# Elmwood Infant and Nursery School

## Data Protection Policy

Linked to the General Data Protection Regulation (GDPR)

Spring 2019

*Article 3 - the best interests of the child must be a top priority in all decisions and actions that affect children*
*Article 16 - the right to privacy*
*Article 36 - Governments must protect children from all forms of exploitation.*

# Elmwood Infant School & Nursery

## Data Protection Policy

(including Freedom of Information)

Linked to the General Data Protection Regulation (GDPR)

**DATE POLICY CREATED:** **Spring 2019**

**DATE OF NEXT REVIEW:** **Spring 2021**

**Statement of Intent**

Elmwood Infant School and Nursery is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR). The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, Department for Education, other schools and educational bodies, children's services and other third parties, such as payroll providers.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR. Organisational methods for keeping data secure are imperative, and Elmwood Infant School believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018.

This policy has been implemented in conjunction with the following school policies:

- E-safety Policy
- Acceptable Use Policy

**Legal Framework**

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now.

**Applicable Data**

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

**Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

**Principles**

In accordance with the requirements outlined in the GDPR, personal data will be:

Processed lawfully, fairly and in a transparent manner in relation to individuals.

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

**Accountability**

Elmwood Infant School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The school will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

Name and details of the organisation

Purpose(s) of the processing

Description of the categories of individuals and personal data

Retention schedules

Categories of recipients of personal data

Description of technical and organisational security measures

The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

Data minimisation.

Pseudonymisation.

Transparency.

Allowing individuals to monitor processing.

Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

**Data Protection Officer (DPO)**

The school has a DPO whose role it is to:

Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.

Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

An existing employee can be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests. Where possible, this role will be carried out by an external provider.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

The DPO will report to the highest level of management at the school, which is the Head Teacher.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

**Lawful Processing**

The legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR, data will be lawfully processed under the following conditions:

The consent of the data subject has been obtained.

Processing is necessary for:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.

— For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

Sensitive data will only be processed under the following conditions:

Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.

Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

Processing relates to personal data manifestly made public by the data subject.

Processing is necessary for:

— Carrying out obligations under employment, social security or social protection law, or a collective agreement.
— Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
— The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
— Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
— The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
— Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
— Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

**Consent**

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

- Where consent is given, a record will be kept documenting how and when consent was given.

- The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

- Consent can be withdrawn by the individual at any time.

- Where a child is under the age of 16 or younger if the law provides it (up to the age of 13), the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

**The Right to be Informed**

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.

The purpose of, and the legal basis for, processing the data.

The legitimate interests of the controller or third party.

Any recipient or categories of recipients of the personal data.

Details of transfers to third countries if applicable and the safeguards in place.

The retention period or criteria used to determine the retention period.

The existence of the data subject's rights, including the right to:

- Withdraw consent at any time.
- Lodge a complaint with a supervisory authority.

The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

Within one month of having obtained the data.

If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.

If the data is used to communicate with the individual, at the latest, when the first communication takes place.

**The Right of Access**

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a **Subject Access Request** (SAR) to gain access to their personal data in order to verify the lawfulness of the processing (see Appendix 3).

**Responding to a Subject Access Request**
Requests for information must be made in writing; which includes email, and be addressed to the Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.

The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement
  *This list is not exhaustive*.

Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information relating to court proceedings.

If there are concerns over the disclosure of information then additional advice should be sought.

Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a ‘reasonable fee’ to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, **within one month** of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

**The Right to Rectification**

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to **within one month**; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

**The Right to Erasure**

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- 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

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

**The Right to Restrict Processing**

Individuals have the right to block or suppress the school's processing of personal data.

In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The school will inform individuals when a restriction on processing has been lifted.

**The Right to Data Portability**

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.

The school will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The school will respond to any requests for portability **within one month**.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

**The Right to Object**

The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

Processing based on legitimate interests or the performance of a task in the public interest

Direct marketing

Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

An individual's grounds for objecting must relate to his or her particular situation.

The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

The school will stop processing personal data for direct marketing purposes as soon as an objection is received.

The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

The individual must have grounds relating to their particular situation in order to exercise their right to object.

Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

**Automated Decision Making and Profiling**

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.

- It produces a legal effect or a similarly significant effect on the individual.

The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

**Privacy by Design and Privacy Impact Assessments**

The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

Systematic and extensive processing activities, such as profiling

Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

The use of CCTV.

The school will ensure that all DPIAs include the following information (see Appendix 1):

A description of the processing operations and the purposes

An assessment of the necessity and proportionality of the processing in relation to the purpose

An outline of the risks to individuals

The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

**Data Breaches**

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- The Head Teacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.
- Staff must report any data breach or potential breach as soon as possible to the Data Protection Officer or a member of the Senior Management Team.
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
- All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.
- The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.
- In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.
- A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
- In the event that a breach is sufficiently serious, the public will be notified without undue delay.
- Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

**Data Security**

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data both on a local hard drive and on the school's network is password-protected. The network drive is backed up daily off-site.
- Access to the school's network is controlled and access to sensitive and confidential data on the network is restricted to only those members of staff who require the information to perform their duties effectively.
- Access to the school's management information system SIMS is password-protected and access to sensitive and confidential data on SIMS is restricted to only those members of staff who require the information to perform their duties effectively.
- Staff are not permitted to use removable storage e.g. external hard drives or memory sticks to store data.
- All electronic devices are password-protected to protect the information on the device in case of theft. Electronic devices are kept securely when not in use, e.g. in a locked cabinet.
- Devices holding pupil and staff photos will be regularly wiped to delete all images. Memory cards will be kept in a locked cabinet when not in use and will be wiped regularly.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff, governors and student teachers, will not use their personal laptops or computers for school purposes.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Staff, governors and student teachers must not use personal email addresses for sharing or viewing any school data. Secure LGFL email accounts are provided for all staff and governors.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- When sending confidential information by fax, staff will always check that the recipient is correct before sending.
- No personal data or sensitive personal data must be shared by text or on social media e.g. Whatsapp. See also the school's e-Safety and IT Acceptable Use Policy.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices or paperwork under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- The person or organisation who will receive the data has been outlined in a privacy notice.

- The person or organisation who will receive the data have confirmed in writing that they comply with the GDPR and any other relevant data protection legislation.

Under no circumstances are volunteers, visitors or unauthorised third parties allowed access to confidential or personal information. Those visiting areas of the school containing sensitive information are supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Elmwood Infant School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Office Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.

**Publication of Information**

Elmwood Infant School has a publication scheme on its website (see Appendix 2) outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Financial information, such as Pupil Premium Grant or Sports Grant

Classes of information specified in the publication scheme are made available quickly and easily on request.

Elmwood Infant School will not publish any personal information, including photos, on its website without the permission of the individual.

When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

**CCTV and Photography**

The school understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for 30 days for security purposes; the Office Manager is responsible for keeping the records secure and allowing access.

The school will always indicate its intentions for taking photographs of pupils and will obtain permission before publishing them.

If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

**Data Retention and Storing Pupil Data**

Data will not be kept for longer than is necessary. The school follows the Information Commissioner's guidance on retention of documents, including the Information and records Management Society's Retention Guidelines for School.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

**DBS Data**

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Complaints

Complaints about the procedures outlined in this policy should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure. Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact the Headteacher who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk

Appendix 1

Data Protection Impact Assessment

Introduction

- Project name.
- Explain what the project aims to achieve, and what the benefits will be to the school, to individuals and to other members of the school community.
- Link to any other relevant documents related to the project, e.g. a project proposal.
- Describe the process for the collection and deletion of any personal data.
- Explain what information will be used used, what it is used for and who will have access to it.
- Detail how many individuals are likely to be affected by the project.

| Question | Yes | No | Unsure | Comments |
|---|---|---|---|---|
| Will the project involve collecting new information about individuals? | | | | |
| Will the project require individuals to provide information about themselves? | | | | |
| Will information about individuals be disclosed to other individuals or organisations who have not previously held information about the individual? | | | | |
| Is any information about individuals held for purposes it is not currently used for, or in a way it is not currently used? | | | | |
| Will the project involve using a new technology that might be perceived as being intrusive to an individual's privacy? | | | | |
| Will the project result in any decisions or actions taken against individuals which may have a significant impact on them? | | | | |
| Will any information about individuals raise privacy concerns, e.g. information they may wish to keep private, such as criminal information held on DBS certificates? | | | | |
| Will the project require you to contact individuals in ways that they may find intrusive? | | | | |

# Risk Assessment

| Potential Risk | Risk Rate H/M/L | Proposed Solutions | Responsibility | Risk reduced to acceptable level Y/N |
|---|---|---|---|---|
| **Risk to individuals** | | | | |
| | | | | |
| **Risk to school** | | | | |
| | | | | |
| **Risk to compliance with GDPR** | | | | |
| | | | | |

**Appendix 2:**

# Publication Scheme

This scheme follows the model approved by the Information Commissioner and sets out the classes of information which we publish or intend to publish; the format in which the information will be made available and whether the information is available free of charge or on payment.

## 1. Classes of information

Information that is available under this scheme includes:

- Who we are and what we do
- What we spend and how we spend it
- What are our priorities are and how we are doing
- How we make decisions
- Our policies and procedures
- The services we offer

Information which **will not** be made available under this scheme includes:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

## 2. Information available on our website

Every local-authority maintained school must publish specific information on its website to comply with The School Information (England) (Amendment) Regulations 2016.

The information specified is as follows:

1. School contact details
2. Admission arrangements
3. Ofsted reports
4. Exam and assessment results
5. Performance tables
6. Curriculum
7. Behaviour policy
8. School complaints procedure
9. Pupil premium
10. PE and sport premium for primary schools
11. Special educational needs (SEN) and disability information
12. Equality objectives
13. Governors' information and duties
14. Charging and remissions policies
15. Values and ethos
16. Details of how to request paper copies of documents

## 3. How to request information

Requested documents under the publication scheme will be delivered electronically where possible, but paper copies can be provided by contacting the school using the below contact details.

To enable us to process your request quickly, please mark all correspondence:
**"FREEDOM OF INFORMATION REQUEST"**

Documents can be translated under disability legislation into accessible formats where possible.

## 4. Charges

Documents contained in this scheme are free to view on the school website or single paper copies are available free of charge to parents and prospective parents of the school who request them.

## 5. Feedback

We welcome any comments or suggestions you may have regarding this scheme. Please contact the school using the below contact details: office@elmwood-inf.croydon.sch.uk

0208 689 7681

**Appendix 3**

# ELMWOOD INFANT SCHOOL & NURSERY

## Subject Access Request Form

Please complete the following form and return it to the school office.

## DATA SUBJECT DETAILS

| | |
|---|---|
| **Title** | |
| **Surname** | |
| **First Name(s)** | |
| **Current Address** | |
| **Telephone (Home)** | |
| **Telephone (Work)** | |
| **Telephone (Mobile)** | |
| **Email address** | |
| **Date of birth** | |
| **Details of identification provided to confirm name of data subject in question** | |
| **Details of data requested** | |

***If the person requesting the information is NOT the data subject, complete the below:***

| | | |
|---|---|---|
| Are you acting on behalf of the data subject with their written consent or in another legal authority? | Yes | No |
| If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor) | | |
| Has proof been provided to confirm you are legally authorised to obtain the information? | Yes | No |

| | |
|---|---|
| **Title** | |
| **Surname** | |
| **First Name(s)** | |
| **Current Address** | |
| **Telephone (Home)** | |
| **Telephone (Work)** | |
| **Telephone (Mobile)** | |
| **Email address** | |

# DECLARATION

I hereby request that Elmwood Infant School and Nursery provide me with the information about the data subject above.

Name ……

Signature: ……

Date: ……

**Appendix 4**

# Privacy Notice for Children

Article 3 - the best interests of the child must be a top priority in all decisions and actions that affect children
Article 36 – Governments must protect children from all forms of exploitation.

Dear Children (and Parents/Carers),

We have to keep information about you to help us ensure that we are meeting all of your needs and enabling you to be the best that you can be. As a Rights Respecting School we also know that you have the right to privacy and so we are very careful with the data that we keep.

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

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information
- Assessment information
- Other information to support your learning, development and progress (such as medical information, special educational needs information, safeguarding information, exclusions and behavioural information)

Why we collect and use this information:

We use your data:

- to support your learning and to monitor and report on progress
- to provide you with the best possible care and to ensure you are kept safe at all times
- to assess the quality of what we do and to comply with the law regarding data sharing.

We are allowed to use and process this information because it links to Article 6 of the General Data Protection Regulation (GDPR) and Article 9 (Special Category Data). This gives us a *Lawful Basis* to use your data.

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.

**Collecting Information**

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

Storing Pupil Data

We will not keep your data for longer than is necessary and follow the Information Commissioner's guidance on retention of documents.

Sharing Pupil Information

We routinely share your information with:

- schools that you attend after leaving Elmwood Infant School and Nursery
- Our local authority and other authorites when necessary
- the Department for Education (DfE)
- Early Help, Health Services and Social Services, when necessary
- OTrack and 2buildaprifle – companies that help us to manage our assessment systems
- CPOMS – a software service that manages our safeguarding, attendance and behaviour data
- Sometimes we use little bits of information like your name, for dojos (reward scheme), the seesaw app and 2build a profle (parent communucaton apps).

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

We share data with the Department for Education (DfE) on a statutory basis. This data sharing helps the government to decide on how schools are funded and to make decisions about funding, assessment and monitoring.

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

You can find out more about the data collection requirements placed on us by the Department for Education by going to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

**Requesting Access to your Personal Data**

Under data protection legislation, you and your parents/carers have the right to request access to the information that we hold about you. To make a request for your personal information, or be given access to your educational record, please contact the Headteacher, Zoe Harris.

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 would like to discuss anything in this privacy notice or have a concern about the way we are collecting or using your personal data, please contact the Headteacher, Zoe Harris, in the first instance.

**********

Parents/Carers: Please can you sign and date this notice to show that you have read and understood the reasons why we store, process and sometimes share your child's data.

Signed:……Parent/Carer Date:…….

Child's Name:…….....

**Appendix 5**

# Privacy Notice for Staff, Governors and Volunteers

Dear Staff, Governors and Volunteers,

The General Data protection Regulations have changed the way that we collect, process, hold and share your information. This privacy notice informs you about what we collect and how we use your personal data.

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

- Personal information (such as name, address, date or birth, employee or teacher number, national insurance number)
- Special categories of data needed for the Disclosure and Barring Service and Single Central Register (such as DBS number, right to work in the UK, convictions/cautions)
- Special categories of data including characteristics information such as gender, age, ethnic group
- Contract information (such as start dates, hours worked, post, roles and salary information)
- Work absence information (such as number of absences and reasons)
- Qualifications (and, where relevant, subjects taught)
- Relevant medical information (such as health clearance information, occupational health reports)
- Payroll information (such as bank details, salary)
  Other information to support the financial and personnel requirements of the school.

**Why we collect and use this information**

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- to comply with the law regarding checks such as DBS checks and medical clearance.

**The lawful basis on which we process this information**

We collect and use workforce information for the reasons above. Our lawful bases for processing this data is set out in Article 6 of the GDPR and Article 9 (Special Category Data).
Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.

**Collecting this information**

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

**Storing this information**

Data will not be kept for longer than is necessary. The school follows the Information Commissioner's guidance on retention of documents.

**Who we share this information with**

We routinely share this information with:

- our local authority
- the Department for Education (DfE)
- When an employment reference has been requested by another establishment for a member of the workforce

**Why we share school workforce information**

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

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

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

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

**Requesting access to your personal data**

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the Headteacher, Zoe Harris

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 ask 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/

**Further information**

If you would like to discuss anything in this privacy notice, please contact the Headteacher, Zoe Harris