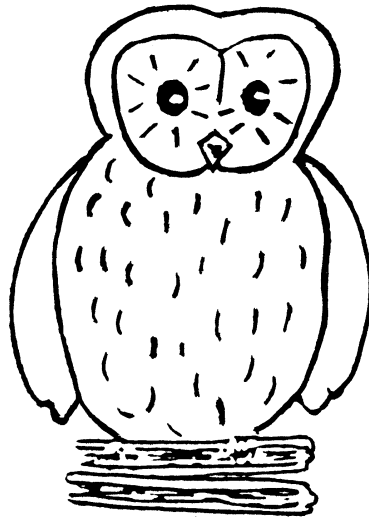


Overstone Primary School



Data Protection Policy

This Policy was approved by the Resources Committee on 24th January 2017
To be ratified by Governors at their meeting on 8th February 2017

To be reviewed on a Bi- Annual basis, i.e. **due for review in March 2019.**

At Overstone Primary School we have a clear understanding of how children learn and continually strive to provide the best possible conditions to facilitate this. We acknowledge that we live in a changing world and that we need to prepare our children for tomorrow's needs. Consequently we not only place value on the key skills of reading, writing, oral communication and mathematical understanding, but also on developing skills for life in modern Britain. We aim to deliver a world class curriculum that will challenge and inspire all our pupils and prepare them for the future.

We have three overall aims for our pupils to become:

- Successful learners who achieve and enjoy learning
- Confident individuals who can live safe and healthy lives
- Responsible citizens who make a positive contribution to society and achieve economic well being

Under the **Data Protection Act 1998** all schools processing personal data must comply with the eight enforceable principles of good practice. Data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with the data subject's rights
- secure
- not transferred to other countries without adequate protection.

To comply with these principles every school processing personal data must notify under the Act.

Overstone Primary School will ensure that:

- An Annual registration notification form and fee is paid to the Information Commissioner's Office to comply with Data Protection Notification.
- Data collection sheets will be given to staff and parents/guardians of pupils annually to check details for accuracy, usually in the Autumn/Winter term.
- A Privacy Statement/Fair Processing Notice will also be given to staff and to the parents/guardians of pupils annually.
- Requests for information comply with Freedom of Information requirements and a FOI Policy/Publication Scheme is held.
- Care will be taken when disclosing any personal details and publishing details of pupils, including photographs/images, to ensure that they do not put individuals at risk from harm; prior consent will be obtained where necessary.
- Personal data will be stored in a secure and safe manner. Effective controls, including passwords and physical security will be maintained to prevent unauthorised access to computerised and manual records.

- Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or to organisations that have a legal right to receive the data without consent being given and never for commercial purposes.
- When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.
- If a request is made in person for personal data to be disclosed it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the individual is not known personally, proof of identity should be requested.
- Information Protection and Security breaches will be investigated; appropriate actions will be taken and documented.
- Staff will be given instructions on information protection and security matters, including the secure handling, disclosure, transfer and final destruction of information.
- Admin staff will ensure secure data transfer systems are used for transferring pupil data onto destination schools.
- Admin staff will ensure pupil files are held in secure areas and passed on securely.
- All SEN information to be held securely, access being limited to appropriate members of staff only.
- Safeguarding information to be held securely with strict access being limited to Child Protection Officers only.
- Back-up tapes/discs for the admin/curriculum servers are stored securely.