

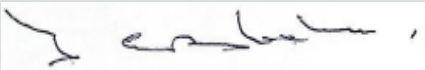
ELMWOOD JUNIOR SCHOOL



Curious Creative Compassionate

UK GDPR Data Protection Policy

Issue 3

Approved by:	Curriculum Committee	Date: 28.04.2021
Approved by:	FGB	Date: 28.04.2021
Next review:	24 Months	
Signed on behalf of FGB:		Date: 19.07.2021

Contents:

Statement of intent

1. Legal framework
2. Applicable data
3. Principles
4. Accountability
5. Data protection officer (DPO)
6. Lawful processing
7. Consent
8. The right to be informed
9. The right of access
10. Parent requests to see the educational record
11. The right to rectification
12. The right to erasure
13. The right to restrict processing
14. The right to data portability
15. The right to object
16. Automated decision making and profiling
17. Privacy by design and privacy impact assessments
18. Data breaches
19. Data security
20. Publication of information
21. CCTV and photography
22. Data retention
23. DBS data
24. Rights Respecting
25. Policy review

Statement of intent

Elmwood Junior School is required to keep and process certain information about its staff members, pupils, governors and other third parties, the school is therefore a data controller and is registered with the ICO. The school keeps and processes data in accordance with its legal obligations under the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (UK GDPR).

The school may, from time to time, be required to share personal information about its staff, pupils, governors or third parties 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 or cashless till services.

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 UK GDPR.

Organisational methods for keeping data secure are imperative, and Elmwood Junior School believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

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

- The Data Protection Act 2018
- The General Data Protection Regulation (UK 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

1.2. This policy will also have regard to guidance published by the Information Commissioners Office guidance on the DPA 2018 and the UK GDPR.

1.3. This policy will be implemented in conjunction with the following other school policies:

- E-safety Policy
- Freedom of Information Policy
- CCTV Policy
- DBS Policy

2. Applicable data

2.1. 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 UK 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.

2.2. **Sensitive personal data** is referred to in the UK 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.

3. Principles

3.1. In accordance with the requirements outlined in the UK 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 UK 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.
- 3.2. The UK GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

4. Accountability

- 4.1. Elmwood Junior School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.
- 4.2. The school will provide comprehensive, clear and transparent privacy policies for pupils (see Appendix 1), staff (Appendix 2) and job applicants (Appendix 3).
- 4.3. 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.
- 4.4. 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
 - Details of transfers to third countries where applicable, including documentation of the transfer mechanism safeguards in place
- 4.5. 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.
- 4.6. Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

The school’s DPO is Judicium Education. They will carry out the following duties:

- Inform and advise the school and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the school's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments and conducting internal audits
- 5.2 The school will appoint a GDPR Lead who is responsible for liaising with the DPO and providing training for school staff.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
 - The data needs to be processed so that the school can comply with a **legal obligation**.
 - The data needs to be processed so that the school, as a public authority, can perform a task in the **public interest** or exercise its official authority.
 - The data needs to be processed so that the school can fulfil a **contract** with the data subject, or the data subject has asked the school to take specific steps before entering into a contract.
 - The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life.
 - The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

6.3. Sensitive data and criminal offence 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).

7. Consent

- 7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- 7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- 7.3. Where consent is given, a record will be kept documenting how and when consent was given.
- 7.4. The school ensures that consent mechanisms meet the standards of the UK 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.
- 7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- 7.6. Consent can be withdrawn by the individual at any time.
- 7.7. 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.

8. The right to be informed

- 8.1. 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.
- 8.2. 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.
- 8.3. 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.
- 8.4. 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.
- 8.5. 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.
- 8.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
- 8.7. 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.

9. The right of access

- 9.1. Individuals have the right to obtain confirmation that their data is being processed.
- 9.2. 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.
- 9.3. The SAR can be submitted in any form but we may be able to respond more quickly where a submission is made in writing and includes the name, contact number, address, email address and details of the information requested.
- 9.4. The school will verify the identity of the person making the request before any information is supplied. The school may ask the person to provide 2 forms of identification.
- 9.5. 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.
- 9.6. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

- 9.7. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- 9.8. All fees will be based on the administrative cost of providing the information.
- 9.9. All requests will be responded to without delay and at the latest, **within one month** of receipt (or receipt of the additional information needed to confirm identity, where relevant.)
- 9.10. 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.
- 9.11. 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.
- 9.12. 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.
- 9.13. Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.
- 9.14. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.
- 9.15. We may not disclose information for a variety of reasons, such as if it:
- Might cause serious harm to the physical or mental health of the pupil or another individual.
 - Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
 - Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
 - Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10. Parental requests to see the educational record

- 10.1. Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 days of a written

request. If the request is for a copy of the record the school may charge a fee to cover the cost of supplying it. This right applies as long as the child concerned is aged under 18.

- 10.2. There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. The right to rectification

- 11.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.
- 11.2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.
- 11.3. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.
- 11.4. Requests for rectification will be responded to **within one month**; this will be extended by two months where the request for rectification is complex.
- 11.5. 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.

12. The right to erasure

- 12.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- 12.2. 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
- 12.3. 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

- 12.4. 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.
- 12.5. 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.
- 12.6. 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.

13. The right to restrict processing

- 13.1. Individuals have the right to block or suppress the school's processing of personal data.
- 13.2. 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.
- 13.3. 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
- 13.4. 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.
- 13.5. The school will inform individuals when a restriction on processing has been lifted.

14. The right to data portability

- 14.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- 14.2. 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.
- 14.3. 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
- 14.4. Personal data will be provided in a structured, commonly used and machine-readable form.
 - 14.5. The school will provide the information free of charge.
 - 14.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.
 - 14.7. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.
 - 14.8. 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.
 - 14.9. The school will respond to any requests for portability **within one month**.
 - 14.10. 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.
 - 14.11. 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.

15. The right to object

- 15.1. 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.
- 15.2. 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.
- 15.3. 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.
- 15.4. 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.
- 15.5. 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.

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

16. Automated decision making and profiling

16.1. 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.

16.2. 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.

16.3. 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.

16.4. 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.

17. Privacy by design and privacy impact assessments

17.1. The school will act in accordance with the UK 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.

17.2. 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.

17.3. 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.

- 17.4. 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.
- 17.5. A DPIA will be used for more than one project, where necessary.
- 17.6. 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.
- 17.7. The school will ensure that all DPIAs include the following information:
- 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
- 17.8. Where a DPIA indicates high risk data processing, the school will consult the DPO to seek its opinion as to whether the processing operation complies with the UK GDPR.

18. Data breaches

- 18.1. 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.
- 18.2. The GDPR Lead will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.
- 18.3. Staff must report any data breach or potential breach as soon as possible to the GDPR Lead or a member of the Senior Leadership Team. Data breaches are recorded by the GDPR Lead.
- 18.4. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority - the Information Commissioner's Office (ICO) - will be informed.
- 18.5. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.
- 18.6. 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.
- 18.7. 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. The notification will be made in writing and will include the contact details of the GDPR Lead and DPO, a clear description of the breach, the likely consequences and the steps taken to mitigate any adverse effects.
- 18.8. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
- 18.9. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

- 18.10. 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.
- 18.11. 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 GDPR Lead and 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
- 18.12. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

19. Data security

- 19.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- 19.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.
- 19.3. 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.
- 19.4. 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.
- 19.5. 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.
- 19.6. Staff are not permitted to use removable storage e.g. external hard drives.
- 19.7. Staff are not permitted to use memory sticks.
- 19.8. 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.
- 19.9. 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.
- 19.10. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- 19.11. Staff, governors and student teachers are permitted to use their personal laptops or computers for school purposes but must only access school personal or confidential data via the secure remote working solution provided or through LGFL secure email. No school personal or confidential data must be saved onto personal devices.

- 19.12. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- 19.13. 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.
- 19.14. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- 19.15. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 19.16. When sending confidential information by fax, staff will always check that the recipient is correct before sending.
- 19.17. 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.
- 19.18. 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.
- 19.19. 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 UK GDPR and any other relevant data protection legislation.
- 19.20. 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.
- 19.21. 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.
- 19.22. Elmwood Junior School takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- 19.23. The School business manager (SBM) is responsible for continuity and recovery measures are in place to ensure the security of protected data.

20. Publication of information

- 20.1. Elmwood Junior School publishes a publication scheme on its website (see Appendix 4) outlining classes of information that will be made routinely available, including:
- Policies and procedures
 - Minutes of meetings

- Annual reports
 - Financial information, such as Pupil Premium Grant or Sports Grant
- 20.2. Classes of information specified in the publication scheme are made available quickly and easily on request.
- 20.3. Elmwood Junior School will not publish any personal information, including photos, on its website without the permission of the affected individual.
- 20.4. 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.

21. CCTV and photography

- 21.1. The school understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles. Please see the school's images and videos parental consent form for more details.
- 21.2. The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via the CCTV Policy which is available on the website.
- 21.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- 21.4. All CCTV footage will be kept for 30 days for security purposes; the SBM is responsible for keeping the records secure and allowing access.
- 21.5. The school will always indicate its intentions for taking photographs of pupils and will obtain permission before publishing them.
- 21.6. 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.
- 21.7. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR. However, we will ask that photos or videos with other pupils in them are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

22. DBS data

- 22.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
- 22.2. Data provided by the DBS will never be duplicated.
- 22.3. 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.

23. Policy review

24.1 This policy will be reviewed by the Head Teacher every 2 years, or in light of any changes to relevant legislation.

Policy approved

The next scheduled review date for this policy is June 2026

Appendix 1 – Privacy Notice for Pupils

Privacy Notice (How we use pupil & their family's information)

Elmwood Junior School holds the legal right to collect and use personal data relating to pupils and their families.

Under the law, the school is required to inform you how we process personal data relating to our pupils and their families.

Elmwood Junior School is the data controller of the personal information which you provide to us. This means that the school determines the purpose for which, and the manner in which, any personal data relating to pupils and their families will be processed.

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

- Personal information (such as name, unique pupil number, address and family contact details)
- Characteristics (such as gender, disability, ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as school reports, test results and observations)
- Behavioural information (such as information collected in accordance with the school's Behaviour Policy)
- Safeguarding information (such as records of disclosures, minutes of meetings and reports from outside agencies)
- Special Educational Needs information (such as records of assessments, minutes of meetings and reports from outside agencies)
- Medical information (such as details of medical conditions, allergies, medication and copies of medical appointments)
- Digital imagery (such as photographs and video of school trips and events)
- CCTV footage (please refer to the CCTV Policy on the school's website)

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to provide appropriate support to pupils with medical conditions or additional needs
- to ensure the safety of pupils and other members of the school community
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use personal data in order to meet legal requirements and in the public interest, as set out in the General Data Protection Regulations 2018 (UK GDPR) and UK law, including:

- Articles 6 and Article 9 of UK GDPR
 - Education Act 1996
 - Section 3 of the Education (Information About Individual Pupils) (England) Regulations 2013
- The submission of school census returns, including a set of named pupil records, is a statutory requirement on schools under Section 537A of the Education Act 1996. This means that schools are not required to obtain parent or pupil consent to collect and process pupil data.

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. When collecting data, we will inform you whether you are required to provide the data or if your consent is needed.

Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

Where we are processing data based on your consent, you have a right to withdraw this consent at any time.

Storing pupil data

Personal data relating to pupils and their families is stored in line with our GDPR Data Retention Policy (see the school's website). In accordance with UK GDPR, we will not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

Who we share pupil information with

We will not share your personal information with any third parties without your consent, unless the law allows us to do so. For example safeguarding information can be shared with appropriate agencies without your consent, in order for us to fulfil our duty to protect pupils or to prevent a crime.

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our local authority, including admissions and departments concerned with safeguarding and social services
- the Department for Education (DfE)
- Ofsted
- the Police
- medical professionals, such as the school nursing team, childrens' mental health services and educational psychologists
- agencies who provide professional support to pupils, such as speech & language therapy, play therapy, young carers support and counselling services
- providers of learning software
- catering services
- companies which provide essential IT and administrative services to the school

Please see Appendix 1A for the most recent list of companies and organisations we are working with. The information that we share with these parties includes the following:

- name and contact details
- safeguarding, medical or SEND information where appropriate
- attendance or behavioural information where appropriate

Where the school outsources data to a third party processor, the same data protection standards that Elmwood Junior School upholds are imposed on the processor.

Why we share pupil information

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

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

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

Data collection requirements:

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

The National Pupil Database (NPD)

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

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

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

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

To contact DfE: <https://www.gov.uk/contact-dfe>
Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the GDPR lead (see contact details below).

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

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

Contact

If you would like to find out more information about how we collect, use and store your personal data, please visit the school's website www.elmwood-jun.croydon.sch.uk or contact:
The GDPR lead via the school office on 0208 684 4007 or by email to gdpr@elmwood-jun.croydon.sch.uk.
Note: the school's data protection officer is Judicium Education who ensure that the school remain compliant with all data protection laws and who we seek regular advice from.

From time to time we will update the school's Privacy Notice and the new version will be uploaded to our website or will be available from the School Office.

Elmwood Junior School Data Protection Declaration

I confirm that I understand:

- Elmwood Junior School has a legal and legitimate interest to collect and process my personal data in order to meet statutory requirements.
- How my data is used.
- Elmwood Junior School may share my data with the Department for Education and also the Local Authority.
- Elmwood Junior School will not share my data with any other third parties without my consent, unless the law requires the school to do so.
- Elmwood Junior School will always ask for explicit consent where this is required and I must provide this consent if I agree to the data being processed.
- Where Elmwood Junior School is processing my data based on consent, I have a right to withdraw this consent at any time.
- My data is retained in line with the school's GDPR Data Retention Policy.
- My rights to the processing of my personal data.
- Where I can find out more information about the processing of my personal data.

CHILD'S NAME: _____ **CLASS:** _____

PARENT/CARER NAME: _____

SIGNATURE: _____

DATE: _____

Please return the signed declaration form to the School Office

Appendix 1A: Providers of Services, IT & Software Suppliers 2023-24

The school works with a number of service providers and IT suppliers in order to effectively perform tasks in the public interest, or to comply with legal obligations. We share certain personal data with these organisations. For more information as to how the data is processed and kept secure, please refer to the organisation's data protection and privacy policies.

Atomwide (AdEPT) – email accounts, online security, remote access & digital signage (pupil, parent, staff & governor data, including sensitive data. Pupil & staff photos.) <https://www.atomwide.com/privacy.html>

Capita plc - SIMS (school management information system: all pupil, parent, staff & governor data, including sensitive data and pupil photos) <https://www.capita-sims.co.uk/privacy-notice>

Capita plc – Reading Cloud library management system (pupil names, dates of birth, class/staff names) <https://www.capita-readingcloud.co.uk/privacy-notice>

Croydon Music & Arts – music tuition (pupil names, ages and sensitive data required to ensure pupil safety/staff names & school email addresses) <https://www.croydon.gov.uk/democracy/data-protection-freedom-information/privacy-notices/education-youth-engagement-service-privacy-notice>

Collins Big Cat Phonics Ebook Library – digital copies of decodable phonics books (pupil name, class, staff school email address)

Croydon Council Local Government Pension Team – pensions support (support staff names, school email addresses & pension details) <https://www.croydonpensionscheme.org/croydon-pension-fund/privacy-policy-and-cookies>

Croydon Teachers Pensions – pensions support (teaching staff names, school email addresses & pension details) <https://www.croydon.gov.uk/democracy/data-protection-freedom-information/privacy-notices/corporate-privacy-notice>

Cunningham's – cashless till (pupil names, staff names and allergy information) <https://www.cunninghams.co.uk/mint-project/uploads/666520732.pdf>

Croydon Drop In – counselling service for pupils (pupil names, ages and sensitive data required to provide the service/staff names & school email addresses). enquiries@croydondropin.org.uk

Eduspot (formerly Teachers2Parents) – texting service (pupil names/ parent, staff names & mobile numbers) <https://eduspot.co.uk/privacy-policy/>

Edukey (TES) - provision maps & intervention tracking (pupil data, including sensitive data/ staff names & school email addresses) <https://www.edukey.co.uk/privacy/>

Epep National Single Sign-on – software for Looked After Children's Personal Education Plan (pupil data, including sensitive data; parent names/mobile numbers/ staff names, school email addresses)

Google G Suite – data storage & sharing (pupil & staff names, school email addresses) <https://policies.google.com/privacy?hl=en-GB>

Groupcall - data extraction from SIMS for library system (pupil names/staff names & school email addresses). <https://www.groupcall.com/privacy>

Guys & St Thomas's NHS Foundation Trust – speech & language support for pupils (pupil names, ages and sensitive data; staff names & school email addresses). <https://www.england.nhs.uk/contact-us/privacy-notice/>

Harrison – school catering service: (pupils names, staff names, allergy information) <https://www.harrisoncatering.co.uk/>

Kittle Photographic – school photographs (individual and class photos for pupils & staff). <https://kittlephoto.com/privacy-policy.html>

London Grid for Learning – broadband, Egress accounts (staff names & school email addresses) <https://static.lgfl.net/LgflNet/downloads/policies/LGfL%20Privacy%20Notice.pdf>

Rakuten Overdrive – e-books (pupil ID's from library system) <https://company.cdn.overdrive.com/policies/privacy-policy.htm>

ParentPay – school meal payments (pupil name, parent & staff names/email addresses/card details). Viewed only by school staff. <https://www.parentpay.com/privacy-policy/>

[Reading Cloud Junior Librarian – children's digital school library management system \(pupil names, class, date of birth\)](#)

Single Central Record – (staff names and sensitive data required to ensure pupil safety) <https://onlinescr.co.uk/>

Strictly Education – HR & payroll provider (staff names, dates of birth, contact details, NI numbers & contract details) <https://www.strictlyeducation.co.uk/privacy-policy>

Wonde – data extraction from SIMS for Eduspot, Education City & Edukey (pupil data, including sensitive data; parent names/mobile numbers/ staff names, school email addresses & mobile numbers)

<https://wonde.com/privacy-policy>

3PLearning – Mathletics & Readwriter online learning (pupil names, dates of birth/ staff names & school email addresses) <https://www.3plearning.com/privacy/>

NFER – Online Assessment Analysis Tool (pupil names, ages and sensitive data required to aid equality of opportunity/staff names & school email addresses <https://www.nfer.ac.uk/privacy/>

Inventry – online register of staff on site and visitors (photographs taken of visitors).

<https://www.inventry.co.uk>

[Testbase – Maths questions software \(staff names, staff school email addresses\)](#)

Times Tables Rockstars - (pupil names, dates of birth/staff names & school email addresses)

<https://trockstars.com/>

Appendix 2 – Privacy Notice for the School Workforce

Privacy Notice (How we use your information)

The categories of school information that we collect and process include:

- Your name, address and contact details, including email address and telephone numbers, date of birth and sex;
- The terms and conditions of your employment or engagement;
- Resignation and notice letters;
- Details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with us;
- Information about your remuneration, including entitlement to benefits such as pensions or insurance cover, any salary sacrifice deductions, pension deductions and tax details;
- Details of your bank/building society account and national insurance number;
- Information about your marital status, next of kin, dependants and emergency contacts;
- Information about your nationality and entitlement to work in the UK and information from related documents such as your passport or other identification information;
- Disclosure & Barring Service information and details of your criminal record where relevant to your employment;
- Details of any allegations regarding children and vulnerable adults;
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief; gender re-assignment, marital status, caring commitments status;
- Details of your schedule (days of work and working hours) and attendance at work;
- Details of periods of leave taken by you, including holiday, sickness absence, family and maternity leave and unpaid leave, and the reasons for the leave;
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- Assessments of your performance, including probation, appraisals, performance reviews and ratings, performance improvement plans and related correspondence;
- Details of training you have participated in and policies that you have received and acknowledge that you will abide by;
- Details of any redundancy estimates and pension costs;
- Information about medical or health conditions, including whether or not you have a disability for which the School needs to make reasonable adjustments;
- Details of trade union membership where subscriptions are deducted from your salary;
- Information about your use of School IT, communication and other systems and other monitoring information. A record that you have received and acknowledge that you will abide by our IT policies;
- Details in references about you that we give to others;
- Health and Safety Records;
- Where you use a car for work purposes, car make, model and details of your business use insurance, evidence of MOT and road tax;
- Digital imagery (such as photographs and video of trips and activities);
- CCTV footage (please refer to the CCTV Policy on the School's website).

This list is not exhaustive and may be subject to change, to access the current Privacy Notice, including the list of categories of information we process please see Teachershare > Policies > Current Policies > Data Protection > Workforce Privacy.

Why we collect and use workforce information

We need to collect and process your data so that we can:

- Run recruitment and promotion processes;
- Maintain accurate and up-to-date employment records and records of employee contractual and statutory rights;
- Maintain accurate and up-to-date contact details (including details of who to contact in the event of an emergency) to ensure effective communication with staff and to put into effect the school's emergency plans when necessary;
- Monitor compliance by you, us and others with our policies and contractual obligations;
- Operate and keep a record of disciplinary and grievance processes raised by or involving you, to ensure acceptable conduct within the workplace;
- Operate and keep a record of employee appraisals and performance related processes, to plan for career development, and for succession planning and workforce management purposes;
- Operate and keep a record of absence and absence management procedures, to allow effective workforce management;
- Obtain occupational health advice, to ensure that we comply with duties in relation to individuals with disabilities and meet our obligations under health and safety law;
- Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that we comply with duties in relation to leave entitlement;
- Ensure that employees are receiving the pay or other benefits to which they are entitled;
- Answer questions from insurers about any insurance policies which apply to you;
- Ensure effective general HR and business administration;
- Provide references on request for current or former employees;
- Prevent and detect fraud or other criminal offences;
- Respond to and defend the School in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure;
- Monitor diversity and equal opportunities and maintain and promote equality in the workplace;
- And any other reason which we may notify you of from time to time.

The School processes your data in accordance with our obligations under the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

The legal basis for our use of your personal data will generally be one or more of the following, under Article 6 of UK GDPR:

- processing is necessary for the performance of the contract of employment;
- processing is necessary to comply with a legal obligation (for example to comply with employment law, tax law, immigration law, health and safety law and safeguarding legislation);
- processing is necessary for the performance of a task carried out in the public interest (and when we process data for this reason we consider whether or not our interests are overridden by the rights and freedoms of employees or workers and have concluded they are not. An example would be when we need to manage performance or conduct);
- Consent (we will only use this in limited circumstances, for example equalities monitoring data).

When we process special categories of data or criminal conviction data we also ensure that one or more of the specified conditions are met under UK GDPR – Article 9.

- Equalities Monitoring:
 - We gather equalities data so that we can monitor equalities data in the workplace. The lawful basis for processing would be consent, and the additional condition that we will rely on is consent. Any equalities reporting would be anonymised. Only the Office team would have access to individualised data in this instance. You have the right to withdraw your consent to processing for this purpose at any time.
- Health and medical information:
 - This is collected to allow us to fulfil legal obligations e.g. those in relation to disabilities, to perform the contract e.g. to pay contractual sick pay and to manage sickness absence. The

conditions we will rely on are to carry out our obligations under employment law and for the purposes of occupational medicine.

- You can refuse to supply information about your health conditions and this may mean decisions will be taken solely on the information available.
- Trade union membership:
 - Information about trade union membership is processed when you authorise us to deduct trade union subscriptions from your salary. The lawful reason for processing is consent, as is the condition for processing.
- Criminal conviction data:
 - Most posts in schools require us to carry out DBS checks, and this means we may access criminal conviction data about you. The statutory guidance “Keeping Children Safe in Education” requires us to undertake the checks for these roles. We therefore have a legal obligation to do this, and the condition we will rely on is UK law.

Collecting workforce information

Much of your personal data is provided by you and is collected through information you give to us including:

- At the start of your working relationship e.g. your application form; new employee forms; identity documents such as your passport or your driving licence;
- During your work at the School e.g. when applying for employee benefits, maternity, adoption, or paternity leave, completing DBS applications, submitting fit notes and pension beneficiary nomination forms;
- From correspondence with you; or through interviews, meetings or other assessments.

In some cases, the School, with your consent, will collect personal data about you from third parties, such as references supplied by former employers and information from criminal records checks permitted by law.

Workforce data is essential for the School’s / local authority’s operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with UK GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please visit Teachershare > Policies > Current Policies > Data Protection > GDPR Data Protection Policy and Retention Schedule, also available from the School website.

Who we share workforce information with

We routinely share relevant information with:

- our local authority;
- the Department for Education (DfE);
- the Governing Body;
- other staff (relevant details only);
- our Payroll provider and HR consultancy (Strictly Education);
- our Occupational Health provider when required (Medigold);
- our childcare voucher provider (Sodexo);
- parents/carers and visitors to the school (basic details only, such as your name, job title and work email address);
- the public, such as in newsletters and articles on the school website (basic details only, as above);
- companies which provide IT and administrative services to the school;

- organisations and professionals who provide services to the school, such as music tuition (Croydon Music & Arts, the Steel Pans Agency,), therapy & counselling services (Croydon Drop-In), language tuition, school photography (Kittle Photographic), school travel and catering services (Nourish);
- the Police and organisations involved with safeguarding.

Our payroll provider organises the transfer of taxation payments and tax information to HMRC and data regarding pension payments to the Croydon sections of the Local Government and Teachers' Pension Schemes.

We require those third parties to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

Please see Appendix 2A for the most recent list of companies and organisations we are working with.

Why we share school workforce information

We do not share information about our 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

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections.

We are required to share information about our School employees with the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

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 Data Protection Officer, via the School Office.

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
- a right to seek redress, either through the ICO, or through the courts.

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/>

Contact

If you would like to discuss anything in this privacy notice, please contact the GDPR Lead, via the School Office.

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce;
- links to school funding and expenditure;
- supports 'longer term' research and monitoring of educational policy.

Data collection requirements

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>.

Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis;
- producing statistics;
- providing information, advice or guidance.

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

- To contact the department: <https://www.gov.uk/contact-dfe>

Appendix 2A: Providers of Services, IT & Software Suppliers 2023-24

The school works with a number of service providers and IT suppliers in order to effectively perform tasks in the public interest, or to comply with legal obligations. We share certain personal data with these organisations. For more information as to how the data is processed and kept secure, please refer to the organisation's data protection and privacy policies.

Asset for Schools – data extraction from SIMS (names & attendance data for Looked After Children) <https://www.assetforschools.org/website/privacy-policy>

Atomwide (AdEPT) – email accounts, online security, remote access & digital signage (pupil, parent, staff & governor data, including sensitive data. Pupil & staff photos.) <https://www.atomwide.com/privacy.html>

Capita plc - SIMS (school management information system: all pupil, parent, staff & governor data, including sensitive data and pupil photos) <https://www.capita-sims.co.uk/privacy-notice>

Capita plc – Reading Cloud library management system (pupil names, dates of birth, class/staff names)
<https://www.capita-readingcloud.co.uk/privacy-notice>

Nourish – school catering service: (pupils names, staff names, allergy information)

Collins Big Cat Phonics Ebook Library – digital copies of decodable phonics books (pupil name, class, staff school email address)

Croydon Music & Arts – music tuition (pupil names, ages and sensitive data required to ensure pupil safety/staff names & school email addresses) <https://www.croydon.gov.uk/democracy/data-protection-freedom-information/privacy-notices/education-youth-engagement-service-privacy-notice>

Croydon Council Local Government Pension Team – pensions support (support staff names, school email addresses & pension details) <https://www.croydonpensionscheme.org/croydon-pension-fund/privacy-policy-and-cookies>

Croydon Teachers Pensions – pensions support (teaching staff names, school email addresses & pension details) <https://www.croydon.gov.uk/democracy/data-protection-freedom-information/privacy-notices/corporate-privacy-notice>

Cunningham's – cashless till (pupil names, staff names and allergy information)
<https://www.cunninghams.co.uk/mint-project/uploads/666520732.pdf>

Croydon Drop In – counselling service for pupils (pupil names, ages and sensitive data required to provide the service/staff names & school email addresses). enquiries@croydondropin.org.uk

Eduspot (formerly Teachers2Parents) – texting service (pupil names/ parent, staff names & mobile numbers) <https://eduspot.co.uk/privacy-policy/>

Edukey (TES) - provision maps & intervention tracking (pupil data, including sensitive data/ staff names & school email addresses) <https://www.edukey.co.uk/privacy/>

Google G Suite – data storage & sharing (pupil & staff names, school email addresses)
<https://policies.google.com/privacy?hl=en-GB>

Groupcall - data extraction from SIMS for library system (pupil names/staff names & school email addresses). <https://www.groupcall.com/privacy>

Guys & St Thomas's NHS Foundation Trust – speech & language support for pupils (pupil names, ages and sensitive data; staff names & school email addresses). <https://www.england.nhs.uk/contact-us/privacy-notice/>

Kittle Photographic – school photographs (individual and class photos for pupils & staff).
<https://kittlephoto.com/privacy-policy.html>

London Grid for Learning – broadband, Egress accounts (staff names & school email addresses)
<https://static.lgfl.net/LgflNet/downloads/policies/LGfL%20Privacy%20Notice.pdf>

Octavo Partnership – IT service provider (access to SIMS data, including sensitive data for pupils and staff)
<https://www.octavopartnership.org/privacy-notice-complaints/>

Rakuten Overdrive – e-books (pupil ID's from library system)
<https://company.cdn.overdrive.com/policies/privacy-policy.htm>

ParentPay – school meal payments (pupil name, parent & staff names/email addresses/card details).
 Viewed only by school staff. <https://www.parentpay.com/privacy-policy/>

Steel Band Agency - music tuition (pupil names, ages and sensitive data required to ensure pupil safety/ staff names & school email addresses). info@steelpanagency.com

Strictly Education – HR & payroll provider (staff names, dates of birth, contact details, NI numbers & contract details) <https://www.strictlyeducation.co.uk/privacy-policy>

WhatsApp – group messaging (staff names & mobile numbers)
<https://www.whatsapp.com/legal?doc=privacy-policy&version=20120707>

Wonde – data extraction from SIMS for Eduspot, Education City & Edukey (pupil data, including sensitive data; parent names/mobile numbers/ staff names, school email addresses & mobile numbers)
<https://wonde.com/privacy-policy>

3PLearning – Mathletics & Readwriter online learning (pupil names, dates of birth/ staff names & school email addresses) <https://www.3plearning.com/privacy/>

Inventry – online register of staff on site and visitors (photographs taken of visitors).

<https://www.inventry.co.uk>

Times Tables Rockstars - (pupil names, dates of birth/staff names & school email addresses)

<https://ttrockstars.com/>

Single Central Record – (staff names and sensitive data required to ensure pupil safety)

<https://onlinescr.co.uk/>

Elmwood Junior School Data Protection Declaration

I confirm that I understand:

- The categories of my personal information that the School collects and uses.
- The reasons why the School processes my data.
- That the School has a lawful basis for collecting and using my personal information.
- That the School will always ask for explicit consent where this is required by law and I must provide this consent if I agree to the data being processed.
- That where the School is processing my data based on consent, I have a right to withdraw this consent at any time.
- That the School may share relevant information with the DfE, LA and other stated organisations and individuals.
- That the School does not share information about me with anyone without my consent, unless the law and our policies allow us to do so.
- That my data is retained securely in line with the school's GDPR Data Retention Policy.
- My rights to the processing of my personal information.
- Where I can find out more information about the processing of my personal data.
- The terms of the School's GDPR Data Protection Policy.

NAME: _____

SIGNATURE: _____

DATE: _____

Please return the signed declaration form to the School Office

Privacy Notice for Job Applicants

This privacy notice describes how Elmwood Junior School collect and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner, and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR. Successful candidates should refer to our privacy notice for staff for information about how their personal data is stored and collected.

Who Collects this Information

Elmwood Junior School is a “data controller.” This means that we are responsible for deciding how we hold and use personal information about you.

Under data protection legislation we are required to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice, together with any other policies mentioned within this privacy notice. This will assist you with understanding how we process your information and the procedures we take to protect your personal data.

Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

Categories of Information We Collect, Process, Hold and Share

We may collect, store, and use the following categories of personal information about you up to the shortlisting stage of the recruitment process: -

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Emergency contact information such as names, relationship, phone numbers and email addresses;
- Information collected during the recruitment process that we retain during your employment including proof of right to work in the UK, information entered on the application form, CV, qualifications;
- Details of your employment history including job titles, salary and working hours;
- Information regarding your criminal record as required by law to enable you to work with children;
- Details of your referees and references;
- Details collected through any pre-employment checks including online searches for data;
- Your racial or ethnic origin, sex, and sexual orientation, religious or similar beliefs.

We may also collect information after the shortlisting and interview stage to make a final decision on where to recruit, including criminal record information, references, information regarding qualifications. We may also ask about details of any conduct, grievance or performance issues, appraisals, time, and attendance from references provided by you.

How We Collect this Information

We may collect this information from you, your referees, your education provider, by searching online resources, from relevant professional bodies the Home Office and from the DBS.

How We Use Your Information

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Where we need to take steps to enter a contract with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.
- Where you have provided your consent for us to process your personal data.

Generally, the purpose of us collecting your data is to enable us to facilitate safe recruitment and determine suitability for the role. We also collect data to carry out equal opportunities monitoring and to ensure appropriate access arrangements are put in place if required.

If you fail to provide certain information when requested, we may not be able to take the steps to enter a contract with you, or we may be prevented from complying with our legal obligations.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

How We Use Particularly Sensitive Information

Sensitive personal information (as defined under the UK GDPR as “special category data”) require higher levels of protection and further justification for collecting, storing, and using this type of personal information. We may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our pension scheme);
- Where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else’s interests) and you are not capable of giving your consent.

Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

Sharing Data

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

These include the following: -

- Academic or regulatory bodies to validate qualifications/experience (for example the teaching agency);
- Referees;
- Other schools;
- DBS; and
- Recruitment and supply agencies.
- Our Local Authority to meet our legal obligations for sharing data with it;
- Medical health clearance required as part of the recruitment process

We may also need to share some of the above categories of personal information with other parties, such as HR consultants and professional advisers. Usually, information will be anonymized, but this may not always be possible. The recipients of the information will be bound by confidentiality obligations. We may also be required to share some personal information with our regulators or as required to comply with the law.

Retention Periods

Except as otherwise permitted or required by applicable law or regulation, the school only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

Once we have finished recruitment for the role you applied for, we will then store your information in accordance with our Retention Policy.

Security

We have put in place measures to protect the security of your information (i.e., against it being accidentally lost, used, or accessed in an unauthorized way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach policy, which can be found on the school's website.

Your Rights of Access, Correction, Erasure and Restriction

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances by law, you have the right to:

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
- To object to processing in certain circumstances (for example for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact Robert Pollock in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

Right to Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing, and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact Robert Pollock. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

How to Raise a Concern

We hope that Robert Pollock can resolve any query you raise about our use of your information in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by Robert Pollock, then you can contact the DPO on the details below: -

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

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.

admin@elmwood-jun.croydon.sch.uk

0208 684 4007