# West Tytherley CE Primary School and the GDPR:
# How we keep data entrusted to us safe

## What is GDPR?

Is essentially about being transparent and responsible in the way we handle personal data (e.g. only sharing it with those who need to have access to it). And collecting only the data that is needed (to meet our legal obligations to run a public service) and getting informed consent for personal data we would like by explaining how it will be used.

## What is personal data?

Data that contains any information that can create personal identification, for example your date of birth and address. Or any information that is held that could be used in conjunction with other information that is accessible to identify someone e.g. full name and the class they are in at school.

## Specifically:

Personal data shall be processed fairly and lawfully and shall be obtained only for one or more specified and lawful purposes; and shall not be further processed in any manner incompatible with that intended purpose.

## What is processing personal data?

How personal data is used within an organisation; and how and why it is shared.

## Exceptions:

Schools do not need consent to process personal data to complete tasks essential to running a school (e.g. submitting a child for an exam).
GDPR does not prevent or limit sharing of personal data in safeguarding.

## What about consent?

We need to apply best principles when creating or processing data for tasks not considered “essential” for running the school. In these instances, parents/ guardians need to explicitly consent to the scope of usage of their children's data outside the processes essential to run the school.

In order for parents to be able to do this, the school must be explicit in what processes they will use the child's information in these circumstances.

Good guiding principles in all cases are: does the information I am using need to be identifiable data? Can I make it non-identifiable?

## What isn’t personal data?

Any data that can not be used to trace a living human. For data to be identifiable it needs to be unique to that individual. For example, in a large school you may have two

children with the same first and second name; which is why name and address together create identifiable data.
Aggregating (pooling all the data of a group of data subjects together) and anonymizing/ psuedonymizing data (creating non- identifiable ways of giving data references to help your process e.g. using random numbers to identify the data such as 'child 1') are a good way of making sure when you use data it isn't personal data.

**What is sensitive personal data?**
Under the GDPR sensitive personal data has even more restrictions to ensure it is protected than personal data. Sensitive data is any data that could be used to discriminate against an individual, for example sexual orientation, race, physical or mental health, political opinions or criminal history.
To process sensitive personal data you *must* satisfy at least one of the special conditions laid out in the GDPR.

**Understanding the principles of good data management under GDPR:**
Good data management means a careful consideration of how data is stored, how long it is retained and how and when it is destroyed. It is also being clear about the risks of data breaches and managing these risks.

Good data management under the GDPR hangs on understanding roles and responsibilities of 3 entities: the data subject, the data controller and the data processor.
-- *Data subject* is the child, or a parent, employee; anyone who is identifiable by the information you hold on them
--*Data controller* is the organisation or person who is responsible for collecting and deciding how that data is processed and shared e.g. registers of children made by WTS for school trips
--*Data processor* can be software or an organisation that is responsible for handling the personal information according to the desires of the data controller e.g. school admission data from HCC makes us the data processor for children's data coming to our school from SIMS

Data processors and data controllers are liable to GDPR. In a lot of our tasks relating to children's data, we are data processors (see data asset register), which means we use data according to central and local government processes to run the school.
Being a data processor does not mean you can neglect your responsibilities for good data management. Under the law, even if you have to process data (e.g. in a safeguarding situation) you are still liable for the manner in which you process, store and share that data.

In situations where WTS is the data controller (creating data on identifiable children) we have to be particularly mindful of good data management principles GDPR enshrines.

**What changes does GDPR bring to the school?**

As a school there is emphasis now on us to be able to demonstrate our compliance with data protection. This involves demonstrating we are undertaking the following 5 actions:

1. To have a "data asset register" of West Tytherley School (what personal data we hold) and a risk assessment of security of this. For data items that score a medium or high risk of data protection breach, to have an action plan in place.

2. To increase awareness for all staff on implications of GDPR.
   All staff working with WTS need to be updated on good data management principles and implications of GDPR when working in a school

3. To communicate to parents and guardians how we are managing personal data at the school and reassure them about our stewardship of their child's and their own personal data

4. To create/ review the mechanism for anyone to report a potential data security breach at the school

5. To review data sharing agreements with all third parties that West Tytherley School deals with and ensure they are robust enough and enshrine good data management principles