THRUSSINGTON C. OF E. PRIMARY SCHOOL (Academy.)
DATA PROTECTION POLICY.

Thrussington C. of E. Primary School is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents, governors and volunteers.

Introduction.

Thrussington C. of E. Primary School needs to gather, use and retain certain information about individuals. This can include our employees, pupils and other people the School has a relationship with or may need to contact. It allows the School to monitor performance, achievement and health and safety, as an example.

This policy describes how this personal data must be collected, handled and stored to meet the School's data protection standards and to comply with the law.

This Act is separate and distinct from the Human Rights Act, 1998.

Why this policy exists.

This data protection policy ensures that Thrussington School:

- Complies with data protection law and follows good practice
- Protects the rights of staff, pupils, parents and other individuals associated with the School
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

1. The Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The School collects a large amount of personal data every year, including: staff records, names and addresses of those requesting information such as prospectuses, examination information, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of local authorities, government agencies and other bodies.

It applies to all data that the School holds relating to identifiable individuals, even if that information falls outside the Data Protection Act, 1998. This can include:

- Names of individuals
- Postal addresses

- E-mail addresses
- Telephone numbers

2. Data protection law.

The Data Protection Act, 1998 (Amendment, 2013) describes how organisations, including schools, must collect, handle and store personal information. It refers to eight principles of compliance.

These rules apply regardless of whether data is stored electronically, on paper or on other materials or medium.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully

The Data Protection Act is underpinned by eight principles which state that personal data must:

1. Be fairly and lawfully processed
2. Processed for specified purposes
3. Be adequate, relevant and not excessive
4. Be accurate and up-to-date
5. Not be kept for longer than is necessary
6. Be processed in line with individuals' rights
7. Be secure
8. Not be transferred outside the European Economic Area without adequate protection

3. Data protection risks.

This policy helps to protect Thrussington C. of E. Primary School from some very real data security risks, including:

- **Breaches of confidentiality.** For example, information being disclosed inappropriately
- **Failing to offer choice.** For example, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For example, the School could be harmed if hackers successfully gained access to sensitive data.

4. Responsibilities.

Everyone who works for or with Thrussington Primary School has some responsibility for ensuring data is collected, stored and handled appropriately. All staff who process or use personal information must ensure that they follow these principles at all times. This Policy does not form part of the contract of employment for staff but it is a condition of employment that employees will abide by the rules and policies made by the School. Any failures to follow the Policy can result, therefore, in disciplinary proceedings.

4.1 The School must:

- Manage and process personal data appropriately – in line with this policy and data protection principles
- Protect individuals' right to privacy
- Provide an individual with access to all personal data held on them

4.2 The School, as a body, is the Data Controller under the 1998 Act and the Governors are ultimately responsible, therefore, for implementation.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

4.3 The School is required to notify the Information Commissioner (I.C.) of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's web-site on the following: http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

4.4 Every member of staff that holds personal information has to comply with the Act when managing that information.

4.5 The School is committed to maintaining the eight principles at all times. This means that the School will:

- inform Data Subjects why they need their personal information, how they will use it and with whom it may beshared. This is known as a Privacy Notice
- check the quality and accuracy of the information held
- apply the records' management policies and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal, it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information with others when it is necessary and legally appropriate to do so
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as access in the Data Protection Act

- train all staff so that they are aware of their responsibilities and of the School's relevant policies and procedures

This policy will be up-dated as necessary to reflect best practice or amendments made to the Data Protection Act, 1998. Note: such an amendment is expected in May, 2018.

4.6 The Board of Directors of Thrussington School is ultimately responsible for ensuring that it meets its legal obligations.

The School has identified its **Designated Data Controller** as the Headteacher. She is responsible for:

- Keeping the Board up-dated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures ad related policies, in line with an agreed schedule
- Arranging data protection procedures training and advice for people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data Thrussington School holds about them (also known as Subject Access Requests)
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
- Approving any data protection statements attached to communications such as e-mails and letters
- Addressing any data protection queries from journalists or media outlets such as newspapers

The Office Manager is responsible for:

- Ensuring that all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services the School is considering using to store or process data
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General staff guidelines.

- The only people able to access data covered by this policy should be those who **need it for their work.**
- Data **should not be shared informally.** When access to confidential information is required, employees can request it from their line managers.
- **Thrussington School will provide training** to all employees to help them understand their responsibilities when handling data.

- Employees are to keep all data secure by taking reasonable precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **is not to be disclosed** to unauthorised people, either within the School or externally.
- Data should be **regularly reviewed and up-dated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from the Office Manager or the Headteacher if they are unsure of any aspect of data protection

5. Data storage.

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Office Manager or the Headteacher.

When data is **stored on paper, it should be kept in a secure place** where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a **locked drawer or filing cabinet –** somewhere secure.

- Employees should make sure paper and printouts are **not left where unauthorised people could see them,** such as on a printer.

- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically,** it must be protected from unauthorised access, accidental deletion and malicious hacking attempts and violations:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.

- If data is **stored on removable media** (e.g. CD or DVD) these should be kept locked away securely when not being used.

- Data should only be stored on **designated drivers and servers** and should only be uploaded to an **approved cloud computing services**.

- Servers containing personal data should be **sited in a secure location**, away from general office space.

- Data should be **backed up frequently**. Those back-ups should be tested regularly, in line with the School's standard back-up procedures.

- Data should **never be saved directly** to lap-tops or other mobile devices such as tablets or smart phones or any recording / saving device.

- All servers and computers containing data should be protected by **approved security software and a firewall.**

6. Data use

Personal data is of no value to Thrussington School unless the School can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked when left unattended.**

- Personal data **should not be shared informally**. In particular, it should never be sent by e-mail, as this form of communication is not secure.

- Data must be **encrypted before being transferred electronically**. The Office Manager can explain how to send data to authorised external contacts.

- Personal data should **never be transferred outside the European Economic Area.**

- Employees **should not save copies of personal data to their own computers**. Always access and up-date the central copy of any data.

7. Data accuracy

The law requires Thrussington School to take reasonable steps to ensure that data is kept accurate and up-to-date.

The more important it is that the personal data is accurate, the greater the effort Thrussington School should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure that it is kept as accurate and up-to-date as possible.

- Data will be held in **as few places as necessary.** Staff should not create any unnecessary additional data sets

- Staff should **take every opportunity to ensure data is up-dated.** For instance, by confirming an individual's details when they call.

- Thrussington School will make it **easy for data subjects to up-date the information** Thrussington School holds on them. An example would be through the web-site.

- Data should be **up-dated as inaccuracies are discovered.** For example, if an individual can no longer be contacted on their stored telephone number, it should be removed from the database.

- It is the Office Manager's responsibility to ensure that **marketing databases are checked against industry suppression files** every six months.

8. Subject access requests

All individuals who are the subject of personal data held by Thrussington School are entitled to:

- Ask **what information** the School holds about them and why.

- Ask **how to gain access** to it.

- Be informed **how to keep it up to date.**

- Be informed how the School is **meeting its data protection obligations.**

If an individual contacts the School requesting this information, this is called a subject access request.

The School may make a charge on each occasion that access is requested in order to meet the costs of providing the details of the information held.
The School aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within forty days, as required by the1998 Act.

The data controller will always verify the identity of anyone making a subject access request before passing on any information.

Subject access requests from individuals should be made by e-mail, addressed to the data controller at office@thrussington.leics.sch.uk .

9. Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Thrussington School will disclose requested data. However, the data controller will ensure that the request is legitimate, seeking assistance from the Board and from the School's legal advisors where necessary.

10. Providing information

Thrussington School aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

There is a limited number of exceptions to the School's duty to disclose the personal data of an employee:

- References received from other employers if disclosure would impart information about another individual (unless that individual consents)
- Documents that would prejudice Thrussington School (i.e. becoming part of a multi- academy trust; redundancies etc.)
- Documents that would compromise Thrussington School's negotiating position (e.g. regarding salaries)
- Documents that are relevant to legal proceedings in relation to legal rights

- Documents that might compromise national security or hamper the detection of crime

11. Breaches

A data breach is an incident in which sensitive, protected or confidential data, potentially, has been viewed, stolen or used by an individual unauthorised to do so. Data breaches may involve personal health information, personally identifiable information, trade secrets or intellectual property.

Any such breach will initiate relevant sanctions (e.g. disciplinary, civil proceedings)

12. Retention of data

Thrussington School has a duty to retain some staff and personal data for a period of time following their departure from School, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time.

Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact the School.

This is on-going. Where any clarifications or actions are required, the Policy will be amended at review.
Autumn, 2015.

Autumn, 2016.

Signed:

To be reviewed: Autumn, 2017.