL PROCESSING OF DATA</b>	
<b>SPECIAL CATEGORY DATA</b>	
<b>CONSENT</b>	
<b>DISCLOSURE AND SHARING OF PERSONAL INFORMATION</b>	
Data Breaches .....	12
Subject Access Requests .....	16
Dealing with a subject access request (SAR).....	16
Data Protection Officer .....	18
Data Security .....	19
Photography and Videos.....	20
CCTV .....	20
Fob system at CR.....	21
Retention Policy.....	21
Training.....	21
Data Processors.....	21

# Introduction

## Scope

This policy reflects West Hove Infant Schools commitment to the General Data Protection Regulation (GDPR) and the expected provision of the 2018 Data Protection Act (DPA), as of May 1<sup>st</sup> 2018 passing through parliament as the Data Protection Bill.

This policy covers the processing of personal data wholly or partly by automated means and the processing (other than by automated means) of personal data which form part of a filing system or are intended to form part of a filing system.

## Definitions

### As defined by the GDPR:

- **personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is a person 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 by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **restriction of processing** means the marking of stored personal data with the aim of limiting their processing in the future;
- **profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- **pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- **filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

- **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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing
- **third party** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- **consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- **genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- **biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- **data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- **enterprise** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- **supervisory authority** means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR;
- **cross-border processing** means either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;
- **relevant and reasoned objection** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
- **information society service** means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;
- **international organisation** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
- **special categories** of personal data means personal data:
  - revealing racial or ethnic origin,
  - revealing political opinions,
  - revealing religious or philosophical beliefs or trade union membership,
  - 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 or sexual orientation shall be prohibited;
- **data breach**: an incident or event in which personal and/or confidential data:
  - has potentially been viewed or used by an individual unauthorised to do so;
  - has had its integrity compromised;
  - is lost or is unavailable for a significant period

# Commitment to GDPR and Data Protection by Design

This policy sets out West Hove Infant School's commitment to GDPR and the implementation of a data protection by design approach. West Hove will refer to documents and guidance from the Information Commissioner's Office and the Department for Education in relation to GDPR and data processing. This includes ensuring by May 25<sup>th</sup> 2018 and beyond:

- Creation and maintenance of a data protection working group;
- Assigning responsibility to an individual within The Organisation;
- Assigning a Data Protection Officer;
- Development and maintenance of a GDPR project;
- Ensuring that all staff are trained in data protection and take responsibility for the collection, processing, storage and destruction of data;
- A lawful basis for processing is documented for all processing activity;
- Principles relating to processing of personal data are adhered to;
- The rights of data subjects are respected;
- Risks to the rights of data subjects are assessed and mitigated for all large-scale and new processing;
- Regular independent reviews of processing activity and processing documentation are carried out;
- Organisational and technical measures are implemented to protect data;
- Data breaches impacting on the rights and freedoms of data subjects will be reported to the Information Commissioner's Office (ICO).

## Data Principles

West Hove Infant School is committed to the principles relating to processing of personal data, in that personal data will be:

- **processed lawfully, fairly and in a transparent manner** in relation to the data subject;
- **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
- **accurate and, where necessary, kept up to date;**

- kept in a form which permits identification of data subjects for no longer than is necessary;
- processed in a manner that ensures appropriate security of the personal data

## Data Subject's Rights

West Hove Infant School supports the rights of data subjects (or the parents/carers of data subjects where data subjects are not able to demonstrate the capacity to understand their rights) in relation to data that is processed or stored about them, as follows:

- Right to fair and transparent processing;
- Right of access;
- Right of rectification;
- Right to erasure (the "right to be forgotten");
- The right to restrict processing;
- Right to be notified of erasure, rectification or restriction;
- Right of data portability;
- Right to object to processing;
- Right to object to processing for the purposes of direct marketing;
- Right to object to processing for scientific, historical or statistical purposes;
- Right to not be evaluated on the basis of automated processing;
- Right to withdraw consent at any time;
- Right to be notified about a data breach;
- Right to an effective judicial remedy against a supervisory authority;
- Right to lodge a complaint with supervisory authority;
- Right to an effective judicial remedy against a controller or processor;
- Right to compensation.

West Hove Infant School shall maintain procedures, policies and notices to ensure that data subjects are informed about their rights.

## Lawful processing

We will only process personal data where a lawful basis for processing exists. Specifically, where:

- the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

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

Special categories of personal data will not be processed unless a specific lawful basis listed in Article 9 of the GDPR applies.

## Information Commissioner's Office

For the purposes of data protection, West Hove Infant School is a data controller; responsible for the determination of the purposes and means of the processing of personal data and where the purposes and means of such processing takes place. As such, West Hove Infant School is supervised by the Information Commissioner's Officer and will pay the data protection fee required by law.

The Data Protection Officer will be the principal point of contact with the Information Commissioner's Office.

## Data Sharing

### FAIR AND TRANSPARENT PROCESSING OF DATA

Data will be shared with third parties only where a lawful basis exists.

Where data is shared with third-party processors, they will only process data with the explicit instructions (either contractual or through a data sharing agreement) of West Hove Infant School and shall not hold or process the data for any other purpose. The minimum data required for the processing task will be provided for the processing. Any third-party processors, where contracts or data sharing agreements are required for the processing to take place will be required to provide evidence of their commitment to GDPR compliance.

Where we have a legal obligation to share information with law enforcement, agencies and government bodies for legitimate purposes relating to criminal justice and taxation we will do so.

We will share information if there is an issue that jeopardises the safety or security of staff, students of school visitors.

Data may be shared for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In this case, efforts will be made to ensure the minimum data required is shared and if possible, anonymised prior to sharing.

Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed fairly, data subjects must and will be made aware of the following in our privacy notices or requests to process data:

- That the personal data is being processed;
- Why the personal data is being processed;
- What the lawful basis is for that processing (see below);
- Whether the personal data will be shared, and if so with whom;
- The period for which the personal data will be held;
- The existence of the data subject's rights in relation to the processing of that personal data; and
- The right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

The organisation will only process data that is **necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any processing.**

Data collected for the purposes of public health (including visitor contact data for COVID-19) will be kept as long as required. Contact data for visitors will be kept for 21 days after the most recent visit, with information on visitors kept as per standard retention requirements. Public Health data may be shared with third-parties as required including, but not limited to:

- National Health Service (including NHS Test and Trace)
- Public Health England
- Other local health authorities

Data collected and processed for public health purposes is done so under GDPR [Article 9\(2\)\(i\)](#) which states: (in part) "processing is necessary for reasons of [public interest](#) in the area of public health, such as protecting against serious cross-border threats to health..." and [Recital 54](#) which includes: "The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject."

As more information is available from local authorities, DfE and Public Health England, we will be updating this section with data protection related content.

Data collected for the purposes of public health (including visitor contact data for COVID-19) will be kept as long as required. Contact data for visitors will be kept for 21 days after the most recent visit, with information on visitors kept as per standard retention requirements. Public Health data may be shared with third-parties as required including, but not limited to:

- National Health Service (including NHS Test and Trace)
- Public Health England
- Other local health authorities

Data collected and processed for public health purposes is done so under GDPR [Article 9\(2\)\(i\)](#) which states: (in part) "processing is necessary for reasons of [public interest](#) in the area of public health, such as protecting against serious cross-border threats to health..." and [Recital 54](#) which includes: "The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject."

Collection and processing of visitor data will be documented in the privacy notices and in a statement available to visitors at the time of data collection to include the following information:

"We collect the following visitor information for the purposes of security, safety and public health:

- Name
- Organisation
- Date and time of visit
- Contact details

These are kept for six years in case of any claims by students, staff or visitors under the Limitations Act (1980).

Contact details will be deleted after 21 days.

Should a positive test for COVID-19 be identified, relevant visitor data will be shared with the required public health authorities.

For further details, please see the Data Protection Policy, or contact the Data Protection Officer"

In addition to the updated statements for the collection of track and trace data included in our Privacy Policy. We are also referring users requiring more resources on the collection of user data for Covid-19 to the NHS Test and Trace "Customer Logging Toolkit":

<https://coronavirusresources.phe.gov.uk/Test-and-Trace/resources/customer-logging-toolkit/>

## LAWFUL PROCESSING OF DATA

For personal data to be processed lawfully it must be processed on the basis on one of the legal grounds set out in the DATA Protection Legislation. The organisation will only process personal data where a lawful basis for processing exists. Specifically, where:

- The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a **legal obligation** to which the controller is subject (e.g the Education Act 2011);
- Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
- Processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller

## SPECIAL CATEGORY DATA

This is data relating to **health; race; sexuality; religion; criminal offences; political opinions and union memberships.**

These special categories of personal data relating to will not be processed unless a specific lawful basis as listed in Article 9 of the GDPR applies. When this special category data is being processed we will normally only do so under the following legal grounds:

- Where the processing is **necessary for employment law** purposes, for example in relation to sickness absence;
- Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- Where the processing is necessary for **health or social care purposes**, for example in relation to pupils with medical conditions or disabilities; and
- **Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data**

## CONSENT

There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

When pupils, staff or our Workforce join the Organisation where appropriate a consent form will be required to be completed in relation to them. This consent form deals with:

In relation to all pupils under the age of 12 years old we will seek consent from an individual with parental responsibility for that pupil.

We will generally only seek consent directly from a pupil if they are legally able to give such consent. The legal age for consent under Data Protection legislation is 12. However we recognise that this may not be appropriate in certain circumstances and therefore the organisation may be required to seek consent from an individual with parental responsibility.

If consent is required for the processing of personal data of any data subject then the form of this consent must:

- Inform the data subject of exactly what we intend to do with their personal data;
- Require them to positively confirm that they consent (we cannot ask them to opt-out rather than opt-in); and
- Inform the data subject of how they can withdraw their consent.

Any **consent must be freely given**, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

The DPO must always be consulted in relation to any consent form before consent is obtained.

A record must always be kept of any consent, including how it was obtained and when.

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include safeguarding, child protection and medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur. Please refer to the organisation Safeguarding Policy, Child Protection Policy and organisation Medical Policy for further information.

## DISCLOSURE AND SHARING OF PERSONAL INFORMATION

We may share personal data that we hold about data subjects, with other organisations, without consent, where we have a lawful basis for doing so. Such organisations include the Department for Education and Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other organisations, and other organisations where we have a lawful basis for doing so.

The organisation will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

Further detail is provided in our Record of Processing Activities.

### Data Breaches

In the case of a personal data breach, West Hove Infant School shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the Information Commissioner's Office is not made within 72 hours, it shall be accompanied by reasons for the delay.

In order to evaluate the personal data breach West Hove Infant School shall inform and involve the Data Protection Officer in the assessment of the breach and in the execution of the data breach procedure to contain and manage the breach.

The notification shall at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

- Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

West Hove Infant School shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in a data breach log. The log shall enable the Information Commissioner's Officer to verify compliance with the data breach rules and raise awareness of minor breaches that may assist in the identification of new data handling processes and training requirements.

### **Examples of data breaches**

- Loss or theft of paper records or loss or theft of equipment on which data is stored e.g. a laptop, mobile phone, tablet device or memory stick;
- A letter or email containing personal and/or confidential data sent to the wrong address (including internal staff or third parties) or an email to an unauthorised group of email boxes;
- Personal data disclosed orally in error in a meeting or over the phone – including "blogging" where information is obtained by deceiving West Hove Infant School, or where information has been disclosed without confirming the true identity of the requester;
- Unauthorised access to information classified as personal or confidential e.g. attaching documents to an outlook diary appointment that is openly accessible;
- Posting information on the world wide web or on a computer otherwise accessible from the Internet without proper information security precautions;
- Sensitive information left on a photo-copier or on a desk in County Council premises;
- Unauthorised alteration or deletion of information;
- Not storing personal and confidential information securely;
- Not ensuring the proper transfer or destruction of files after closure of offices/buildings e.g. not following building decommissioning procedures;
- Failure to safeguard/remove personal data on office equipment (including computers and smart phones) before disposal/sale.

### **Breaches caused by IT Security Incidents**

Examples:

- Unauthorised access to IT systems because of misconfigured and/or inappropriate access controls;
- Hacking or phishing attacks and related suspicious activity;
- Virus or malware attacks and related suspicious activity;
- ICT infrastructure-generated suspicious activity;
- Divulging a password to another user without authority.

## Subject Access Requests

West Hove Infant School is committed to:

- Ensuring that individuals' rights to their own personal information can be appropriately exercised;
- Providing adequate training for staff to recognise and handle subject access requests;
- Ensuring that everyone handling personal information knows where to find further guidance on individuals' rights in relation to their own personal information;
- Ensuring that queries about individuals' rights to their own personal information are dealt with effectively and promptly;
- Being fair and transparent in dealing with a subject access request;
- Logging all subject access requests to assist the Information Commissioner's Office with any complaints related to subject access as well as identifying any issues that may assist in the identification of new data handling processes and training requirements.

All staff are responsible for ensuring that any request for information they receive is dealt with in line with the requirements of the GDPR and in compliance with this policy.

All staff have a responsibility to recognise a request for information and ensure it is passed to the responsible member of staff and/or the Data Protection Officer within two working days.

If a parent/carer requests a copy of their child's education record, we will include:

- School reports
- Attendance records
- Phonic check score (Y1)
- SATs results (Y2)
- Progress data

## Dealing with a subject access request (SAR)

What must I do?	Why?	How?
Be clear about the nature of the request and identify what information is being requested.	Being clear about the nature of the request will enable you to decide whether the request needs to be dealt with in accordance with statutory requirements, who needs to deal with the request, and/or whether this is business as usual (BAU). If needed ask the submitter	Review the request and identify: If the request is for the personal information of the requester or made by an individual on behalf of another person (e.g. on behalf of a child or an adult lacking capacity) – this is a subject access request; If the request is for non-personal

What must I do?	Why?	How?
	of the request for clarity.	<p>information – this may be dealt with as BAU or formally under the Freedom of Information Act 2000 (the FOIA) or the Environmental Information Regulations 2004 (the EIR).</p> <p>NB: The request can be received in a range of different formats e.g. letter, email, a completed form, or can be made via social media (e.g. a Facebook page or Twitter account).</p>
<p>If the request is a SAR the request must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two working days of receipt of the request.</p>	<p>The GDPR stipulates that SARs must be completed within one month of the request – but in reality as soon as possible.</p>	<p>Log the SAR in the subject access request log and inform all appropriate staff required to deal with the request.</p>
<p>If the information requested is for non-personal information i.e. is organisational or statistical information, this will fall under the FOIA or EIR, or BAU and will be dealt with, as follows:-</p> <p>All non-routine FOIA or EIR requests must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two working days of receipt of the request.</p>	<p>The FOIA and EIR stipulates that requests must be completed within 20 working days of the request – therefore the more swiftly request are being dealt with, the more likely West Hove Infant School will meet its statutory deadlines.</p> <p>BAU requests need to be dealt with by an individual in that particular service area who can identify and locate the information requested and provide a response within a reasonable timeframe.</p>	<p>If the request is for non-routine/FOIA/EIR information contact the responsible member of staff (usually the Headteacher) and the Data Protection Officer.</p>
<p>If the information requested is for the personal information of an individual for use in a criminal investigation by the police, or any other agency investigating criminal offences, this will fall under either the regulatory Investigative Powers Act 2000 (RIPA) or Data Protection Act 2018.</p> <p>The request can be for either hard copy or any type of electronic information including email traffic ie the time and information that an email is sent.</p> <p>The request must be forwarded to</p>	<p>It is in the public interest that requests are identified and dealt with as quickly as possible.</p>	<p>Scan and email the request to the responsible member of staff (usually the Headteacher) and the Data Protection Officer as needed.</p>

What must I do?	Why?	How?
the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two days.		

## Data Protection Officer

The named Data Protection Officer for West Hove Infant School is: **James English**

The Data Protection Officer can be contacted at: [dpo@dataprotection.education](mailto:dpo@dataprotection.education)

West Hove Infant School shall maintain a named Data Protection Officer to represent the rights of data subjects.

West Hove Infant School shall ensure that the data protection officer is involved properly and in a timely manner, in all issues which relate to the protection of personal data.

West Hove Infant School shall support the data protection officer in performing the responsibilities outlined below by providing resources necessary to carry out those tasks and access to personal data and processing operations. The Data Protection Officer shall maintain his or her expert knowledge.

West Hove Infant School shall ensure that the data protection officer does not receive any instructions regarding the exercise of their tasks. They shall not be dismissed or penalised by the controller or the processor for performing his tasks.

The data protection officer shall directly report to the highest management level of West Hove Infant School, as needed and report to the Board of Governors at least once a year.

Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks.

The Data Protection Officer shall have the following responsibilities:

- Review of all data processing activities (inventory / mapping);
- Conduct of regular health checks/audits and issue recommendations;
- Assistance with data protection impact assessments and monitoring performance;
- Monitoring and advice relating to subject access requests and data breaches;
- Assisting schools with maintenance of records;
- Monitoring and advice relating to FOI and other information requests;
- Co-operation with, and act as the contact point for the supervisory authority, the Information Commissioner's Office;
- Act as the contact point for data subjects to deal with requests and complaints;
- Training staff.

## Data Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, West Hove Infant School will implement appropriate technical and organisational measures to ensure a level of security of the processing of Personal Data appropriate to the risk.

These measures shall include as appropriate:

- measures to ensure that the Personal Data can be accessed only by authorised personnel for the purposes agreed in the record of processing activity and outlined in the privacy notice;
- in assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of personal data;
- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regular testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of personal data;
- measures to identify vulnerabilities with regards to the processing of personal data in systems used to provide services to The Organisation

## Photography and Videos

Photographs and videos will be used where they are deemed essential for performing the public task of the school or relative to providing education. Where photographs are required for other purposes, these purposes will be documented and explicit consent will be sought.

The retention period for photographs and videos will be documented in the retention policy. At the end of the retention period photographs will either be destroyed or they may be retained as photos for archiving purposes in the public interest.

## CCTV

CCTV may be used for the purpose of protecting the safety of staff, students and visitors, site security and for monitoring behaviour. Where appropriate and on request, we may share this information with a third party; i.e. police. At both sites, cameras are located both in and outside the reception foyer, inside corridors and the playgrounds. Outside cameras only capture approximately five meters of the pavement and surrounding area.

All CCTV footage is securely stored and can only be accessed by appropriate members of staff. All images recorded by CCTV will be deleted as defined in the retention schedule.

Where West Hove Infant School installs new CCTV cameras, a data privacy impact assessment will be carried out prior to installation.

The nominated person responsible for CCTV in West Hove Infant School is the schools office manager.

## Fob system at CR

A fob system records when individual members of staff gain entry/exit to a particular door within the building. This information is stored on the main office computer at CR (RS) and is password protected by RS. The retention period for this information is documented in the retention policy. Should a fob card be lost or stolen, only a hexagonal code would be accessible.

## Retention Policy

West Hove Infant School will not keep personal data longer than necessary and will maintain a retention schedule outlining the retention requirements of electronic and paper records. West Hove Infant School will retain the minimum amount of information that it requires to carry out its' statutory functions and the provision of services.

In circumstances where a retention period of a specific document has expired, checks will be made to confirm disposal and consideration given to the method of disposal to be used based on the data to be disposed of. These checks will include:

- Have the documents been checked to ensure they are appropriate for destruction?
- Is retention required to fulfil statutory obligations or other regulatory obligations, including child protection?
- Is retention required for evidence?
- Is retention required to meet the operational needs of the service?
- Is retention required because the document or record is of historic interest, intrinsic value or required for organisational memory?

## Training

West Hove Infant School shall ensure that all members of staff receive data protection training, including information handling appropriate to ensure data protection competence in their role, a minimum of every two years.

## DATA PROCESSORS

The organisation contract with various organisations who provide services to the organisation, including:

- Payroll Providers – to enable us to pay our employees;
- Parent payment systems – to enable parents to pay for organisation meals, trips and/or uniforms;
- Pupil Assessment systems – to support us with the tracking and monitoring of pupil achievement;
- Communication systems – to enable us to effectively communicate with parent and pupils;
- organisation meal providers – to support with the provision and payment for organisation meals;
- Photographers – to enable us to store pupil photographs for safeguarding purposes;
- HR Systems – for the effective management of all aspects of staff management;

In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.

Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the organisation.

The organisation will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of Data Subjects.