Thaxted Primary School

Data Protection Policy

Policy Date: Autumn 2021	**Review Date:** Autumn 2022	**Responsible Person:** Headteacher **In Conjunction with:** Business Manager
Other Policies to be read in conjunction with this policy:		Data Protection Policy Statement Statutory Requests for Information Privacy Notices Security Measures

This policy was approved by the Full Governing Board on the 15/10/2021

Thaxted Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

1. PURPOSE

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998 and General Data Protection Regulations 2018 and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to the guidelines below.

2. WHAT IS PERSONAL INFORMATION?

Personal information or data is defined as data, which relates to a living individual who can be identified from that data, or other information held.

3. GUIDELINES FOR STAFF

- All employees must comply with the requirements of Data Protection Law and Article 8 of the Human Rights Act when processing the personal data of living individuals.
- Where personal data is used, the school must make sure that the data subjects have access to a complete and current Privacy Notice.
- The school must formally assess the risk to privacy rights introduced by any new (or change to an existing) system or process, which processes personal data.
- The school must process only the minimum amount of personal data necessary to deliver services.
- All employees who record opinions or intentions about service users must do so carefully and professionally.
- The school must take reasonable steps to ensure the personal data we hold is accurate, up to date and not misleading.
- The school must rely on consent as a condition for processing personal data only if there is no relevant legal power or other condition.
- Consent must be obtained if personal data is to be used for promoting or marketing goods and services.
- Consent will expire at the end of each 'Key Stage' period unless it is reconfirmed
- The school must ensure that the personal data it processes is reviewed and destroyed when it is no longer necessary.
- If the school receives a request from a member of the public or colleagues asking to access their personal data, it must handle it as a Subject Access Request under the Data Protection Act 2018 or a request for the Education Record under the Education (Pupil Information) (England) Regulations 2005.
- If the school receives a request from anyone asking to access the personal data of someone other than themselves, personnel must fully consider Data Protection law before disclosing it.

- When someone contacts the school requesting it changes the way it is processing their personal data, personnel must consider their rights under Data Protection law.
- Employees of the school must not access personal data, which they have no right to view.
- Employees of the school must follow system user guidance or other formal processes which are in place to ensure that only those with a business need to access personal data are able to do so
- The school must share personal data with external bodies who request it only if there is a current agreement in place to do so or it is approved by the Data Protection Officer or SIRO.
- Where the content of telephone calls, emails, internet activity and video images of employees and the public is recorded, monitored and disclosed this must be done in compliance with the law and the regulator's Code of Practice.
- All employees must be trained to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely.
- When using 'data matching' techniques, this must only be done for specific purposes in line with formal codes of practice, informing service users of the details, their legal rights and getting their consent where appropriate.
- The school must maintain an up to date entry in the Public Register of Data Controllers
- Where personal data needs to be anonymised or pseudonymised, for example for research purposes, the school must follow the relevant procedure.
- The school must not share any personal data with an individual or organisation based in any country outside of the United Kingdom without seeking advice from the SIRO or Data Protection Officer
- The school must identify Special Categories of personal data and make sure it is handled with appropriate security and only accessible to authorised persons.
- When sending Special Category data to an external person or organisation, it should be marked as "OFFICIAL-SENSITIVE" and where possible, sent by a secure method.

4. GENERAL STATEMENT

The school is committed to maintaining the above principles at all times. Therefore, the school will:

- Approve and review a compliant Privacy Notice annually and make it available to the data subjects.
- Complete and approve a Privacy Impact Assessment, or Data Protection Impact Assessment where the processing is "high risk" to the rights of the data subjects.
- Ensure that the means it uses to gather personal data (such as forms etc) only asks for the information that is required in order to deliver the service.
- Consider that anything committed to record about an individual may be accessible by that individual in the future or challenged over its accuracy.
- Check annually the currency of the data held about service users and if contact is re-established with a service user it will check that the information held is still correct.
- Review personal data regularly and delete information, which is no longer required; although it must take account of statutory and recommended minimum retention periods. Subject to certain conditions, the law allows organisations to keep indefinitely personal data processed only for historical, statistical or research purposes. The Retention Schedule will give guidance in these areas. All data will be destroyed appropriately and securely.
- Follow the points in the Consent form completed by parents
- Send to parents in the last year of a key stage a communication to ask them to refresh their consents. If they do not respond ahead of a deadline date then consent should be assumed to be no longer valid.
- By following the points in the Statutory Requests for Information Policy, be aware that data subjects can ask others to make a request on their behalf. There must be evidence of consent provided by the Data Subject to support this.

- By following the points in the Statutory Requests for Information Policy recognised that such requests would typically be managed under the Freedom of Information Act (if from a member of the public) or under Data Protection or Justice law if for a criminal investigation, however the decision whether or not to disclose someone's personal data to a third party must satisfy the requirements of Data Protection law
- Review the impact of any requested change on any statutory duty being fulfilled by the Organisation.
- Ensure that all staff are aware, through training and guidance from the school's SIRO, what information is appropriate for them to access to do their job. Systems and other data storage must be designed to protect access to personal data. All staff must inform their manager if they have access to data, which they suspect they are not entitled to view.
- Ensure that appropriate security controls are in place and rules to support those controls are followed. The following should be in place:
    - technical methods, such as encryption, password protection of systems, restricting access to network folders;
    - physical measures, such as locking cabinets, keeping equipment like laptops out of sight, ensuring buildings are physically secure; and
    - organisational measures, such as:
        - Providing appropriate induction and training so that staff know what is expected of them. In all cases training will be compulsory relevant to each role. Training content for each role will be determined by feedback on current training methods and the outcome of investigating security incidents. This will be reviewed frequently. Records will be kept of induction training and annual refresher training.
        - Taking reasonable steps to ensure the reliability of staff that access personal data, for example, by the use of Disclosure and Barring Service (DBS) checks.
        - Making sure that passwords are kept secure, forced to be changed after an agreed period and are never shared.
- Ensure that employees and members of the public are fully aware of what personal data is being recorded about them and why, and it what circumstances that data may be used. Operation of overt surveillance equipment such as CCTV must always be done in line with relevant codes of practice captured in the Surveillance Management. Procedure. Any covert surveillance must be done in line with the provisions in the Investigatory Powers Act (2016)
- Publish a Data Minimisation Procedure and adhere to it.
- Store Special Categories of Personal Data securely and in a way that access is restricted to those internal staff that have a valid need to access it. It should only be shared externally after verifying that the recipient is entitled to access this data through secure means. Special Categories of Personal Data are information revealing *racial or ethnic origin*, *political opinions*, *religious or philosophical beliefs*, or *trade union membership*, and *genetic data*, *biometric data* for the purpose of uniquely identifying an individual, *data concerning health* or *data concerning an individual's sex life or sexual orientation*.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.

5. COMPLAINTS

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

6. BREACHES

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against the employee.

7. REFERENCES

- General Data Protection Regulations 2018
- Data Protection Act 1998
- Article 8, The Human Rights Act 1998
- Education (Pupil Information) (England) Regulations 2005
- Investigatory Powers Act 2016

8. REVIEW

This policy will be reviewed annually by the Headteacher or nominated representative and approved by the school's Governing Body.