GDPR Data Privacy Policy

Schools Name	**The Alderton Infant School**
Document Version	**v1**
Date	**May 2018**
Person Responsible	**Mrs S Dalby**
Next Review Date	**May 2020**

Introduction

The Epping Forest Schools Partnership Trust is transparent about how it collects and uses Personal Identifiable information (PII). This policy sets out the Trust will meet its obligations under the EU General Data Protection Regulation.

The Trust is developing a Privacy Framework of Policies and Procedures that will help all staff adhere to the requirements of the EU GDPR. This Policy forms the core to the framework. Privacy has and will be considered for three main categories:

- Pupils
- Staff
- Parents

This Privacy Policy applies to all Governors and staff in the trust. All staff must read, understand and comply with this Privacy Policy. Compliance with this Policy is mandatory. It will be the responsibility of the CEO of the trust and his delegated to staff to ensure compliance. The Trust will be appointing a data protection officer (DPO) who will promote a culture of data privacy and advise on legal obligations.

This Policy will cover the following:

1. What is Personal Data
2. Key Definitions
3. Information audit and documentation of processing
4. Lawful basis for processing
5. Consent
6. The right to be informed
7. The right of access
8. The right to rectification
9. The right to erasure
10. The right to restrict processing
11. The right to data portability
12. The right to object
13. Accountability and Governance
14. Data protection awareness training.
15. Contracts with data processors.

This Policy has been approved by the Senior Management of the Trust, published and communicated to all staff. It will be reviewed and updated at planned intervals or when required to ensure it remains relevant.

1. What is Personal Data

The EU GDPR applies to 'personal data' meaning any information relating to a person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including the following:

- Name
- Identification number
- Location data or online identifier (reflecting changes in technology and the way organisations collect information about people)
- Physical
- Physiological
- Genetic
- Mental
- Economic
- Cultural
- Social

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

The GDPR refers to sensitive personal data as "special categories of personal data". These include:

- Racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- Genetic or biometric data (where processed to uniquely identify an individual.)
- Health information
- Sex life
- Sexual orientation

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

2. Key Definitions

- Processing - Obtaining, recording and holding data
- Data Subject - The person whose personal data is held or processed
- Data controller - A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
- Data processor - A person, other than an employee of the data controller, who processes the data on behalf of the data controller

3. Information audit and documentation of processing

All schools in the Trust conduct regular information audits to understand what personal data they hold and how if flows through the school's systems. An information asset register will be details what personal data we hold, where it came from, who we share it with and what we do with it.

Data Privacy requires a risk-based approach and as such, during the information audits schools identify the risks attached to the personal data. This is documented and maintained in a risk register.

Staff guidelines exist to assist staff on how to manage personal information.

The Data Protection Officer will be responsible for auditing and reporting on compliance.

4. Lawful basis for processing

GDPR requires us to look at the types of data processing that we carry out and identify our lawful basis for doing so. We regularly review the types of data we hold on Pupils, Staff and Parents and examine what legal basis can be applied. Our privacy notices to parent and staff set out our current legal basis for processing.

5. Consent

Consent is just one of the legal basis for processing personal data and should not be relied on. Obtaining Consent forms are used when a new pupil starts at a school. This consent will be for very few processing activities, such as contacting parents/guardians in relation to fund raising or marketing activities or taking photographs of a pupil.

The obtaining consent form meets the following GDPR requirements:

- Prominent and separate from other terms and conditions.
- Ask individuals to positively opt in.
- Use unticked opt-in boxes or similar active opt-in methods.
- Use clear, plain language that is easy to understand.
- Specify why we want the data and what we are going to do with it.
- Give granular options to allow individuals to consent separately to different types of processing wherever appropriate.
- Name the school and any specific third-party organisations who will rely on this consent.
- Tell individuals they can withdraw consent at any time and how to do this.
- Ensure that individuals can refuse to consent without detriment.
- Don't make consent a precondition of service.

We keep records of when and how we obtained consent from the individual as well as exactly what the individuals were told at the time. Consent is regularly reviewed to check that the relationship, processing and purposes have not changed. Specifically, consent will be renewed when the pupil progresses from Key Stage 1 to Key Stage 2. The schools will be acting on withdrawals of consent as soon as they can.

Where current consent doesn't meet the above standards or is poorly documented, the school will seek to obtain refreshed GDPR-compliant consent.

Where schools offer online services directly to children eg online homework, creating personal email addresses for pupils, creating online profiles etc they will ensure that

they obtain the parent or guardian's consent or authority. Records will be kept regarding obtaining and maintaining consent.

6. The right to be informed

The right to be informed covers some of the key transparency requirements of the GDPR. It is about providing people with clear and concise information about what you do with their personal data.

Articles 13 and 14 of the GDPR specify what individuals have the right to be informed about. This is managed through our privacy notices.

Privacy notices are displayed on every school's website and is communicated to parents during the admissions process. Staff are also provided with a privacy notice when they join the school and copies are made readily available. Our privacy notices meet the following GDPR requirements:

- let individuals know who you are, why you are processing their data and who you share it with;
- be concise and to the point;
- be easy to understand;
- be clearly signposted and easy to access;
- be written in clear and plain language, particularly if addressed to a child;
- free of charge;
- include different information depending on whether you obtained the data directly from the individual or not; and
- be reviewed regularly to make sure it remains accurate and up to date.

Where required, the Trust's privacy notices to children will be concise, transparent, intelligible and easily accessible. They will be written in clear and plain language that can be understood by a child (age appropriate). They will explain the risks involved in the processing and the safeguards we have put in place. The notice will be reviewed regularly to make sure it remains accurate and up to date.

7. The right of access

Under GDPR the data subject has the right to confirm that their data is being processed and have access to their personal data. As such, processes are in place to allow the Trust to recognise and respond to any subject access requests within 30 days. These processes are detailed in the data protection policy. Staff are regularly

trained to provide awareness and specialist training is provided to individuals who deal with any requests.

8. The right to rectification

The fifth principle of the EU GDPR states that personal data must be:

"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".

Also, under Article 16 of the GDPR individuals have the right to have inaccurate personal data rectified.

As such, the trust has implemented procedures to allow individuals to challenge the accuracy of the information we hold about them and have it corrected if necessary. We also have procedures in place to inform any data processors (third parties) that we have disclosed the information to, about the rectification.

To support this, we also have a documents management framework that sets out guidelines for creating and keeping records (including emails). Data sets (such as what is required in a pupil file) are regularly reviewed to ensure the information continues to be adequate for the purposes of processing (for which it was collected). The document management framework provides a retention guide detailing when to review information to identify if we need to correct inaccurate records, remove irrelevant ones and update out-of-date ones. Staff training on data privacy ensures that we are promoting data quality to staff.

9. The right to erasure

Article 17 of the GDPR empowers data subjects the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;

- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child.

Our document management framework provides a retention guide seting out how long to keep the information for and how to dispose of it (preventing the disclosure of personal data prior to, during and after disposal). The schedule is reviewed regularly to ensure that it continues to meet the Trust's needs and statutory requirements. This review process is a dedicated responsibility of a trained member of staff.

We respect the rights of the data subject and as such, we have procedures in place which allow individuals to request the deletion or erasure of their information that we hold (where there is no compelling reason for its continued processing). We also have procedures in place to inform any data processors (third parties) who we shared the information with about the request for erasure. To complete the entire erasure process, we have procedures to delete information from any back-up systems.

Where we use third parties to dispose of personal data, we have ensured that the contracts include the requirement for them to have appropriate security measures and the facility to allow us to undertake an audit.

10. The right to restrict processing

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that the Trust uses their data. This is an alternative to requesting the erasure of their data. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information we hold or how we have processed their data. In most cases we will not be required to restrict an individual's personal data indefinitely but will need to have the restriction in place for a certain period of time. When processing is restricted, we are permitted to store the

personal data, but not use it. An individual can make a request for restriction verbally or in writing and we have one calendar month to respond to a request.

Individuals have the right to request we restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

As a matter of good practice we automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question.

We have a process in place to act on an individual's request to block or restrict the processing of their personal data. Where possible, we will inform any data processors (third parties) that we have shared the information with.

11. The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

Personal data will be provided in a structured, commonly used and machine-readable form. There will be appropriate technical measures in place to protect the data. The medium in which the data is provided allows individuals to move, copy or

transfer that data easily from one organisation to another without hindrance. The trust will provide the information free of charge.

12. The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Our privacy notice(s) inform individuals of their right to object at the point of first communication. The privacy notice(s) also detail to the data subject how to submit an objection request (include an online option). We have processes in place to investigate an individual's objection to the processing of their personal data within the legitimate grounds outlined within the GDPR. We also provide training and raise awareness amongst our staff to ensure they are able to recognise and respond to an objection raised by an individual.

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

Where personal data is processed for direct marketing purposes:

- The trust will stop processing personal data for direct marketing purposes as soon as an
- objection is received.
- The trust cannot refuse an individual's objection regarding data that is being processed for
- direct marketing purposes.

Where personal data is processed for research purposes:

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

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

13. Accountability and Governance

The accountability principle in Article 5(2) requires the Trust to demonstrate that we comply with the principles of GDPR. As such, we have a process to monitor compliance to this and related policies. We regularly test the measures that are detailed within the policies to provide assurances that they continue to be effective. We ensure that responsibility for monitoring compliance with the policies is independent and have a Data Protection Officer for this role. The DPO will report any results to senior management.

14. Data protection awareness training.

We provide induction training on or shortly after staff are appointed and update all staff at regular intervals or when required (for example, intranet articles, circulars, team briefings and posters). We provide specialist training for staff with specific duties, such as marketing, information security and database management.

15. Contracts with data processors.

Where we use a processor (a third party who processes personal data on your behalf) there is a written contract in place. These contracts ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).

16. Managing information risks

We have an information security policy and supporting procedures which assign responsibilities to support good information risk management. Our information risk register logs any identified threats, vulnerabilities, and potential impacts which are associated with the school's activities. Where appropriate and proportionate, we have applied controls to mitigate the identified risks and we regularly test these controls to ensure they remain effective.

17. Technical and organisational measures

Where possible, we look to continually minimise the amount and type of data we collect, process and store. We chose to pseudonymise the personal data where appropriate to render the data record less identifying and therefore reduce concerns with data sharing and data retention. We regularly undertake reviews of our public-facing documents, policies and privacy notice(s).

We also review and improve our data security features and controls on an ongoing basis.

18. Data Privacy Impact Assessments

The Trust has a privacy by design approach. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the trust's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to our reputation which might otherwise occur. A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

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

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

19. Information security policy supported by appropriate security measures.

We have implement and communicated (to all staff) an information security policy which covers key information security topics such as network security, physical security, access controls, secure configuration, patch management, email and internet use, data storage and maintenance and security breach / incident management. We have applied appropriate technical and organisational measures to ensure a level of security appropriate to the risk. We conduct periodic checks for compliance with policy, to give assurances that security controls are operational and effective. We also deliver regular staff training on all areas within the information security policy.

20. Transferring personal data outside the European Economic Area

We ensure that any data we transfer outside the EU is handled in compliance with the conditions for transfer set out in Chapter 5 of the GDPR. We ensure that there is adequate safeguards and data security in place, that is documented in a written contract using standard data protection contract clauses. We have implement measures to audit any documented security arrangements on a periodic basis.

21. Data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Broadly this means the incident has affected the confidentiality, integrity or availability of personal data.

We will report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. Where we are unable to fully investigate the breach within 72 hours, we will provide the required information in phases and without undue delay. We will prioritise the investigation, give it adequate resources, and expedite it urgently.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, we will inform those concerned directly and without undue delay. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. We will therefore assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring.

In such cases, we will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. When informing an individual about a breach we will use clear and plain language. We will inform them about the nature of the personal data breach and, at least:

- the name and contact details of our data protection officer
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

We record all breaches, regardless of whether or not they need to be reported to the ICO. We will document the facts relating to the breach, its effects and the remedial action taken.

As with any security incident, we investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.