

Elmfield Rudolf Steiner School

Data Protection Policy

Issued by	Operations Manager
Last review	19/08/22
Approved by Council	
Circulation	Elmfield Website Google Drive - Policies

Contents

Policy Section	Page Number
1. Purpose	3
2. Introduction	3
3. Definitions and Common Terminology	3
4. Data Protection Principles and How Elmfield School Complies	4
5. Data Processing Measures	6
6. Use of Personal Data	6
7. Photographs and Videos	7
8. Data Security and Storage of Data	7
9. A Data Subject's Rights	8
10. Subject Access Requests	8
11. Complaints to the Information Commissioner	10
12. Destruction of Records	10
13. Data Breaches	11
14. Training	11
15. Contact Details	11

1. Purpose

Elmfield School's Data Protection Policy is intended to ensure that personal information is dealt with securely and in accordance with the Data Protection Act 2018, UK General Data Protection Regulation (GDPR). It will apply to all data held by the school regardless of the way it is used, recorded and stored and whether it is held by the school in paper files or electronic form.

2. Introduction

Elmfield School collects and uses certain types of personal information about pupils, parents, staff, volunteers, governors, job applicants and other individuals who come into contact with the school in order to provide education, employment and other associated functions. Our school is required by law to collect and use certain types of information to comply with statutory obligations related to education, safeguarding and employment, and this policy is intended to ensure that personal information is dealt with securely and in accordance with the GDPR. The GDPR applies to all electronic and manual data files containing personally identifiable information (PII) or sensitive data. This policy will apply to any member of staff in the school who process PII. Elmfield School will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the GDPR. Elmfield School will take all reasonable steps and apply robust procedures to ensure that all PII is held securely and is not accessible to unauthorised persons. This policy will be updated when amendments to the data protection legislation are made or to reflect best practice where necessary. The policy will be reviewed every 2 years.

3. Definitions and Common Terminology

Data Controller – a natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Data Processor – a natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the data controller.

Data Subject – an identified or identifiable living individual whose personal data is held or processed.

Personally Identifiable Information – any information relating to an identified or identifiable, living individual.

Special Categories of Personal Data – personal data, which is more sensitive and so needs more protection, including information about an individual, racial, or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetics; biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes, Health – physical or mental, sex life or sexual orientation.

Data Protection Officer – a person who is tasked with helping to protect PII and helping an organisation to meet the GDPR compliance requirements, does not hold ultimate accountability for compliance.

Subject Access Request – a right that a person has to obtain a copy of information held about them by the organisation.

Data Breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

ICO – Information Commissioners Office (Supervising Authority in the UK) 4. Data Protection Principles and How Elmfield School Complies

As the Data Controller, Elmfield School processes personal data in line with the GDPR sets of guiding principles as follows:

4. Data Protection Principles How the School Complies

As the Data Controller, Elmfield School processes personal data in line with the GDPR sets of guiding principles as follows:

Data Protection Principles	How the School Will Comply
<p>Legality, Transparency and Fairness</p> <p>Personal data will only be processed by the School, where it is able to demonstrate that it has a 'lawful basis' for the processing activity</p>	<p>A data mapping document identifies all data processed by the School to monitor and review the 'lawful basis' for collecting, processing, sharing, storing, and destroying data. A Privacy Notice for pupils, parents/carers, staff, and visitors to school is readily available and on the School's website, and includes all details of the data collected. The privacy notice also contains details of how a data subject (pupil, parent, member of staff etc) can access their data, which is stored and processed by the School</p>
<p>Purpose Limitation</p> <p>Personal data should be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes</p>	<p>A data mapping document will identify the purposes for which processing will take place, the description of the categories of individuals and personal data, the categories of recipients of the data (eg third party organisations who the School shares the data with). Retention schedules for the personal data will also be noted. Robust procedures are in place to ensure PII is only used for the purpose that it was collected for</p>
<p>Data Minimisation</p> <p>The personal data must be 'Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'</p>	<p>Data collection forms will be regularly reviewed to ensure information is appropriate and not excessive</p>

<p>Accuracy</p> <p>All reasonable steps will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay</p>	<p>Data will be regularly checked to ensure it is as accurate as possible through a variety of measures:</p> <ul style="list-style-type: none"> ○ Issue data collection forms on an annual basis to parents/carers to check and amend data held ○ Reminders on school newsletters ○ During Parents' Evening and/or Pupil progress meeting
<p>Storage Limitation</p> <p>Personal data shall be kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.</p>	<p>Retention periods for various data held in the School are recorded within the data mapping document.</p> <p>The School refers to the Information Record Management Toolkit to establish appropriate retention periods and data is archived and destroyed as set out in these guidelines.</p>
<p>Integrity and Confidential (Security)</p> <p>Personal data will be processed in a manner, which 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</p>	<ul style="list-style-type: none"> ○ Electronic devices, such as computers, laptops, iPad, etc are password protected. Passwords are a minimum of 8 characters and contain a mixture of upper-case, lowercase letters and numbers. ○ Passwords are changed on a regular basis ○ Computers are locked when not in use. ○ Secure transmission of data: Secure password protected exchange sites are used to transfer data ○ Clear desk policy is in place around school. ○ Paper based data is stored in secure lockable cabinets. ○ Offices around school are locked at all times, when not occupied. ○ Access to the school site is secure with an intercom secure system in operation
<p>Accountability</p> <p>Elmfield School, as data controller, will be able to demonstrate compliance with the previous principles.</p>	<p>A data protection officer is appointed.</p> <p>A data protection lead is first point of contact.</p> <p>Elmfield School has clear procedures in place for handling a data breach and a Subject Access Request 4 Third party agreement/assurances are in place for all data shared with such organisations who process data on behalf of the school.</p> <p>School staff are GDPR trained on an annual basis.</p>

Regular Data Audits and reviews will be undertaken to check the robustness of processes and systems for continued GDPR compliance

5. Data Processing Measures

The school have put measures in place to show that data protection requirements are integrated into all data processing activities. These include:

- Appointment of a suitably qualified Data Protection Officer (DPO) which is provided to the school by SIPS Education, and contactable via gdpr@sips.co.uk or 0121 296 3000
- Maintaining up to date, data mapping records to ensure that processing of personal data or a specific purpose is undertaken in line with the data protection principles as set out in GDPR
- Where the school is introducing new technologies or it is considered that the processing of personal data presents a high risk to the rights and freedoms of individuals, data protection impact assessments will be completed by the relevant staff in liaison with the
- Data Protection Lead within the School

6. Use of Personal Data

Elmfield School processes personal data on pupils, parents, staff, visitors, trustees etc. Personal data for each individual will be processed in accordance with the GDPR principles as outlined in point

In accordance with the principle of transparency, the School has developed and will maintain privacy notices for different categories of data subject. These outline the categories of data captured, the purpose of processing, and if the information is shared with third parties.

Our data mapping document informs the content of our privacy notices, which can be found on our website or within the shared area of the School's electronic system for staff.

Privacy notices have been drafted for the following categories of data subjects:

- Pupils
- Parents/carers
- Staff and volunteers
- Visitors and contractors
- School trustees
- Job applicants

7. Photographs and Videos

The school may take photographs and videos of individuals as part of school activities. Such images may be used for:

- Notice boards around school, school newsletters, brochures etc
- External agencies such as the school photographer, newspapers/media campaigns
- School website or social media

In order to do this we will obtain written consent from parents/carers before we take photographs or videos of your child. We will do this as part of your child's induction process. When we seek your consent, we will clearly explain how the photographs and/or videos are to be used.

You have the right to withdraw consent at any time, upon which we will delete any images already taken and we will not distribute those images further.

As part of our 'public task', we may take a photograph of your child without requesting consent from you. This would be in circumstances where identification of a child with an existing medical condition/allergies is required in order to meet the needs of your child and to keep them safe, or to be stored on the School's MIS and retained for identification purposes only.

Where photographs and/or videos are taken by parents/carers at school events for your own personal use, the requirements of data protection legislation do not apply. However, we do ask that, should your photos/videos capture images of other pupils in addition to your own child, you do not share these in any public way (including on social media sites) for safeguarding reasons, unless all relevant parents/carers have given their consent for you to do so.

8. Data Security and Storage of Data

All devices used in school and provided to staff including mobile phone, laptop, memory stick, tablet, external hard drive, computer etc, will be encrypted. Care will be taken to safeguard the equipment against loss or damage. Passwords used on all devices to encrypt information, will not be shared or written down.

All devices provided by the School will only be used for the purposes for which they were supplied.

Memory sticks that do not require a password to access the data contained on them will not be used and are not permitted by the School.

Any storage devices no longer required, which may contain information that is surplus to requirements will be disposed of securely.

Media such as CDs or DVDs, which contain data and are no longer required will be physically destroyed.

Paper-based documents and files containing personal data, which is stored in school will be protected by one of the following measures:

- Locked filing cabinets with restricted access to keys by appropriate staff only. Keys
- will be stored away from cabinets
- Locked safe
- Stored in a secure area protected by access controls

Depending on the content of the sensitive data contained within paper-based documents and files, an appropriate member of staff will be responsible for the storing and protecting of the data in line with the secure filing system process.

9. A Data Subject's Rights

Under the GDPR, with regards to their personal information, data subjects have the following rights:

- To be informed about the collection and the use of their personal data
- Of access personal data and supplementary information
- To have inaccurate personal data rectified, or completed if it is incomplete
- To erasure (to be forgotten) in certain circumstances
- To restrict processing in certain circumstances
- To data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services
- To object to processing in certain circumstances
- Complain to the Information Commissioner

Individuals should submit any request to exercise these rights to the Data Protection Lead in school; this can be done verbally or in written form. If staff receive such a request, they will immediately forward it to the Data Protection Lead, who will liaise with the Data Protection officer as necessary.

10. Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the School holds about them, as well as:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purpose of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for or, if this isn't possible, the criteria used to determine this period
-

- Where relevant, the existence of the right to request rectification, erasure, or restrictions, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority;
- The source of the data, if not the individual
- The safeguards provided if the data is being transferred internationally

It is important to bear in mind that a child's personal data is just that – their data – and does not belong to their parent/carer. As such, if a parent or carer wishes to make a subject access request for data relating to their child, the pupil needs to have given their consent dependent on their age and level of understanding.

The age of 13 is used as a guide to determine when a child is generally likely to be mature enough to understand their rights, and accordingly any requests for their personal data from this age onwards would generally be expected to come from the child themselves.

For children below this age, it is less likely that they will fully understand the implications of SARs, and so it would normally be acceptable for the request to come from the parent/carer. However, both situations are used as a guide only, and each request (and requestor) will be judged on an individual case-by-case basis.

Subject access requests can be submitted in any form to any member of staff within the School. However, the School may contact the requester for more details in order to be able to respond to requests appropriately. If staff receive a subject access request in any form they will forward it to the data protection lead within the School immediately. The data protection officer will also be advised to ensure appropriate support is provided to the School to fulfil the request. Parents can also contact the data protection lead within the School to make a subject access request. The details are as follows: Vikki Highams, Operations Manager, 01384 394633 or vikki.highams@elmfield.com.

Information about how to make a Subject Access Request or for more details can be obtained from the Data Protection Lead within the School, contact details above. Alternatively, see Appendix A for completion if you wish to submit a Subject Access Request now.

Responding to a Subject Access Request.

When responding to requests, the School may:

- Contact the individual via telephone to confirm the request has been made by them
- Ask the individual to provide further details so that the School can verify and confirm the data required
- Request two forms of identification of the individual; proof of address will also be verified
- If a third party is requesting data, written authority or a power of attorney will be verified
- Requests will be responded to within one calendar month from receipt of the request

However, if additional information is required in order for the School to fulfil the request, the response period will be from receipt of all information obtained; this includes receipt of proof of identity and proof of address where relevant.

Based on the complexity of the request and in line with Article 12 (3) GDPR, the timeframe in

which to respond to a Subject Access Request may be extended up to three calendar months if required. In such instances the School will liaise at the earliest opportunity, with the Data Protection Officer and the requester, to advise of the response time or any delays. Data provided to the requester may contain details of other individuals and therefore such data will be redacted (blacked out) to protect those individuals' identity and personal data. Details contained within the documents will pertain to the appropriate individual only.

When responding to the request, the School may decide against disclosing information for a variety of reasons, including if it:

- Would have an adverse effect on the rights and freedom of others
- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Contains adoption and parental order records
- May be used in legal proceedings
- Would include personal data relating to another individual, where the School cannot sufficiently anonymise the data to protect that individual's rights, we do not have their consent to release that individuals' data, and it would be unreasonable to proceed without such consent

If a request is determined to be 'unfounded or excessive', the School has the right to refuse the request or, in some cases, charge a reasonable fee to cover the administrative costs of responding to the request.

If the School refuses a request, they will inform the individual of the reasons why and advise them of their right to complain to the ICO, if they wish to do so.

11. Complaints to the Information Commissioner

If you are dissatisfied with the way the School has handled your request and want to make a complaint, you may write to the Information Commissioner, who is an independent regulator. Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.

The Information Commissioner can be contacted at: Information Commissioners Office, Wycliffe House Water Lane Wilmslow Cheshire, SK9 5AF Tel: 0303 123 1113; website: <https://ico.org.uk>

12. Destruction of Records

Personal data that is no longer required either because it is out of date, inaccurate or in line with the School retention policy, will be disposed of securely.

The School will shred paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the School's behalf. If we do so, a third-party assurance will be obtained to provide us with sufficient guarantees that the company complies with data protection law.

13. Data Breaches

The School will make all reasonable endeavours to ensure that there are no personal data breaches. The School has robust procedures in place to deal with any personal data breaches and will notify the ICO where we are legally required to do so. Data subjects will be notified in instances where the rights and freedoms of such individuals have been compromised. The School will work with their Data Protection Officer to address a breach and school processes will be reviewed to mitigate risks, if it is appropriate to do so. In the event of you becoming aware of a data breach, please notify Vikki Highams, Operations Manager, 01384 394633 or vikki.highams@elmfield.com as soon as possible, with details.

14. Training

All staff and trustees are provided with data protection training on an annual basis, or more regularly where there are changes to legislation guidance or school processes. Training is also part of the induction process for new employees to the school.

15. Contact Details

If you wish to make a Subject Access Request (see point 11 and/or appendix A) or have general queries in relation to data protection within school, these should be directed to the Data Protection Lead within the school: Vikki Highams, Operations Manager, 01384 394633, vikki.highams@elmfield.com.

In the first instance concerns, questions, or complaints can be discussed with the Data Protection Officer at gdpr@sips.co.uk or telephone number 0121 296 3000. This would include situations where there are concerns about the way a Subject Access Request or a data breach has been addressed or the robustness of policy or procedures within school in relation to Data Protection.

If you remain dissatisfied with the assistance that you have received, or if you do not feel your subject access request has been dealt with appropriately, or you have concerns with regards to a possible breach, you can make a formal complaint to the Information Commissioners Office. This can be done via the website at www.ico.org.uk. Telephone: 0303 123 1113 or in writing to: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5A

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any change or amendments made to the UK General Data Protection Regulation and Data Protection Act 2018