Keep personal data safe

Personal data: any information relating to an **identifiable living person**, e.g name, contact details, ID numbers, attendance and assessment information.

Sensitive personal data: information that reveals someone's ethnic origin, political opinions, religion, sexuality or health. In our school, it also means whether a child is looked-after, has SEN, or is eligible for free school meals

DO:

✓ Keep personal data anonymous where possible

✓ Only collect information about pupils and parents/carers that you actually need

✓ Think before you put information up on the wall ...
  - Do you have a good reason to display it?
  - Do you need consent from the parent or pupil?
  - Might there be a safeguarding risk in displaying it?

✓ Keep data in a safe place when taking it home

✓ Double-check that you're emailing personal data to the correct person, who has the right to view it

✓ Password-protect email attachments that contain personal data

✓ Read and understand all of the school's policies on data protection

✓ Report safeguarding concerns to the relevant people where you're concerned about a child – data protection laws DO NOT stop you from doing this

DON'T:

✗ Leave personal data unattended on your desk, or anywhere else someone might see it when they aren't supposed to

✗ Take any sensitive or confidential personal information home with you

✗ Use a memory stick. If you really need to, make sure it's encrypted

If in doubt, talk to our data protection officer: _____

Report to them **immediately** if you think personal data has been lost, stolen or wrongly disclosed, so that we can quickly take steps to mitigate the impact. Also speak to them if you have any concerns at all about keeping personal data safe.