

Trent CE Primary School



Data Protection Policy

Table of Contents

1. Introduction.....	2
2. Statement of intent	4
3. Data controller	5
4. Data security.....	5
5. Subject Consent	6
6. Rights to access information	6
7. Publication of information	7
8. Data retention	7
9. Challenges and compensation	7

DATA PROTECTION POLICY

1. Introduction

Trent CE Primary School holds a considerable amount of both personal and public data. It is essential that data, which is personal, remains confidential and data that is public can be made safely available if requested. However, there is sometimes confusion over what is personal and what is public data. The aim of this policy is to provide guidance in this respect. The eight data protection principles are the key to finding that balance and ensuring compliance with the DPA

The Eight Data Protection Act Principles

The act contains eight “Data Protection Principles”. These specify that personal data must be:

1. Processed fairly and lawfully.
2. Obtained for specified and lawful purposes.
3. Adequate, relevant and not excessive.
4. Accurate and up to date.
5. Not kept any longer than necessary.
6. Processed in accordance with the “data subject’s” (the individual’s) rights.
7. Securely kept.
8. Not transferred to any other country without adequate protection in situ.

Practical considerations

Personal data – we recognise the need to handle personal information in line with the data protection principles.

Fair processing – we let pupils and staff know what we do with the personal information recorded about them. We make sure we restrict access to personal information to those who need it.

Security – we keep confidential information secure when storing it, using it and sharing it with others.

Disposal – when disposing of records and equipment, we make sure personal information cannot be retrieved from them.

Policies – we have clear, practical policies and procedures on information governance for staff and governors to follow, and monitor their operation.

Subject access requests – we recognise, log and monitor subject access requests.

Data sharing – we check to be sure that we are allowed to share information with others and make sure it is kept secure when shared.

Websites – we control access to any restricted area. We make sure we are allowed to publish any personal information (including images) on our website.

CCTV – we inform people what it is used for and review retention periods.

Photographs – if our school takes photos for publication, we mention our intentions in our fair processing/privacy notice.

Processing by others – we recognise when others are processing personal information for us and make sure they do it securely.

Training – we train staff and governors in the basics of information governance; we recognise where the law and good practice need to be considered; and we know where to turn for further advice.

Freedom of information – after consultation, we notify staff what personal information we would provide about them when answering FOI requests.

Definitions

Personal data is information that relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records

Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences.

The difference between processing personal data and sensitive personal data is that there are greater legal restrictions on the latter.

Procedures

Physical Security and Procedures

We regularly review the physical security of buildings and storage systems, and access to them. This includes storage of paper records and the equipment used to store and process information electronically. Where there is an increased risk of vandalism or burglary, we take these into account

Electronic personal data

Strong passwords, i.e. at least eight characters long and containing special symbols, are used to access any electronic equipment that holds confidential personal information. Some portable devices use encryption software to protect confidential personal information, particularly if they are taken from school premises

Memory sticks should not be used to hold personal information or they should be password protected and fully encrypted

Use of private computer equipment

If any of the school's personal information is held on private equipment, the school will remain responsible unless it can prove it did everything reasonably possible to keep the information secure.

Paper-based personal data

Whenever possible, storage rooms, strong cabinets, and other storage systems with locks should be used to store paper records.

Papers containing confidential personal information should not be left in public view.

Particular care should be taken if documents have to be taken out of school.

Disposal of data

Disposal is a form of processing that needs to be done fairly and in accordance with the seventh principle.

“The method of destruction of personal data should take into account the nature of the information. In all cases you must ensure that data is disposed of in a way that creates little risk of an unauthorised third party using it to the data subject’s detriment. If any confidential information is held on paper records, they should be shredded or pulped; electronic memories should be scrubbed clean or destroyed”

Policies

The Headteacher has responsibility for raising general data protection awareness and ensuring that policies are adhered to and updated as necessary

Subject access requests

Section 7 of the DPA gives individuals the right to request the personal information a school holds about them – the right of subject access.

Subject access requests (SARs) are answered within 40 calendar days of receipt. We charge a fee of £10 for answering a SAR. A valid SAR should be in writing – this can include fax or email – and should confirm the requester’s identity. We can recognise a subject access request and know who to turn to for detailed advice to ensure compliance with the DPA. We keep a log of the requests that require formal consideration.

Sharing personal information

At times we share personal information with other organisations. Sharing personal information involves providing it to another organisation or person so that they can make use of it. It does not extend to the use of personal information within the school, including use by the governing body.

The main organisations that we share personal data with are:

- local authorities;
- other schools and educational bodies; and
- social services.

When sharing information with other organisations, we use secure internal email systems. When we share paper-based confidential personal information, we make sure it reaches the intended recipient.

Freedom of Information Act /Environmental Information Regulations

We have an approved publication scheme and reply to requests for information in line with this legislation.

2. Statement of intent

Trent CE Primary School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the Data Protection Act 1998.

This policy will outline how Trent CE Primary School will comply with the key principles of the Data Protection Act:

- Data must be processed fairly and lawfully.
- Data must only be acquired for one or more lawful purposes and should not be processed for other reasons.
- Data must be adequate, relevant and not excessive.
- Data must be kept accurate and up-to-date.
- Data must not be kept for longer than is necessary.

- Data must be processed in accordance with the data subject's rights.
- Appropriate measures must be taken to prevent unauthorised or unlawful access to the data and against loss, destruction or damage to data.
- Data must not be transferred to a country or territory unless it ensures an adequate level of protection for the rights of the subject.

Mrs Yarwood Headteacher Mrs R Taylor Acting Chair of Governors

Next review May 2016

3. Data controller

The school as the corporate body is the Data Controller.

The governing body of Trent School therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The Mrs K Bagai the School Business Manager will deal with the day-to-day matters relating to data protection. Mrs Louise Yarwood, Head teacher remains the lead contact.

Staff responsibilities

Trent School recognises that its staff members and pupils need to know what the School does with the information it holds about them.

All staff members, including members of the School Governing Body will receive training in their responsibilities under the Data Protection Act as part of their HR induction.

Parents will also receive a copy of the Data Protection Policy upon registration of their child at Trent CE Primary School as well as an overview of the information that the School will keep about their child.

Staff members and parents are responsible for checking that any information that they provide to Trent School in connection with their employment or in regard to a registered pupil is accurate and up-to-date.

The Trent School cannot be held accountable for any errors unless the employee or parent has informed the school about such changes.

4. Data security

Staff members of Trent CE Primary School will ensure that personal data is secured in accordance with the provisions of the Data Protection Act by:

- Keeping the data in a locked filing cabinet.
- Ensuring that computerised data is coded, encrypted or password protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage, holding the storage device in a locked filing cabinet.

Trent CE Primary School takes its duties under the Data Protection Act seriously and any unauthorised disclosure may result in disciplinary action.

5. Subject Consent

Trent Primary School understands that subjects have certain legal rights to their personal data, which will be respected.

The school will not process personal data without the consent of the subject, although the processing of data will sometimes be necessary where:

- The processing is necessary for the performance of a contract to which the subject is party or in the taking of steps with a view to entering a contract.
- The processing is necessary for compliance with a legal obligation to which the school is subject.
- The processing is necessary for the administration of justice, legal functions of persons or departments, or functions of a public nature exercised in the public interest.
- Where the processing is necessary for the purposes of legitimate interests of the school unless the decision prejudices the rights, freedoms or legitimate interests of the subject.

Staff members of the school will be working in close contact with children. Disclosure and Barring Service (DBS) checks will therefore be made a condition of employment in order to ensure that potential employees do not pose a threat or danger.

Sensitive data can only be processed with the explicit consent of the subject, including information relating to a subject's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, their sex life, or the commission of any offence.

Sensitive data will only be processed if:

- It is necessary to protect the subject's vital interests.
- It is carried out in the course of legitimate activities by a not for profit body or association with appropriate safeguards.
- It is necessary for the administration of justice or other legal purposes.
- It has been ordered by the Secretary of State.
- It is necessary to prevent fraud.
- It is necessary for medical purposes.
- It is necessary for equality reasons.
- It was made public deliberately by the data subject.

6. Rights to access information

All staff members, parents of registered pupils and other users are entitled to:

- Know what information the school holds and processes about them or their child and why.
- Understand how to gain access to it.

- Understand how to keep it up-to-date.
- Understand what the school is doing to comply with its obligations under the Data Protection Act.

All staff members, parents of registered pupils and other users have the right under the Data Protection Act 1998 to access certain personal data being held about them or their child.

The school aims to comply with requests for access to personal information as quickly as possible, but will ensure that it meets its duty under the Data Protection Act to provide it within 40 working days.

The school may make a charge, no more than £20 on each occasion that access is requested.

However, the school is not obliged to provide unstructured personal data if the administrative cost is deemed to exceed the limit of £450 as contained in the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations.

7. Publication of information

Trent Primary School will publish a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Trent policies and procedures.
- Minutes of meetings.
- Annual reports.
- Financial information.

Classes of information specified in the publication scheme will be made available quickly and easily on request.

8. Data retention

The Data Protection Act 1998 states that data should not be kept for longer than is necessary.

In the case of Trent Primary School, unrequired data will be deleted as soon as practicable.

Some educational records relating to a former pupil or employee of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Records of DBS checks will be destroyed immediately, although the date that the check was made will be retained in the school's file.

9. Challenges and compensation

Trent understands that staff members and the parents of registered pupils have the right to prevent the processing of personal data if it is likely to cause damage or distress.

Concerns related to the processing of personal data should be raised with the [designated data controller](#).

Data subjects reserve the right to take their concerns to a court of law and will be entitled to compensation if it is judged that the school contravened the provisions of the Data Protection Act.

Individuals who are not the subject of the data, but suffer damage as a result of the contravention, are also entitled to compensation.

The school will immediately rectify, block, erase or destroy any data that a court of law judges to have contravened the requirements of the Data Protection Act.